58

АДМИНИСТРАЦИЯ
МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ ГОРОДСКОЙ ОКРУГ
ГОРОД-КУРОРТ СОЧИ КРАСНОДАРСКОГО КРАЯ

Р А С П О Р Я Ж Е Н И Е

от 16.08.2021 № 300-р

Об утверждении документов, определяющих правила и процедуры для обеспечения защиты информации в администрации муниципального образования городской округ город-курорт Сочи Краснодарского края

02136

В целях реализации полномочий администрации муниципального образования городской округ город-курорт Сочи Краснодарского края, а также отраслевых (функциональных) и территориальных органов администрации муниципального образования городской округ город-курорт Сочи Краснодарского края и обеспечения их взаимодействия при осуществлении деятельности по обеспечению информационной безопасности защищаемой информации, на основании Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», Постановления Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Постановления Правительства Российской Федерации от 21 марта 2012 года № 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», приказа Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»:

1. Утвердить:

1.1. Политику обработки персональных данных администрации муниципального образования городской округ город-курорт Сочи Краснодарского края (приложение № 1).

1.2. Правила обработки персональных данных в администрации муниципального образования городской округ город-курорт Сочи Краснодарского края (приложение № 2).

1.3. Перечень защищаемой информации в администрации муниципального образования городской округ город-курорт Сочи Краснодарского края (приложение № 3).

1.4. Инструкцию по модификации и техническому обслуживанию программного обеспечения и аппаратных средств информационных систем администрации муниципального образования городской округ город-курорт Сочи Краснодарского края (приложение № 4).

1.5. Инструкцию пользователя информационных систем администрации муниципального образования городской округ город-курорт Сочи Краснодарского края (приложение № 5).

1.6. Политику резервного копирования и восстановления работоспособности технических средств и программного обеспечения, баз данных, средств и систем защиты информации в информационных системах администрации муниципального образования городской округ город-курорт Сочи Краснодарского края (приложение № 6).

1.7. Правила аудита и регистрации событий безопасности в информационных системах администрации муниципального образования городской округ город-курорт Сочи Краснодарского края (приложение № 7).

1.8. Правила идентификации и аутентификации пользователей в информационных системах администрации муниципального образования городской округ город-курорт Сочи Краснодарского края (приложение № 8).

1.9. Правила использования мобильных устройств в информационных системах администрации муниципального образования городской округ город-курорт Сочи Краснодарского края (приложение № 9).

1.10. Политику использования съемных носителей информации в информационных системах администрации муниципального образования городской округ город-курорт Сочи Краснодарского края (приложение № 10).

1.11. Политику контроля защищенности в информационных системах администрации муниципального образования городской округ город-курорт Сочи Краснодарского края (приложение № 11).

1.12. Политику контроля и управления доступом к информационным системам администрации муниципального образования городской округ город-курорт Сочи Краснодарского края (приложение № 12).

1.13. Политику обеспечения безопасности удаленного доступа к информационным системам администрации муниципального образования городской округ город-курорт Сочи Краснодарского края (приложение № 13).

1.14. Правила организации антивирусной защиты в информационных системах администрации муниципального образования городской округ город-курорт Сочи Краснодарского края (приложение № 14).

1.15. Правила по внесению изменений в списки пользователей и наделению их полномочиями доступа к информационным системам

администрации муниципального образования городской округ город-курорт Сочи Краснодарского края (приложение № 15).

1.16. Политику управления изменениями программного обеспечения и технических средств в информационных системах администрации муниципального образования городской округ город-курорт Сочи Краснодарского края (приложение № 16).

1.17. План мероприятий по защите информации в информационных системах администрации муниципального образования городской округ город-курорт Сочи Краснодарского края (приложение № 17).

1.18. Политику защиты технических средств администрации муниципального образования городской округ город-курорт Сочи Краснодарского края (приложение № 18).

1.19. Инструкцию об осуществлении контроля выполнения требований по защите персональных данных в администрации муниципального образования городской округ город-курорт Сочи Краснодарского края (приложение № 19).

1.20. Порядок доступа служащих администрации муниципального образования городской округ город-курорт Сочи Краснодарского края в помещения, в которых ведётся обработка персональных данных (приложение № 20).

1.21. Положение по работе с инцидентами информационной безопасности в администрации муниципального образования городской округ город-курорт Сочи Краснодарского края (приложение № 21).

2. Отраслевым (функциональным) и территориальным органам администрации муниципального образования городской округ город-курорт Сочи Краснодарского края, обладающим правом юридического лица, в своей деятельности по обеспечению безопасности информации, в том числе персональных данных, руководствоваться утвержденными настоящим распоряжением документами.

3. Руководителям отраслевых (функциональных) и территориальных органов администрации муниципального образования городской округ город-курорт Сочи Краснодарского края в тридцатидневный срок со дня вступления в силу настоящего распоряжения обеспечить ознакомление муниципальных служащих с настоящим распоряжением.

4. Отраслевым (функциональным) и территориальным органам администрации муниципального образования городской округ город-курорт Сочи Краснодарского края, не обладающим правом юридического лица, предоставить листы ознакомления в департамент муниципальной службы и кадровой политики администрации муниципального образования городской округ город-курорт Сочи Краснодарского края.

5. Отраслевым (функциональным) и территориальным органам администрации муниципального образования городской округ город-курорт Сочи Краснодарского края, обладающим правом юридического лица, обеспечить надежное хранение листов ознакомления.

6. Управлению информатизации и связи администрации

муниципального образования городской округ город-курорт Сочи Краснодарского края (Лавриенко) разместить настоящее распоряжение на официальном сайте администрации муниципального образования городской округ город-курорт Сочи Краснодарского края в информационно-коммуникационной сети Интернет.

7. Контроль за выполнением настоящего распоряжения возложить на заместителя главы муниципального образования городской округ город-курорт Сочи Краснодарского края Петухову И.А.

8. Настоящее распоряжение вступает в силу со дня его подписания.

Глава города Сочи А.С.Копайгородский

Департамент муниципальной службы и кадровой политики

Приложение № 1
к распоряжению администрации
муниципального образования городской
округ город-курорт Сочи
Краснодарского края
от 16.08.2021 № 300-р

ПОЛИТИКА
обработки персональных данных администрации муниципального образования городской округ город-курорт Сочи Краснодарского края

1. Общие положения

1.1. Назначение политики

Настоящая политика обработки персональных данных администрации муниципального образования городской округ город-курорт Сочи Краснодарского края (далее – Политика) определяет цели и общие принципы обработки персональных данных, а также реализуемые меры защиты персональных данных в администрации муниципального образования городской округ город курорт Сочи Краснодарского края, а также отраслевых (функциональных) и территориальных органах администрации муниципального образования городской округ город-курорт Сочи Краснодарского края (далее – Оператор). Политика является общедоступным документом Оператора и предусматривает возможность ознакомления с ней любых лиц.

1.2. Основные понятия

автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;

безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных;

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

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

конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания;

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

средств, аналогичных им по своим функциональному предназначению и техническим характеристикам;

обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

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

оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

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

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

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

технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации;

трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;

угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение

персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных;

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.

1.3. Основные права Оператора

Оператор оставляет за собой право проверить полноту и точность предоставленных персональных данных. В случае выявления ошибочных или неполных персональных данных, Оператор имеет право прекратить все отношения с субъектом персональных данных.

1.4. Основные обязанности Оператора

Оператор не собирает персональные данные, не обрабатывает и не передаёт персональные данные субъектов персональных данных третьим лицам, без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

1.5. Основные права субъекта

Субъект персональных данных имеет право:

1) получить сведения, касающиеся обработки его персональных данных Оператором;

2) потребовать 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;

3) отозвать согласие на обработку персональных данных в предусмотренных законом случаях.

2. Цели сбора персональных данных

Целями обработки персональных данных являются:

1) реализация функций исполнительно-распорядительного органа муниципального образования городской округ город-курорт Сочи Краснодарского края;

2) исполнение договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект персональных данных, а также заключение договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

3) реализация функций работодателя.

3. Правовые основания обработки персональных данных

Оператор обрабатывает персональные данные, руководствуясь:

1) договорами с контрагентами;

2) Федеральным законом от 2 марта 2007 года № 25-ФЗ «О муниципальной службе в Российской Федерации»;

3) Федеральным законом от 2 мая 2006 года № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»;

4) статьями 86-90 Трудового кодекса Российской Федерации;

5) Федеральный закон от 27 июля 2004 года № 79-ФЗ «О государственной гражданской службе Российской Федерации»;

6) Федеральным законом от 06 октября 2003 года № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации»;

7) Уставом муниципального образования городской округ город-курорт Сочи Краснодарского края;

8) Административными регламентами предоставления муниципальных услуг.

4. Объем и категории обрабатываемых персональных данных, категории субъектов персональных данных

Оператор осуществляет на законной и справедливой основе обработку персональных данных (далее – ПДн) следующих физических лиц (субъектов ПДн):

4.1. Цель: «реализация функций исполнительно-распорядительного органа муниципального образования городской округ город-курорт Сочи Краснодарского края» достигается посредством обработки персональных данных следующих категорий для следующих субъектов:

1) получатели муниципальных услуг (граждане, в том числе индивидуальные предприниматели):

Специальные категории: национальная принадлежность.

Иные категории: фамилия, имя, отчество, год рождения, дата рождения, место рождения, адрес, паспортные данные, контактные сведения, гражданство, СНИЛС, ИНН, социальное положение, имущественное положение, ОГРНИП, семейное положение, дата, время, причина смерти, информация о трудовой деятельности, состав семьи, адрес электронной почты, данные доверенности.

Объем: менее чем 100 000 субъектов персональных данных

2) граждане:

Иные категории: адрес, фамилия, имя, отчество, контактные сведения.

Объем: менее чем 100 000 субъектов персональных данных

4.2. Цель «исполнение договора с субъектом» достигается посредством обработки персональных данных следующих категорий для следующих субъектов:

1) контрагенты:

Иные категории: контактные сведения, банковские реквизиты, адрес, ИНН, фамилия, имя, отчество, паспортные данные, сведения о доверенности, гражданство, ОГРНИП.

Объем: менее чем 100 000 субъектов персональных данных

4.3. Цель «реализация функций работодателя» достигается посредством обработки персональных данных следующих категорий для следующих субъектов:

1) ближайшие родственники муниципальных служащих:

Иные категории: фамилия, имя, отчество, трудоспособность, дата рождения, сведения о доходах, имуществе и обязательствах имущественного характера, пребывание за границей, адрес, информация о трудовой деятельности, степень родства.

Объем: менее чем 100 000 субъектов персональных данных

2) уволенные (уволившиеся) муниципальные служащие:

Специальные категории: судимость.

Иные категории: фамилия, имя, отчество, адрес, гражданство, семейное положение, степень родства, доходы, профессия, ИНН, банковские реквизиты, государственные награды, дата рождения, контактные сведения, состав семьи, имущественное положение, информация о трудовой деятельности, СНИЛС, фотография, прежние фамилия, имя, отчество, допуск к государственной тайне, сведения о доходах, имуществе и обязательствах имущественного характера, место рождения, паспортные данные, сведения о воинском учёте, образование, трудоспособность, звание, классный чин федеральной гражданской службы, дипломатический ранг, воинское или специальное звание, классный чин правоохранительной службы, классный чин гражданской службы субъекта Российской Федерации, квалификационный разряд государственной службы, квалификационный разряд или классный чин муниципальной службы, пребывание за границей, данные загранпаспорта, результаты обязательных предварительных (при поступлении на работу) и периодических медицинских осмотров (обследований), а также обязательного психиатрического освидетельствования, наличие (отсутствие) заболевания препятствующего поступлению на государственную гражданскую службу Российской Федерации или её прохождению, подтверждённого заключением медицинского учреждения, сведения о повышении квалификации, ученая степень.

Объем: менее чем 100 000 субъектов персональных данных

3) муниципальные служащие:

Специальные категории: судимость.

Иные категории: место рождения, паспортные данные, семейное положение, имущественное положение, информация о трудовой деятельности, СНИЛС, результаты обязательных предварительных (при поступлении на работу) и периодических медицинских осмотров (обследований), а также обязательного психиатрического освидетельствования, наличие (отсутствие) заболевания препятствующего поступлению на государственную гражданскую службу Российской Федерации или её прохождению, подтверждённого заключением медицинского учреждения, сведения о доходах, имуществе и обязательствах имущественного характера, допуск к государственной тайне, фамилия, имя, отчество, адрес, сведения о воинском учёте, состав семьи, доходы, профессия, трудоспособность, банковские реквизиты, прежние фамилия, имя, отчество, дата рождения, контактные сведения, гражданство, степень родства, образование, ИНН, пребывание за границей, данные загранпаспорта, государственные награды, звание, классный чин федеральной гражданской службы, дипломатический ранг, воинское или специальное звание, классный чин правоохранительной службы, классный чин гражданской службы субъекта

Российской Федерации, квалификационный разряд государственной службы, квалификационный разряд или классный чин муниципальной службы, сведения о повышении квалификации, ученая степень, фотография.

Объем: менее чем 100 000 субъектов персональных данных.

5. Порядок и условия обработки персональных данных

5.1. Перечень действий с персональными данными, осуществляемых Оператором.

Оператором осуществляются следующие действия с персональными данными: запись, извлечение, использование, накопление, передача (предоставление, доступ), сбор, систематизация, удаление, уточнение (обновление, изменение), хранение.

5.2. Способы обработки персональных данных

Оператором применяются следующие способы обработки персональных данных: смешанная обработка персональных данных с передачей по внутренней сети и сети интернет.

5.3. Передача персональных данных третьим лицам

1) Публичное акционерное общество «Сбербанк России»

Условия передачи персональных данных: поручение Оператора.

Местонахождение третьего лица: Россия, г. Москва, ул. Вавилова, д. 19.

Трансграничная передача персональных данных не осуществляется.

Цели передачи персональных данных: начисление заработной платы в рамках банковского зарплатного проекта.

Объем передаваемых данных: менее чем 100 000 субъектов персональных данных.

Перечень действий, разрешенных третьему лицу: запись, хранение, извлечение, удаление, сбор, систематизация, накопление, уточнение (обновление, изменение), использование, передача (предоставление, доступ).

Способы обработки ПДн третьим лицом: смешанная обработка персональных данных без передачи по внутренней сети, но с передачей в сеть интернет.

2) Акционерное общество «Райффайзенбанк»

Условия передачи персональных данных: поручение Оператора.

Местонахождение третьего лица: Россия, г. Москва, ул. Троицкая, д. 17, стр. 1.

Трансграничная передача персональных данных не осуществляется.

Цели передачи персональных данных: начисление заработной платы в рамках банковского зарплатного проекта.

Объем передаваемых данных: менее чем 100 000 субъектов персональных данных.

Перечень действий, разрешенных третьему лицу: уточнение (обновление, изменение), передача (предоставление, доступ), сбор, запись, систематизация, накопление, хранение, извлечение, использование, удаление.

Способы обработки ПДн третьим лицом: смешанная обработка персональных данных без передачи по внутренней сети, но с передачей в сеть интернет.

3) Публичное акционерное общество «Банк ВТБ»

Условия передачи персональных данных: поручение Оператора.

Местонахождение третьего лица: Россия, г. Москва, ул. Воронцовская, д. 43, стр. 1.

Трансграничная передача персональных данных не осуществляется.

Цели передачи персональных данных: начисление заработной платы в рамках банковского зарплатного проекта.

Объем передаваемых данных: менее чем 100 000 субъектов персональных данных.

Перечень действий, разрешенных третьему лицу: запись, хранение, извлечение, удаление, сбор, систематизация, накопление, уточнение (обновление, изменение), использование, передача (предоставление, доступ).

Способы обработки ПДн третьим лицом: смешанная обработка персональных данных без передачи по внутренней сети, но с передачей в сеть интернет.

4) Публичное акционерное общество «Промсвязьбанк»

Условия передачи персональных данных: поручение Оператора.

Местонахождение третьего лица: Россия, г. Москва, ул. Смирновская, д. 10, стр. 22.

Трансграничная передача персональных данных не осуществляется.

Цели передачи персональных данных: начисление заработной платы в рамках банковского зарплатного проекта.

Объем передаваемых данных: менее чем 100 000 субъектов персональных данных.

Перечень действий, разрешенных третьему лицу: запись, хранение, извлечение, удаление, сбор, систематизация, накопление, уточнение (обновление, изменение), использование, передача (предоставление, доступ).

Способы обработки ПДн третьим лицом: смешанная обработка персональных данных без передачи по внутренней сети, но с передачей в сеть интернет.

В случае поручения обработки персональных данных третьему лицу, ему предъявляются требования принимать необходимые организационные, технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении персональных данных, в том числе: определение угроз безопасности персональных данных при их обработке в информационных системах; учёт машинных носителей персональных данных; обнаружение фактов несанкционированного доступа к персональным данным и принятием мер; контроль принимаемых мер по обеспечению безопасности персональных данных и уровня защищённости информационных систем персональных данных.

При передаче персональных данных на основе федерального закона условия передачи персональных данных устанавливаются соответствующим федеральным законом.

5.4. Обеспечение безопасности персональных данных Оператором достигается, в частности следующими мерами:

1) оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», соотношение указанного вреда и принимаемых защитных мер;

2) учет машинных носителей персональных данных;

3) назначение Ответственного за организацию обработки персональных данных;

4) ознакомление работников (служащих), осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, политикой Организации в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников (служащих);

5) издание политики Организации в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных;

6) восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

7) применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации (сертифицированные СЗИ);

8) контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных;

9) определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

10) установление правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных.

5.5. Базы персональных данных Оператора в полном объеме находятся в пределах территории Российской Федерации.

5.6. Сроки обработки персональных данных

Персональные данные субъектов, обрабатываемые Оператором, подлежат уничтожению либо обезличиванию в случае:

1) достижения целей обработки персональных данных или утраты необходимости в достижении этих целей;

2) прекращения деятельности Оператора.

5.7. Условия обработки персональных данных без использования средств автоматизации

При обработке персональных данных, осуществляемой без использования средств автоматизации, Оператор выполняет требования, установленные постановлением Правительства Российской Федерации от 15 сентября 2008 года

№ 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

6. **Регламент реагирования на запросы обращения субъектов персональных данных и их представителей**

При обращении, запросе в письменной или электронной форме субъекта персональных данных или его законного представителя, на доступ к своим персональным данным Оператор руководствуется требованиями статей 14, 18 и 20 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

Субъект или его законный представитель может воспользоваться формами запросов (приложения 1-3).

Доступ субъекта персональных данных или его законного представителя к своим персональным данным Оператор предоставляет только под контролем ответственного за организацию обработки персональных данных Оператора.

Обращение субъекта персональных данных или его законного представителя фиксируются в журнале учета обращений граждан (субъектов персональных данных) по вопросам обработки персональных данных.

Запрос в письменной или электронной форме субъекта персональных данных или его законного представителя фиксируются в журнале регистрации письменных запросов граждан на доступ к своим персональным данным.

Ответственный за организацию обработки персональных данных принимает решение о предоставлении доступа субъекта к персональным данным.

В случае, если данных предоставленных субъектом недостаточно для установления его личности или предоставление персональных данных нарушает конституционные права и свободы других лиц ответственный за организацию обработки персональных данных подготавливает мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий тридцати рабочих дней со дня обращения субъекта персональных данных или его законного представителя либо от даты получения запроса субъекта персональных данных или его законного представителя.

Для предоставления доступа субъекта персональных данных или его законного представителя к персональным данным субъекта ответственный за организацию обработки персональных данных привлекает работника (служащего) отраслевого (функционального), территориального органа, обрабатывающего персональные данные субъекта по согласованию с руководителем этого отраслевого (функционального), территориального органа.

Сведения о наличии персональных данных Оператор предоставляет субъекту персональных данных в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных. Контроль предоставления сведений субъекту или его

законному представителю осуществляет ответственный за организацию обработки персональных данных.

Сведения о наличии персональных данных предоставляются субъекту при ответе на запрос в течение тридцати дней от даты получения запроса субъекта персональных данных или его законного представителя.

7. **Регламент реагирования на запросы обращения уполномоченных органов**

В соответствии с частью 4 статьи 20 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» Оператор сообщает в уполномоченный орган по защите прав субъектов персональных данных по его запросу информацию, необходимую для осуществления деятельности указанного органа, в течение тридцати дней с даты получения такого запроса.

Сбор сведений для составления мотивированного ответа на запрос надзорных органов осуществляет ответственный за организацию обработки персональных данных при необходимости с привлечением работников (служащих) Оператора.

В течение установленного срока ответственный за организацию обработки персональных данных подготавливает и направляет в уполномоченный орган мотивированный ответ и другие необходимые документы.

Начальник управления информатизации
и связи администрации муниципального
образования городской округ
город-курорт Сочи Краснодарского края Н.Р.Лавриенко

Департамент муниципальной службы и кадровой политики

Приложение № 1
к Политике обработки персональных данных администрации муниципального образования городской округ город-курорт Сочи Краснодарского края

Форма запроса субъекта персональных данных, в случае выявления недостоверных персональных данных

Главе муниципального образования
городской округ город-курорт Сочи
Краснодарского края

от _____
(Ф.И.О., номер основного документа, удостоверяющего личность

_____
субъекта или его законного представителя, сведения о дате выдачи

_____
указанного документа и выдавшем органе,

_____
адрес, контактные данные)

З А П Р О С
на уточнение/блокирование/уничтожение персональных данных, в связи с выявлением недостоверных персональных данных

Прошу:

☐ уточнить

☐ заблокировать

☐ уничтожить

мои персональные данные, обрабатываемые в администрации муниципального образования городской округ город-курорт Сочи Краснодарского края, в связи с выявлением следующих недостоверных сведений:

_____
_____
_____
_____
_____
(перечислить)

_____ _____ _____
(дата) (подпись) (расшифровка)

Приложение № 2
к Политике обработки персональных данных администрации муниципального образования городской округ город-курорт Сочи Краснодарского края

Форма запроса субъекта персональных данных, в случае выявления недостоверных персональных данных

Главе муниципального образования
городской округ город-курорт Сочи
Краснодарского края

от _____
(Ф.И.О., номер основного документа, удостоверяющего личность

_____
субъекта или его законного представителя, сведения о дате выдачи

_____
указанного документа и выдавшем органе,

_____
адрес, контактные данные)

З А П Р О С
на прекращение обработки персональных данных

Прошу прекратить обработку моих персональных данных в связи с:

_____
_____
_____
_____
_____
_____
(перечислить)

_____ _____ _____
(дата) (подпись) (расшифровка)

Приложение № 3
к Политике обработки персональных данных администрации муниципального образования городской округ город-курорт Сочи Краснодарского края

Форма запроса субъекта персональных данных на предоставление доступа к своим персональным данным

Главе муниципального образования городской округ город-курорт Сочи Краснодарского края

от _____
(Ф.И.О., номер основного документа, удостоверяющего личность

_____
субъекта или его законного представителя, сведения о дате выдачи

_____
указанного документа и выдавшем органе,

_____
адрес, контактные данные)

З А П Р О С
на получение доступа к персональным данным

Прошу предоставить мне для ознакомления следующую информацию (в том числе документы), составляющую мои персональные данные:

_____
_____
_____
_____
_____
_____
(перечислить)

_____ _____ _____
(дата) (подпись) (расшифровка)

Приложение № 2
к распоряжению администрации муниципального образования городской округ город-курорт Сочи Краснодарского края
от 16.08.2021 № 300-р

ПРАВИЛА
обработки персональных данных в администрации муниципального образования городской округ город-курорт Сочи Краснодарского края

1. Общие положения

Настоящие правила обработки персональных данных в администрации муниципального образования городской округ город-курорт Сочи Краснодарского края (далее – Правила) разработаны для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных администрации муниципального образования городской округ город-курорт Сочи Краснодарского края, а также отраслевых (функциональных) и территориальных органов администрации муниципального образования городской округ город-курорт Сочи Краснодарского края (далее – администрация города Сочи), а также защиты прав и свобод граждан при обработке их персональных данных в администрации города Сочи, в том числе право на неприкосновенность частной жизни, личную и семейную тайну, а также разъяснение ответственности должностных лиц (служащих), имеющих доступ к персональным данным, за невыполнение требований норм и правил, регулирующих обработку и защиту персональных данных.

Настоящие Правила устанавливают порядок обработки персональных данных субъектов персональных данных в администрации города Сочи и направлены на выявление, предотвращение и профилактику нарушений законодательства Российской Федерации в сфере персональных данных.

Субъектами персональных данных в администрации города Сочи учреждении являются:

1) ближайшие родственники муниципальных служащих;

2) граждане;

3) контрагенты;

4) муниципальные служащие;

5) получатели муниципальных услуг (граждане, в том числе индивидуальные предприниматели);

6) уволенные (уволившиеся) муниципальные служащие.

Под обработкой персональных данных понимается любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Настоящие Правила определяют необходимый минимальный объём мер, соблюдение которых позволяет предотвратить утечку сведений, относящихся к персональным данным. При необходимости могут быть введены дополнительные меры, направленные на усиление защиты персональных данных.

Настоящие Правила разработаны в соответствии со следующими нормативно-правовыми актами (документами) Российской Федерации:

1) Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных от 28 января 1981 года с поправками, одобренными Комитетом министров Совета Европы 15 июня 1999 года, ратифицированная Федеральным законом Российской Федерации от 19 декабря 2005 года № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных» в рамках, определяемых данным Федеральным законом, заявлений;

2) Конституция Российской Федерации;

3) Гражданский кодекс Российской Федерации;

4) Кодекс об административных правонарушениях Российской Федерации;

5) Трудовой кодекс Российской Федерации;

6) Уголовный кодекс Российской Федерации;

7) Федеральный закон от 27 июля 2004 года № 79-ФЗ «О государственной гражданской службе Российской федерации»;

8) Федеральный закон от 2 марта 2007 года № 25-ФЗ «О муниципальной службе в Российской Федерации»;

9) Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ);

10) Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

11) Перечень сведений конфиденциального характера, утвержденный Указом Президента Российской Федерации от 6 марта 1997 года № 188;

12) Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утверждённое постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687;

13) Перечень 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, утверждённый постановлением Правительства Российской Федерации от 21 марта 2012 года № 211;

14) Требования к защите персональных данных при их обработке в информационных системах персональных данных, утвержденные постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119.

В соответствии с законодательством Российской Федерации об обработке

и защите персональных данных персональные данные субъектов являются конфиденциальной информацией.

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 те персональные данные, которые отвечают целям их обработки и не должны быть избыточными по отношению к заявленным целям.

При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных.

В случаях, предусмотренных действующим законодательством, сведения о доходах, об имуществе и обязательствах имущественного характера муниципального служащего, его супруги (супруга) и несовершеннолетних детей могут размещаться на официальном сайте администрации города Сочи или предоставляться региональным средствам массовой информации по их запросам для последующего опубликования.

Порядок регистрации, учёта, оформления, тиражирования, хранения, использования и уничтожения документов и других материальных носителей персональных данных определяют законодательство Российской Федерации об обработке и защите персональных данных, а также действующие нормативные правовые акты администрации города Сочи.

Администрация города Сочи является оператором персональных данных субъектов, указанных в настоящем документе. На основании соглашения (договора) администрация города Сочи может поручать обработку персональных данных третьим лицам с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта (далее – поручение администрации города Сочи). Лицо, осуществляющее обработку персональных данных по поручению администрации города Сочи, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом № 152-ФЗ. В поручении администрации города Сочи, должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона № 152-ФЗ.

Лицо, осуществляющее обработку персональных данных по поручению администрации города Сочи, не обязано получать согласие субъекта персональных данных на обработку его персональных данных.

В случаях, когда администрация города Сочи поручает обработку

персональных данных третьему лицу, ответственность перед субъектом персональных данных за действия указанного лица несет администрация города Сочи. Лицо, осуществляющее обработку персональных данных по поручению администрации города Сочи, несет ответственность перед администрацией города Сочи.

Администрация города Сочи, подведомственные учреждение и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

При передаче подведомственному учреждению муниципальных функций, исполнение которых связано с обработкой персональных данных субъектов персональных данных, контроль за исполнением требований по организации обработки и защите персональных данных в подведомственном учреждении возлагается на руководителя отраслевого (функционального) или территориального органа администрации города Сочи, чьи функции были переданы.

В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьёй 24 Конституции Российской Федерации, администрация города Сочи вправе получать и обрабатывать данные о частной жизни гражданских служащих и(или) работников администрации города Сочи только с их письменного согласия.

В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, сообщаемые субъектом персональных данных.

Администрация города Сочи не имеет права получать и обрабатывать персональные данные субъекта о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных законодательством Российской Федерации.

Настоящие Правила вступают в силу с момента их утверждения и действуют до замены их новыми Правилами обработки персональных данных.

Все изменения в Правила вносятся распоряжением администрации муниципального образования городской округ город-курорт Сочи Краснодарского края.

2. Цель и содержание обработки персональных данных

Целями обработки персональных данных в администрации города Сочи являются:

1) реализация функций исполнительно-распорядительного органа муниципального образования городской округ город-курорт Сочи Краснодарского края;

2) исполнение договора с субъектом;

3) реализация функций работодателя.

2.1. Цель «реализация функций исполнительно-распорядительного органа муниципального образования городской округ город-курорт Сочи Краснодарского края» достигается посредством обработки персональных данных следующих категорий для следующих субъектов:

1) получатели муниципальных услуг (граждане, в том числе индивидуальные предприниматели):

Специальные категории: национальная принадлежность.

Иные категории: фамилия, имя, отчество, год рождения, дата рождения, место рождения, адрес, паспортные данные, контактные сведения, гражданство, СНИЛС, ИНН, социальное положение, имущественное положение, ОГРНИП, семейное положение, дата, время, причина смерти, информация о трудовой деятельности, состав семьи, адрес электронной почты, данные доверенности.

Объем: менее чем 100 000 субъектов персональных данных.

2) граждане:

Иные категории: адрес, фамилия, имя, отчество, контактные сведения.

Объем: менее чем 100 000 субъектов персональных данных.

2.2. Цель «исполнение договора с субъектом» достигается посредством обработки персональных данных следующих категорий для следующих субъектов:

1) контрагенты:

Иные категории: контактные сведения, банковские реквизиты, адрес, ИНН, фамилия, имя, отчество, паспортные данные, сведения о доверенности, гражданство, ОГРНИП.

Объем: менее чем 100 000 субъектов персональных данных.

2.3. Цель «реализация функций работодателя» достигается посредством обработки персональных данных следующих категорий для следующих субъектов:

1) ближайшие родственники муниципальных служащих:

Иные категории: фамилия, имя, отчество, трудоспособность, дата рождения, сведения о доходах, имуществе и обязательствах имущественного характера, пребывание за границей, адрес, информация о трудовой деятельности, степень родства.

Объем: менее чем 100 000 субъектов персональных данных.

2) уволенные (уволившиеся) муниципальные служащие:

Специальные категории: судимость.

Иные категории: фамилия, имя, отчество, адрес, гражданство, семейное положение, степень родства, доходы, профессия, ИНН, банковские реквизиты, государственные награды, дата рождения, контактные сведения, состав семьи, имущественное положение, информация о трудовой деятельности, СНИЛС, фотография, прежние фамилия, имя, отчество, допуск к государственной тайне, сведения о доходах, имуществе и обязательствах имущественного характера, место рождения, паспортные данные, сведения о воинском учёте, образование, трудоспособность, звание, классный чин федеральной гражданской службы, дипломатический ранг, воинское или специальное звание, классный чин правоохранительной службы, классный чин гражданской службы субъекта

Российской Федерации, квалификационный разряд государственной службы, квалификационный разряд или классный чин муниципальной службы, пребывание за границей, данные загранпаспорта, результаты обязательных предварительных (при поступлении на работу) и периодических медицинских осмотров (обследований), а также обязательного психиатрического освидетельствования, наличие (отсутствие) заболевания препятствующего поступлению на государственную гражданскую службу Российской Федерации или её прохождению, подтверждённого заключением медицинского учреждения, сведения о повышении квалификации, ученая степень.

Объем: менее чем 100 000 субъектов персональных данных.

3) муниципальные служащие:

Специальные категории: судимость.

Иные категории: место рождения, паспортные данные, семейное положение, имущественное положение, информация о трудовой деятельности, СНИЛС, результаты обязательных предварительных (при поступлении на работу) и периодических медицинских осмотров (обследований), а также обязательного психиатрического освидетельствования, наличие (отсутствие) заболевания препятствующего поступлению на государственную гражданскую службу Российской Федерации или её прохождению, подтверждённого заключением медицинского учреждения, сведения о доходах, имуществе и обязательствах имущественного характера, допуск к государственной тайне, фамилия, имя, отчество, адрес, сведения о воинском учёте, состав семьи, доходы, профессия, трудоспособность, банковские реквизиты, прежние фамилия, имя, отчество, дата рождения, контактные сведения, гражданство, степень родства, образование, ИНН, пребывание за границей, данные загранпаспорта, государственные награды, звание, классный чин федеральной гражданской службы, дипломатический ранг, воинское или специальное звание, классный чин правоохранительной службы, классный чин гражданской службы субъекта Российской Федерации, квалификационный разряд государственной службы, квалификационный разряд или классный чин муниципальной службы, сведения о повышении квалификации, ученая степень, фотография.

Объем: менее чем 100 000 субъектов персональных данных.

3. Правила обработки персональных данных

Все персональные данные субъектов администрация города Сочи получает от них самих либо от их законных представителей.

Персональные данные ближайших родственников работников (служащих), необходимые для ведения кадрового учёта, администрация города Сочи получает от самих работников (служащих).

Обработка персональных данных осуществляется на законной и справедливой основе, а также с соблюдением принципов и правил, предусмотренных Федеральным законом № 152-ФЗ, на основании согласия субъекта персональных данных на обработку его персональных данных, кроме случаев, предусмотренных Федеральным законом № 152-ФЗ. Форма согласия утверждается отдельным распоряжением. Допускается совмещение формы

согласия субъекта с типовыми формами документов, содержащих персональные данные субъекта (например: анкеты, бланки).

Субъект персональных данных принимает решение о предоставлении своих персональных данных и даёт согласие на их обработку свободно, своей волей и в своём интересе.

Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. В случае отзыва субъектом персональных данных согласия на обработку персональных данных администрация города Сочи вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона № 152-ФЗ.

Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются администрацией города Сочи.

В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает законный представитель субъекта персональных данных.

В случае смерти субъекта персональных данных согласие на обработку его персональных данных дают наследники субъекта персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни.

Администрация города Сочи оставляет за собой право не осуществлять свои функции в отношении субъекта персональных данных в случае предоставления неполных или недостоверных персональных данных, а также в случае отказа дать письменное согласие на обработку персональных данных.

При установлении договорных отношений с субъектом персональных данных получение письменного согласия на обработку его персональных данных не требуется.

Получение персональных данных субъекта у третьих лиц возможно только при предварительном уведомлении субъекта и с его письменного согласия. Форма согласия утверждается отдельным распоряжением. Допускается совмещение формы согласия субъекта с типовыми формами документов, содержащих персональные данные субъекта (например, анкеты, бланки).

Персональные данные могут быть получены администрацией города Сочи от лица, не являющегося субъектом персональных данных, при условии предоставления администрации города Сочи подтверждения наличия оснований, указанных в Федеральном законе № 152-ФЗ.

Персональные данные субъектов администрации города Сочи обрабатываются в отраслевых (функциональных) и территориальных органах в соответствии с исполняемыми ими функциями и обязанностями.

Доступ к персональным данным, обрабатываемым без использования средств автоматизации, осуществляется в соответствии с утвержденным списком допущенных лиц, утверждённым в порядке, определяемом в администрации города Сочи. В отраслевых (функциональных) и территориальных органах, обладающих правом юридического лица, список допущенных лиц утверждается приказом или распоряжением руководителя органа.

Доступ к персональным данным, обрабатываемым в информационных системах персональных данных, осуществляется в соответствии с утвержденным списком допущенных лиц, утверждённым в порядке, определяемом в администрации города Сочи. В отраслевых (функциональных) и территориальных органах, обладающих правом юридического лица, список допущенных лиц утверждается приказом или распоряжением руководителя органа.

Уполномоченные лица, допущенные к персональным данным субъектов администрации города Сочи, имеют право получать только те персональные данные субъекта, которые необходимы для выполнения конкретных функций, в соответствии с должностными инструкциями (обязанностями) указанных лиц.

Обработка персональных данных, осуществляемая без использования средств автоматизации, должна выполняться в соответствии с требованиями Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утверждённого Постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687.

Персональные данные при такой их обработке, должны обособляться от иной информации, в частности путём фиксации их на отдельных материальных носителях персональных данных, в специальных разделах или на полях форм (бланков).

Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки.

Хранение материальных носителей персональных данных осуществляется в специально оборудованных шкафах и сейфах. Места хранения определяются распоряжением об утверждении мест хранения материальных носителей персональных данных администрации города Сочи. В отраслевых (функциональных) и территориальных органах, обладающих правом юридического лица, места хранения определяются приказом или распоряжением руководителя органа.

Персональные данные могут подлежать блокированию, уточнению, уничтожению либо обезличиванию в одном из следующих случаев:

1) выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его законного представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных;

2) выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу

уполномоченного органа по защите прав субъектов персональных данных;

3) выявления неправомерной обработки персональных данных, осуществляемой администрацией города Сочи, или лицом, действующим по поручению администрации города Сочи и невозможности обеспечить правомерную обработку персональных данных;

4) достижения целей обработки или в случае утраты необходимости в их достижении;

5) отзыва согласия субъекта персональных данных на обработку его персональных данных;

6) представления субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные являются неполными, неточными, неактуальными (устаревшими), незаконно полученными или не являются необходимыми для заявленной цели обработки.

В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его законного представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных администрация города Сочи осуществляет блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению администрации города Сочи) с момента такого обращения или получения указанного запроса на период проверки.

В случае выявления неточных персональных данных при обращении субъекта персональных данных или его законного представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных администрация города Сочи осуществляет блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению администрации города Сочи) 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 администрация города Сочи на основании сведений, представленных субъектом персональных данных или его законным представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов уточняет персональные данные либо обеспечивает их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению администрации города Сочи) в течение 7 рабочих дней со дня представления таких сведений и снимает блокирование персональных данных.

В случае выявления неправомерной обработки персональных данных, осуществляемой администрацией города Сочи, или лицом, действующим по поручению администрации города Сочи, администрация города Сочи в срок, не

превышающий 3-х рабочих дней с даты этого выявления, осуществляет прекращение неправомерной обработки персональных данных или обеспечивает прекращение неправомерной обработки персональных данных лицом, действующим по поручению администрации города Сочи.

В случае, если обеспечить правомерность обработки персональных данных невозможно, администрация города Сочи в срок, не превышающий 10 рабочих дней с даты выявления неправомерной обработки персональных данных, осуществляет уничтожение таких персональных данных или обеспечивает их уничтожение. Решение о неправомерности обработки персональных данных и необходимости уничтожения персональных данных принимает ответственный за организацию обработки персональных данных, который доводит соответствующую информацию до руководства. Об устранении допущенных нарушений или об уничтожении персональных данных администрация города Сочи уведомляет субъекта персональных данных или его законного представителя, а в случае, если обращение субъекта персональных данных или его законного представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

В случае достижения цели обработки персональных данных администрация города Сочи прекращает обработку персональных данных или обеспечивает ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению администрации города Сочи) и уничтожает персональные данные или обеспечивает их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению администрации города Сочи) в срок, не превышающий 30 дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если администрация города Сочи не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом № 152-ФЗ или другими федеральными законами.

В случае отзыва субъектом персональных данных согласия на обработку его персональных данных администрация города Сочи прекращает их обработку или обеспечивает прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению администрации города Сочи) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожает персональные данные или обеспечивает их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению администрации города Сочи) в срок, не превышающий 30 дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому

является субъект персональных данных, иным соглашением между администрацией города Сочи и субъектом персональных данных либо если администрация города Сочи не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом № 152-ФЗ или другими федеральными законами.

В срок, не превышающий 7 рабочих дней со дня предоставления субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, администрация города Сочи вносит в них необходимые изменения.

В срок, не превышающий 7 рабочих дней со дня представления субъектом персональных данных или его законным представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, администрация города Сочи уничтожает такие персональные данные. При этом администрация города Сочи уведомляет субъекта персональных данных или его законного представителя о внесенных изменениях и предпринятых мерах и принимает разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

В случае отсутствия возможности уничтожения персональных данных в течение срока, указанные выше по тексту, администрация города Сочи осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению администрации города Сочи) и обеспечивает уничтожение персональных данных в срок не более чем 6 месяцев, если иной срок не установлен федеральными законами.

Уничтожение персональных данных осуществляет комиссия в составе руководителя и работников (служащих) отраслевого (функционального), территориального органа, обрабатывавшего персональные данные субъекта и установившего необходимость уничтожения персональных данных под контролем руководителя этого отраслевого (функционального), территориального органа.

Способ уничтожения материальных носителей персональных данных определяется комиссией. Допускается применение следующих способов:

1) сжигание;

2) шредирование (измельчение);

3) передача на специализированные полигоны (свалки);

4) химическая обработка.

При этом составляется «Акт уничтожения документов администрации города Сочи, содержащих персональные данные субъекта». Форма акта утверждается отдельным распоряжением.

При необходимости уничтожения большого количества материальных носителей или применения специальных способов уничтожения допускается привлечение специализированных организаций. При этом к акту уничтожения

необходимо приложить накладную на передачу материальных носителей персональных данных, подлежащих уничтожению, в специализированную организацию.

Уничтожение полей баз данных администрации города Сочи, содержащих персональные данные субъекта, выполняется по заявке руководителя отраслевого (функционального), территориального органа, обрабатывавшего персональные данные субъекта и установившего необходимость их уничтожения.

Уничтожение осуществляет комиссия, в состав которой входят лица, ответственные за администрирование информационных систем, которым принадлежат базы данных, работники (служащие) отраслевого (функционального) и/или территориального органа, обрабатывавшего персональные данные субъекта и установившего необходимость их уничтожения.

Уничтожение достигается путём затирания информации на носителях информации (в том числе и резервных копиях) или путём механического нарушения целостности носителя информации, не позволяющего произвести считывание или восстановление персональных данных. При этом составляется «Акт уничтожения полей баз данных администрации города Сочи, содержащих персональные данные субъекта». Форма акта утверждается отдельным распоряжением.

Уничтожение архивов электронных документов и протоколов электронного взаимодействия может не производиться, если ведение и сохранность их в течение определённого срока предусмотрены соответствующими нормативными и (или) договорными документами.

При невозможности осуществления уничтожения информации в базах данных или на носителях, допускается проведение обезличивания путём перезаписи полей баз данных. Перезапись должна быть осуществлена таким образом, чтобы дальнейшая идентификация субъекта персональных данных была не возможна.

Контроль выполнения процедур уничтожения персональных данных осуществляет ответственный за организацию обработки персональных данных в администрации города Сочи.

Особенности обработки специальных категорий персональных данных, а также сведения, характеризующие физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные), установлены соответственно статьями 10 и 11 Федерального закона № 152-ФЗ.

Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается, за исключением случаев, предусмотренных частью 2 статьи 10 Федерального закона № 152-ФЗ. Обработка персональных данных о судимости может осуществляться муниципальными органами в пределах полномочий, предоставленных им в соответствии с законодательством Российской

Федерации, а также иными лицами в случаях и в порядке, которые определяются в соответствии с федеральными законами.

Обработка биометрических персональных данных может осуществляться только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных частью 2 статьи 11 Федерального закона № 152-ФЗ.

Форма согласия утверждается отдельным распоряжением. Допускается совмещение формы согласия субъекта с типовыми формами документов, содержащих персональные данные субъекта (например: анкеты, бланки).

Решение, порождающее юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия в письменной форме субъекта персональных данных.

Работники (служащие) администрации города Сочи должны быть ознакомлены под роспись с требованиями законодательства Российской Федерации, касающимися обработки персональных данных, настоящими Правилами и другими документами администрации города Сочи, устанавливающими порядок обработки персональных данных субъектов, а также права и обязанности в этой области.

4. Передача персональных данных третьим лицам

При обработке персональных данных субъекта муниципальные служащие, допущенные к обработке персональных данных, должны соблюдать следующие требования:

1) не сообщать персональные данные субъекта третьей стороне без письменного согласия субъекта. Форма согласия утверждается отдельным распоряжением. Допускается совмещение формы согласия субъекта с типовыми формами документов, содержащими персональные данные субъекта, при условии соблюдения требований статьи 9 Федерального закона № 152;

2) предупреждать лиц, получающих персональные данные субъекта, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные субъекта, обязаны соблюдать режим конфиденциальности в отношении этих данных.

При необходимости трансграничной передачи персональных данных на территорию иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, администрация города Сочи запрашивает согласие субъекта в письменной форме. Форма согласия утверждается отдельным распоряжением. Допускается совмещение формы согласия субъекта с типовой формой документов, содержащих персональные данные субъекта (например: анкеты). Допускается совмещение формы согласия субъекта с другими формами согласий.

5. Права субъектов персональных данных

В целях обеспечения своих законных интересов субъекты персональных данных или его представители имеют право:

1) получать полную информацию о своих персональных данных и обработке этих данных (в том числе автоматизированной);

2) осуществлять свободный бесплатный доступ к своим персональным данным, включая право получать копии любой записи, содержащей персональные данные субъекта, за исключением случаев, предусмотренных Федеральным законом № 152-ФЗ;

3) требовать уточнение его персональных данных, их блокирование или уничтожение в случаях, 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. Субъект персональных данных при отказе администрации города Сочи исключить или исправить, блокировать или уничтожить его персональные данные имеет право заявить в письменной форме о своем несогласии, обосновав соответствующим образом такое несогласие. Персональные данные оценочного характера субъект персональных данных имеет право дополнить заявлением, выражающим его собственную точку зрения;

4) требовать от администрации города Сочи уведомления всех лиц, которым ранее были сообщены неверные или неполные, устаревшие, неточные, незаконно полученные или не являющиеся необходимыми для заявленной цели обработки персональные данные субъекта, обо всех произведённых в них изменениях или исключениях из них, в том числе блокирование или уничтожение этих данных третьими лицами;

5) обжаловать в суде или в уполномоченном органе по защите прав субъектов персональных данных любые неправомерные действия или бездействие администрации города Сочи при обработке и защите персональных данных субъекта персональных данных, если субъект персональных данных считает, что администрация города Сочи осуществляет обработку его персональных данных с нарушением требований Федерального закона № 152-ФЗ или иным образом нарушает его права и свободы.

В случае, если обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно в администрацию города Сочи или направить ему повторный запрос в целях получения сведений, и ознакомления с персональными данными не ранее, чем через 30 дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

Субъект персональных данных вправе обратиться повторно до истечения 30 дневного срока в случае, если сведения и (или) обрабатываемые

персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос должен содержать обоснование направления повторного запроса.

Администрация города Сочи вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренные частями 4 и 5 Федерального закона № 152-ФЗ. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на администрации города Сочи.

Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами Российской Федерации.

6. Порядок действий в случае запросов надзорных органов

В соответствии с частью 4 статьи 20 Федерального закона № 152 администрация города Сочи сообщает в уполномоченный орган по защите прав субъектов персональных данных по его запросу информацию, необходимую для осуществления деятельности указанного органа, в течение 30 дней с даты получения такого запроса.

Сбор сведений для составления мотивированного ответа на запрос надзорных органов осуществляет ответственный за организацию обработки персональных данных в администрации города Сочи при необходимости с привлечением работников (служащих) администрации города Сочи.

В течение установленного законодательством срока ответственный за организацию обработки персональных данных в администрации города Сочи подготавливает и направляет в уполномоченный орган мотивированный ответ и другие необходимые документы.

7. Защита персональных данных субъекта

Защиту персональных данных субъектов от неправомерного их использования или утраты администрация города Сочи, а также подведомственные учреждения обеспечивают за счёт собственных средств в порядке, установленном законодательством Российской Федерации.

При обработке персональных данных должны быть приняты необходимые организационные и технические меры по обеспечению их конфиденциальности.

Технические меры защиты персональных данных при их обработке техническими средствами устанавливаются в соответствии с:

1) руководящим документом Федеральной службы по техническому и экспортному контролю России (далее – ФСТЭК России) – «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденным приказом ФСТЭК России от 18 февраля 2013 года № 21;

2) руководящим документом ФСТЭК России – «Об утверждении требований о защите информации, не составляющей государственную тайну,

содержащейся в государственных информационных системах», утвержденным приказом ФСТЭК России от 11 февраля 2013 года № 17;

3) специальными требованиями и рекомендациями по технической защите конфиденциальной информации (СТР-К), утвержденными приказом Гостехкомиссии России от 30 августа 2002 года № 282;

4) внутренними документами администрации города Сочи, действующими в сфере обеспечения информационной безопасности.

Защита персональных данных предусматривает ограничение к ним доступа.

Ответственные за организацию обработки персональных данных, администрирование средств и механизмов защиты, техническое обслуживание информационных систем персональных данных назначаются распоряжением главы муниципального образования городской округ город-курорт Сочи Краснодарского края, а также приказами руководителей отраслевых (функциональных) и территориальных органов администрации города Сочи, обладающих правом юридического лица.

Руководитель отраслевого (функционального), территориального органа администрации города Сочи, осуществляющего обработку персональных данных:

1) несёт ответственность за организацию защиты персональных данных в отраслевом (функциональном), территориальном органе администрации города Сочи;

2) закрепляет за работниками, уполномоченными обрабатывать персональные данные, конкретные материальные носители, на которых допускается хранение персональных данных в случае, если такие носители необходимы для выполнения возложенных на работников функций и задач;

3) организовывает изучение подчинёнными работниками, в чьи обязанности входит обработка персональных данных, нормативных правовых актов по защите персональных данных и требует их неукоснительного исполнения;

4) обеспечивает режим конфиденциальности в отношении персональных данных, обрабатываемых в отраслевом (функциональном), территориальном органе администрации города Сочи;

5) контролирует порядок доступа к персональным данным в соответствии с функциональными обязанностями работников отраслевого (функционального), территориального органа администрации города Сочи.

Работники, допущенные к персональным данным дают письменное обязательство о неразглашении таких данных.

8. Обязанности лиц, допущенных к обработке персональных данных

Работники, допущенные к работе с персональными данными, обязаны:

1) знать законодательство Российской Федерации в области обработки и защиты персональных данных, нормативные документы администрации города Сочи по обработке и защите персональных данных;

2) сохранять конфиденциальность персональных данных;

3) обеспечивать сохранность закреплённых за ними носителей персональных данных;

4) контролировать срок истечения действия согласий на обработку персональных данных и, при необходимости дальнейшей обработки персональных данных, обеспечивать своевременное получение новых согласий или прекращение обработки персональных данных;

5) докладывать своему непосредственному руководителю отраслевого (функционального), территориального органа администрации города Сочи обо всех фактах и попытках несанкционированного доступа к персональным данным и других нарушениях.

Ответственный за организацию обработки персональных данных администрации города Сочи организует проведение инструктажа и ознакомление работников администрации города Сочи, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику администрации города Сочи в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных.

9. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных субъектов

Лица, виновные в нарушении норм, регулирующих получение, обработку, передачу и защиту персональных данных субъекта, привлекаются к материальной, административной, уголовной и гражданско-правовой ответственности на основании судебного решения, а также к дисциплинарной ответственности в соответствии с действующим законодательством Российской Федерации.

К данным лицам могут быть применены следующие дисциплинарные взыскания:

1) замечание;
2) выговор;
3) предупреждение о неполном должностном соответствии;
4) освобождение или отстранение от занимаемой должности;
5) увольнение с муниципальной службы.

Начальник управления информатизации
и связи администрации муниципального
образования городской округ
город-курорт Сочи Краснодарского края Н.Р.Лавриенко

Приложение № 3
к распоряжению администрации
муниципального образования городской
округ город-курорт Сочи
Краснодарского края
от 16.08.2021 № 300-р

ПЕРЕЧЕНЬ
защищаемой информации в администрации города Сочи

№ п/п	Наименование сведений
1	Персональные данные (ПДн) муниципальных служащих, в т.ч. бывших и будущих (бухгалтерия, система учёта кадров, в т.ч. кадрового резерва и ветеранов, награжденных)
2	ПДн, используемые органом местного самоуправления при реализации своих полномочий – оказание государственных и муниципальных услуг, исполнении муниципальных функций
3	Проекты нормативных правовых и распорядительных актов, касающиеся субъектов экономической деятельности, общественных объединений и отдельных граждан
4	Оперативная информация о финансовом, хозяйственном, правовом состоянии администрации города Сочи – исполнительно-распорядительном органе муниципального образования городской округ город-курорт Сочи Краснодарского края
5	Неопубликованная конкурсная документация для проведения конкурсов по: приобретению товаров, выполнению работ, оказанию услуг; заключению договоров аренды; приобретению или предоставлению прав управлению имуществом; предоставления прав по распоряжению природными или иными ресурсами.
6	Информация, полученная от других органов государственной власти и местного самоуправления, бюджетных, коммерческих организаций, объединений граждан и отдельных граждан во исполнение возложенных на органы местного самоуправления (муниципальных) функций либо для оказания ими государственных (муниципальных) услуг
7	Сведения, раскрывающие систему защиты информации: логины, пароли, конфигурационные настройки сетевого оборудования и серверов, применяемые средства защиты информации, техническая документация защищаемых (аттестованных) автоматизированных систем, система нормативных и методических документов по защите информации и т.п.
8.	Требования по обеспечению сохранения информации для служебного пользования при выполнении работ в организации.
9.	Порядок передачи служебной информации ограниченного распространения другим организациям.

Начальник управления информатизации
и связи администрации муниципального
образования городской округ
город-курорт Сочи Краснодарского края Н.Р.Лавриенко

Приложение № 4
к распоряжению администрации
муниципального образования городской
округ город-курорт Сочи
Краснодарского края
от 16.08.2021 № 300-р

ИНСТРУКЦИЯ
по модификации и техническому обслуживанию программного обеспечения и аппаратных средств информационных систем администрации муниципального образования городской округ город-курорт Сочи Краснодарского края

1. Порядок внесения изменений в программное обеспечение

Изменения в состав программных средств информационных систем администрации муниципального образования городской округ город-курорт Сочи Краснодарского края, а также отраслевых (функциональных) и территориальных органов администрации муниципального образования городской округ город-курорт Сочи Краснодарского края (далее – ИС) могут вноситься путем инсталляции программного обеспечения (далее – ПО) с лицензионных дистрибутивов официально приобретаемого ПО либо ПО, полученного из официальных источников свободно распространяемого ПО. Устанавливаемое ПО должно иметь необходимую эксплуатационную документацию.

При необходимости внесения изменений в программную среду заявка подается через портал технической поддержки администрации муниципального образования городской округ город-курорт Сочи Краснодарского края sd.sochiadm.ru. Ответственность за обоснование необходимости внесения изменений в программную среду и использование нового ПО несет должностное лицо, подающее заявку (далее – пользователь).

Перед установкой нового ПО, пользователь совместно с представителем техподдержки производят антивирусный контроль дистрибутива.

В случае обнаружения не декларированных (не описанных в документации) возможностей ПО, пользователь немедленно докладывают начальнику своего подразделения и администратору информационной безопасности. Дальнейшее использование ПО до получения специальных указаний прекращается.

Пользователи, в части их касающейся, обязаны знать документацию на ПО и уметь правильно его эксплуатировать.

2. Порядок технического обслуживания и ремонта технических средств

2.1. Техническое обслуживание и ремонтные работы на технических средствах ИС должны осуществляться только уполномоченными работниками, назначенными ответственными за их обслуживание (сопровождение). Их вызов осуществляется работниками подразделения, эксплуатирующего ИС, при возникновении нештатных ситуаций.

К нештатным ситуациям относятся:

– выход из строя или неустойчивое функционирование АРМ, серверов или периферийных устройств (например, дисковода, принтера) ИС;

– выход из строя системы электроснабжения ИС.

Техническое обслуживание и регламентные работы могут проводиться в плановом порядке.

Ответственность за соблюдение требований по обеспечению безопасности информации при проведении технического обслуживания и ремонтных работ возлагается на отдел технического сопровождения систем информационной безопасности МКУ «Электронный Сочи».

Уполномоченные работники допускаются к ИС для разбора нештатных ситуаций при обнаружении сбоев в работе только для тестирования АРМ и серверов с использованием установленных в ИС тестовых средств.

При изъятии АРМ или серверов их передача на склад, в ремонт или в другое подразделение для решения иных задач осуществляется только после того, как работник МКУ «Электронный Сочи» снимет с АРМ или серверов жесткие диски и предпримет необходимые меры для затирания защищаемой информации, которая хранилась на дисках компьютера.

Начальник управления информатизации
и связи администрации муниципального
образования городской округ
город-курорт Сочи Краснодарского края Н.Р.Лавриенко

Департамент муниципальной службы и кадровой политики

Приложение № 5
к распоряжению администрации
муниципального образования городской
округ город-курорт Сочи
Краснодарского края
от 16.08.2021 № 300-р

ИНСТРУКЦИЯ
пользователя информационных систем администрации муниципального образования городской округ город-курорт Сочи Краснодарского края

1. Общие сведения

Настоящая инструкция пользователя информационных систем администрации муниципального образования городской округ город-курорт Сочи Краснодарского края (далее – Инструкция) определяет общие права и обязанности пользователей, допущенных к обработке защищаемой информации на средствах вычислительной техники в информационных системах администрации муниципального образования городской округ город-курорт Сочи Краснодарского края, а также отраслевых (функциональных) и территориальных органов администрации муниципального образования городской округ город курорт Сочи Краснодарского края.

Настоящая инструкция разработана на основании:

– Постановления Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– Методического документа от 11 февраля 2014 года «Меры защиты информации в государственных информационных системах».

Настоящая Инструкция предназначена для руководителей отраслевых (функциональных) и территориальных органов администрации муниципального образования городской округ город курорт Сочи Краснодарского края, администратора информационной безопасности (далее – администратор ИБ), администратора информационных систем (далее – администратор ИС) и пользователей, осуществляющих обработку защищаемой информации в информационных системах.

2. Общие права и обязанности пользователей при работе в информационных системах

Каждый пользователь информационных систем, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным информационных систем, несет

персональную ответственность за свои действия и имеет право доступа к информационных систем в соответствии с матрицей доступа, а также **обязан**:

– строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами информационных систем;

– знать и строго выполнять правила работы со средствами защиты информации, установленными в информационных системах;

– хранить в тайне свои пароли. Выполнять требования «Политики парольной защиты в информационных системах администрации муниципального образования городской округ город-курорт Сочи Краснодарского края»;

– хранить в тайне информацию, ставшую ему известной во время работы или иным путем, и пресекать действия других лиц, которые могут привести к разглашению защищаемой информации;

– передавать для хранения установленным порядком свои реквизиты разграничения доступа только руководителю отраслевого (функционального), территориального органа или ответственному за информационную безопасность;

– выполнять требования «Правил организации антивирусной защиты в информационных системах администрации муниципального образования городской округ город курорт Сочи Краснодарского края» в части, касающейся действий пользователей;

– немедленно сообщать администратору ИБ и ставить в известность руководителя отраслевого (функционального), территориального органа о случаях утери личных реквизитов доступа, утери носителя информации или при подозрении компрометации личных паролей, а также при обнаружении:

1) нарушений целостности пломб (наклеек) на аппаратных средствах информационных систем или иных фактов совершения в его отсутствие попыток несанкционированного доступа (далее – НСД) к техническим средствам информационных систем;

2) несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств информационных систем;

3) отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию информационных систем, выхода из строя или неустойчивого функционирования узлов информационных систем или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения;

4) некорректного функционирования установленных технических средств защиты информации;

5) непредусмотренных отводов кабелей и подключенных устройств;

6) присутствовать при работах по внесению изменений в аппаратно-программную конфигурацию закрепленного за ним автоматизированного рабочего места (далее – АРМ);

7) контролировать вывод информации на съемные носители информации. Пометка на носителе должна быть не ниже пометки записываемой информации.

Пользователям категорически запрещается:

– использовать компоненты программного и аппаратного обеспечения информационных систем в неслужебных целях;

– самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств информационных систем или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные техническим паспортом информационных систем (в том числе отключать (блокировать) СЗИ);

– передавать кому бы то ни было, устно или письменно, информацию, а также личные ключи и атрибуты доступа к ресурсам ИС;

– подключать к АРМ и информационным системам личные внешние носители и мобильные устройства;

– подключать личные АРМ, в том числе ноутбуки, к локально-вычислительной сети администрации муниципального образования городской округ город-курорт Сочи Краснодарского края;

– осуществлять обработку персональных данных и иной информации ограниченного доступа в присутствии посторонних (не допущенных к данной информации) лиц;

– допускать к работе на закрепленном за пользователем АРМ лиц, не допущенных к обработке защищаемой информации;

– записывать и хранить защищаемую информацию (содержащую сведения ограниченного распространения) на неучтенных съемных носителях информации;

– оставлять включенным без присмотра АРМ, не активизировав средства защиты от несанкционированного доступа;

– оставлять без личного присмотра на рабочем месте или где бы то ни было свои персональные реквизиты доступа, машинные носители и распечатки, содержащие защищаемую информацию (сведения ограниченного распространения);

– умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации. Об обнаружении такого рода ошибок ставить в известность администратора ИБ и руководителя отраслевого (функционального), территориального органа.

3. Действия пользователей до идентификации и аутентификации в системе

Пользователям до идентификации и аутентификации **разрешается**:

– производить включение, выключение, перезагрузку автоматизированных рабочих мест;

– предъявлять личный идентификатор и вводить пароль для авторизации в системе.

Пользователям до идентификации и аутентификации **запрещается**:

– входить в настройки базовой системы ввода-вывода технических средств и систем;

– осуществлять загрузку нештатных операционных систем со сторонних носителей информации.

Начальник управления информатизации
и связи администрации муниципального
образования городской округ
город-курорт Сочи Краснодарского края Н.Р.Лавриенко

Департамент муниципальной службы и кадровой политики

Приложение № 6
к распоряжению администрации
муниципального образования городской
округ город-курорт Сочи
Краснодарского края
от 16.08.2021 № 300-р

ПОЛИТИКА
резервного копирования и восстановления работоспособности технических средств и программного обеспечения, баз данных, средств и систем защиты информации в информационных системах администрации муниципального образования городской округ город-курорт Сочи Краснодарского края, а также в отраслевых (функциональных) и территориальных органах администрации муниципального образования городской округ город-курорт Сочи Краснодарского края

1. **Общие положения**

1.1. Настоящая политика разработана в соответствии с требованиями:

– Приказа Федеральной службы по техническому и экспортному контролю России от 11 февраля 2013 года № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

– Методического документа от 11 февраля 2014 года «Меры защиты информации в государственных информационных системах».

1.2. Настоящая политика определяет правила и объёмы резервирования, а также порядок восстановления работоспособности информационных ресурсов в информационных системах администрации муниципального образования городской округ город-курорт Сочи Краснодарского края, а также в отраслевых (функциональных) и территориальных органах администрации муниципального образования городской округ город-курорт Сочи Краснодарского края (далее – Политика).

1.3. Носители информации, используемые для резервирования информации ограниченного доступа в информационных системах администрации муниципального образования городской округ город-курорт Сочи Краснодарского края, а также в отраслевых (функциональных) и территориальных органах администрации муниципального образования городской округ город-курорт Сочи Краснодарского края, в том числе и персональных данных, подлежат защите в той же степени, что и резервируемая конфиденциальная информация.

1.4. Контроль за исполнением настоящей политики осуществляют ответственный за техническое обслуживание информационных систем и ответственный за обеспечение безопасности информационных систем администрации муниципального образования городской округ город-курорт Сочи Краснодарского края.

2. Назначение и область действия

2.1. Настоящая Политика предназначена для ответственного за техническое обслуживание информационных систем администрации муниципального образования городской округ город-курорт Сочи Краснодарского края (далее – администратор ИС), а также муниципальных служащих, участвующих в обработке информации в информационных системах администрации муниципального образования городской округ город-курорт Сочи Краснодарского края (далее – пользователи).

2.2. Настоящая Политика описывает действия администратора ИС и пользователей по обеспечению резервного копирования и восстановления информации, обрабатываемой в информационных системах администрации муниципального образования городской округ город-курорт Сочи Краснодарского края.

3. Информационные ресурсы, подлежащие резервированию

3.1. Резервному копированию подлежат все информационные ресурсы, содержащие информацию ограниченного доступа:

– файлы баз данных;

– электронные документы;

– файлы сообщений электронной почты;

– отсканированные и хранящиеся в информационных системах изображения (скан копии) документов;

– иная информация в информационных системах.

3.2. Резервному копированию могут так же подвергаться системное и прикладное программное обеспечение информационных систем.

3.3. Резервному копированию в обязательном порядке должны подвергаться программные компоненты средств защиты информации и настройки средств защиты информации в информационных системах.

4. Порядок резервирования

4.1. Резервирование информационных ресурсов информационных систем выполняется администратором ИС.

4.2. Определяется 2 вида резервирования информации ограниченного доступа:

– полное резервирование – резервное копирование всей информации, хранящейся в информационных системах;

– неполное резервирование информации – резервное копирование части информации, хранящейся в информационных системах.

Целью неполного резервирования является сохранение изменений в информационных системах с момента полного резервирования.

4.3. Периодичность проведения работ по резервированию определяется ответственным за организацию обработки персональных данных с учётом специфики работы информационных систем, но не менее 1 раза в месяц для полного резервирования и 1 раза в неделю для неполного резервирования.

4.4. В случаях, когда информация хранится на автоматизированных рабочих местах пользователей, ответственность за проведение неполного резервирования возлагается на пользователей информационных систем.

4.5. Администратор ИС использует средства резервного копирования информационных систем для резервирования информации на выделенный серверный сегмент системы хранения данных. Резервное копирование с использованием незащищённых каналов связи общего пользования не допустимо.

4.6. Администратор ИС не имеет права ознакомления с резервируемыми персональными данными. Факт ознакомления администратора ИС с резервируемой информацией может быть расценён как превышение служебных полномочий в соответствии с Трудовым Кодексом Российской Федерации и Кодексом об Административных Правонарушениях Российской Федерации.

4.7. При резервировании информации не допускается хранение на одном носителе резервных копий, извлечённых из различных информационных систем. Для осуществления резервирования различных информационных систем, для каждой из них должен быть предусмотрен отдельный носитель информации.

4.8. В случае удаления информации из информационной системы должна быть так же удалена резервная копия этой информации.

4.9. Резервное копирование программных компонентов средств защиты информации и их настроек должно осуществляться путем ведения двух копий программных компонентов средств защиты информации и (или) настроек СЗИ, периодического обновления СЗИ и контроля работоспособности.

5. Порядок хранения резервных копий

5.1. Хранение резервных копий должно исключать любой несанкционированный доступ посторонних лиц к носителям информации.

5.2. Хранение носителей резервных копий необходимо осуществлять в сейфах, несгораемых шкафах, металлических шкафах с устройством опечатывания. Доступ к местам хранения носителей резервных копий должен быть предоставлен только для ответственных лиц за обработку и защиту персональных данных.

5.3. На носителе информации, содержащем резервные копии, не должна храниться посторонняя информация.

5.4. Должно быть обеспечено одновременное хранение не менее двух носителей информации, хранящих полную резервную копию информационных систем.

6. Порядок восстановления информации после сбоя

6.1. В случае сбоя в работе информационных систем, восстановление информации из резервных копий осуществляет администратор ИС.

6.2. Временной норматив по восстановлению информации устанавливается ответственным за обработку и защиту персональных данных с учётом специфики работы информационных систем.

Начальник управления информатизации и связи администрации муниципального образования городской округ город-курорт Сочи Краснодарского края Н.Р.Лавриенко

Приложение № 7
к распоряжению администрации
муниципального образования городской
округ город-курорт Сочи
Краснодарского края
от 16.08.2021 № 300-р

ПРАВИЛА
аудита и регистрации событий безопасности в информационных системах администрации муниципального образования городской округ город-курорт Сочи Краснодарского края

1. Общие положения

1.1. Настоящие правила разработаны на основании:

– Постановления Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– Приказа Федеральной службы по техническому и экспортному контролю России от 11 февраля 2013 года № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

– Методического документа от 11 февраля 2014 года «Меры защиты информации в государственных информационных системах».

1.2. Настоящие правила определяют процедуры и объёмы аудита, сроки и порядок хранения, а также порядок защиты информации о событиях безопасности в информационных системах (далее – ИС) администрации муниципального образования городской округ город-курорт Сочи Краснодарского края (далее – администрация города Сочи).

1.3. Контроль за исполнением настоящих правил осуществляет администратор информационной безопасности (далее – администратор ИБ).

2. Назначение и область действия

2.1. Настоящие правила предназначены для администратора ИБ.

Настоящие правила распространяются на ИС, используемые в администрации города Сочи.

3. События безопасности, подлежащие регистрации

3.1. Определяются следующие события безопасности, подлежащие аудиту:

1) Вход/выход пользователей в ИС. В соответствии с мерой РСБ.1 необходимо осуществлять аудит входа/выхода пользователей средствами прикладного программное обеспечения (далее – ППО) ИС. Дополнительно, необходимо регистрировать успешные и неуспешные попытки входа в операционную систему (далее – ОС) ИС, время таких попыток, результат

входа/выхода, а также при возможности технической реализации – предъявленный идентификатор (учетная запись, смарт-карта) и пароль;

2) Доступ к ППО ИС. Необходимо осуществлять аудит доступа к ППО ИС;

3) События, связанные с функционированием средств защиты информации. Необходимо осуществлять аудит событий изменения параметров безопасности средств защиты информации;

4) События удаленного входа в ОС ИС. Необходимо осуществлять регистрацию неуспешных попыток удаленного входа в ОС ИС, аналогично регистрации событий локального входа.

5) События входа в ИС с учтенных мобильных устройств и носителей информации, подвергающихся регулярной ревизии и контролю.

4. Сроки хранения событий безопасности

4.1. Устанавливаются следующие сроки хранения информации о событиях безопасности:

– журнал аудита операционной системы – по мере переполнения;

– журнал аудита средства защиты информации от несанкционированного доступа – не менее 3 месяцев;

– журналы средств антивирусной защиты – по мере переполнения;

– журналы межсетевых экранов / систем обнаружения вторжений – не менее 3 месяцев.

4.2. При возможности технической реализации необходимо производить архивирование журнала событий безопасности.

5. Защита информации о события безопасности

5.1. Доступ к информации о событиях безопасности должны иметь администратор ИБ и ответственный за техническое обслуживание ИС.

5.2. Хранение информации о событиях безопасности должно осуществляться исключительно на выделенном серверном сегменте системы хранения данных, подлежащему строгому разграничению доступа и резервному копированию данных.

6. Пересмотр набора событий безопасности, подлежащих регистрации

6.1. Чтобы убедиться в том, что текущий набор событий по-прежнему необходимым и достаточен, периодически должны осуществляться пересмотр и обновление набора событий безопасности.

6.2. Обязательно осуществляются пересмотр и обновление набора событий безопасности, подвергаемых аудиту при:

– проведении работ по модернизации ИС;

– внедрении новых информационных технологий;

– проведении процедуры оценки эффективности.

7. Мониторинг результатов регистрации событий

7.1. Мониторинг результатов событий безопасности осуществляется администратором ИБ.

7.2. Просмотр и анализ результатов событий безопасности осуществляется еженедельно.

7.3. При возникновении нештатной ситуации просмотр и анализ результатов событий безопасности осуществляется безотлагательно.

Начальник управления информатизации и связи администрации муниципального образования городской округ город-курорт Сочи Краснодарского края Н.Р.Лавриенко

Приложение № 8
к распоряжению администрации
муниципального образования городской
округ город-курорт Сочи
Краснодарского края
от 16.08.2021 № 300-р

ПРАВИЛА
идентификации и аутентификации пользователей в информационных системах администрации муниципального образования городской округ город-курорт Сочи Краснодарского края

1. Общие сведения

1.1. Настоящие правила регламентируют организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (отключение учетных записей пользователей) в информационных системах администрации муниципального образования городской округ город-курорт Сочи Краснодарского края, а также отраслевых (функциональных) и территориальных органов администрации муниципального образования городской округ город-курорт Сочи Краснодарского края (далее – Правила).

1.2. Настоящие Правила разработаны на основании

– Приказа Федеральной службы по техническому и экспортному контролю России от 11 февраля 2013 года № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных система»;

– Методического документа от 11 февраля 2014 года «Меры защиты информации в государственных информационных системах».

1.3. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах и контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями возлагается на администратора информационной безопасности.

2. Требования к паролям

2.1. Личные пароли должны выбираться пользователями ИС самостоятельно с учетом следующих требований:

– длина пароля должна быть не менее 8 символов;

– пароль не должен включать в себя легко вычисляемые сочетания символов (qwerty, password, admin, administrator и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);

– личный пароль пользователь не имеет права сообщать никому.

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

2.3. Для генерации «стойких» значений паролей могут применяться специальные программные средства. Система генерации паролей должна исключать возможность ознакомления других работников с паролями исполнителей.

3. Использование паролей

3.1. Количество неуспешных попыток ввода пароля пользователем не должно превышать 10 попыток.

3.2. Временной период блокировки учетной записи пользователя в случае превышения допустимого количества неуспешных попыток ввода пароля должно составлять 10 минут.

3.3. Полная плановая смена паролей пользователей должна проводиться не более чем раз в 120 дней.

3.4. Внеплановая смена личного пароля пользователя или отключение учетной записи пользователя ИС в случае прекращения его полномочий (увольнение, переход на другую работу внутри организации и т.п.) должна производиться уполномоченным работником отдела технического обеспечения систем информационной безопасности МКУ «Электронный Сочи» немедленно после окончания последнего сеанса работы данного пользователя с системой.

4. Хранение и контроль

4.1. Хранение пользователем ИС значений своих паролей на бумажном носителе запрещена.

4.2. Повседневный контроль за действиями пользователей при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на руководителей подразделений, периодический контроль – возлагается на отдел технического обеспечения систем информационной безопасности МКУ «Электронный Сочи».

4.3. В случае компрометации личного пароля пользователя ИС должны быть немедленно предприняты меры по изменению пароля и выявлению последствий компрометации.

Начальник управления информатизации
и связи администрации муниципального
образования городской округ
город-курорт Сочи Краснодарского края Н.Р.Лавриенко

Приложение № 9
к распоряжению администрации
муниципального образования городской
округ город-курорт Сочи
Краснодарского края
от 16.08.2021 № 300-р

ПРАВИЛА
использования мобильных устройств в информационных системах администрации муниципального образования городской округ город-курорт Сочи Краснодарского края

1. Общие положения

1.1. Настоящие правила разработаны на основании:

– Приказа Федеральной службы по техническому и экспортному контролю России от 11 февраля 2013 года № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

– Методического документа от 11 февраля 2014 года «Меры защиты информации в государственных информационных системах».

1.2. Правила определяют порядок использования мобильных устройств и носителей информации в информационных системах (далее – ИС) администрации муниципального образования городской округ город-курорт Сочи Краснодарского края (далее – администрация города Сочи).

1.3. Данные правила распространяются на всех пользователей ИС, системных администраторов и администраторов информационной безопасности (далее – ИБ) администрации города Сочи, использующих для работы в информационных системах мобильные устройства и носители информации.

2. Порядок использования мобильных устройств и носителей информации

2.1. К мобильным устройствам в данных правилах относятся: ноутбуки, нетбуки, планшеты, сотовые телефоны и иные устройства.

2.2. Под использованием мобильных устройств и носителей информации в ИС администрации города Сочи понимается их подключение к инфраструктуре ИС с целью обработки, приема/передачи информации (в том числе персональных данных (далее – ПДн) между ИС и мобильными устройствами.

2.3. В ИС допускается использование только учтенных мобильных устройств и носителей информации, подвергающихся регулярной ревизии и контролю.

2.4. К используемым в администрации города Сочи мобильным устройствам и носителям информации предъявляются те же требования по защите информации, что и для стационарных автоматизированных рабочих мест (далее – АРМ).

2.5. При использовании предоставленных пользователям администрации города Сочи мобильных устройств и носителей информации, необходимо:

– использовать мобильные устройства и носители информации исключительно для выполнения своих должностных обязанностей;

– ставить в известность администратора ИБ о любых фактах нарушения требований настоящих правил;

– эксплуатировать и транспортировать мобильные устройствами и носители информации в соответствии с требованиями производителей;

– обеспечивать физическую безопасность мобильных устройств и носителей информации;

– извещать администратора ИБ о фактах утраты (кражи) мобильных устройств и носителей информации.

2.6. При использовании предоставленных пользователям администрации города Сочи мобильных устройств и носителей информации, запрещено:

– использовать мобильные устройства и носители информации в личных целях;

– передавать мобильные устройства и носители информации другим лицам (за исключением администратора ИБ);

– оставлять мобильные устройства и носители информации без присмотра, если не предприняты действия по обеспечению их физической безопасности.

2.7. Любое взаимодействие (обработка, прием/передача ПДн) инициированное пользователем ИС администрации города Сочи между ИС и неучтенными (личными) мобильными устройствами, а также носителями информации, рассматривается как несанкционированное (за исключением случаев, оговоренных с администратором ИБ заранее). Администрация города Сочи оставляет за собой право блокировать или ограничивать использование таких устройств и носителей информации.

2.8. Информация об использовании пользователями ИС администрации города Сочи мобильных устройств и носителей информации в ИС фиксируется, в соответствии с правилами аудита и регистрации событий безопасности, и при необходимости, может быть представлена руководителям пользователей.

2.9. При подозрении пользователя ИС администрации города Сочи в несанкционированном или нецелевом использовании мобильных устройств и носителей информации, инициализируется расследование допущенных нарушений, производимое администратором ИБ.

2.10. Информация, хранящаяся на предоставляемых мобильных устройствах и носителях информации, подлежит обязательной проверке на отсутствие вредоносного программного обеспечения.

3. Ответственность

Пользователи, нарушившие требования настоящих правил, несут ответственность, в соответствии с действующим законодательством Российской Федерации и нормативными актами администрации города Сочи.

Начальник управления информатизации и связи администрации муниципального образования городской округ город-курорт Сочи Краснодарского края Н.Р.Лавриенко

Приложение № 10
к распоряжению администрации
муниципального образования городской
округ город-курорт Сочи
Краснодарского края
от 16.08.2021 № 300-р

ПОЛИТИКА
учета и использования носителей информации в информационных системах администрации муниципального образования городской округ город-курорт Сочи Краснодарского края

1. Общие положения

Политика использования съемных носителей информации в информационной системе администрации муниципального образования городской округ город-курорт Сочи Краснодарского края, а также отраслевых (функциональных) и территориальных органов администрации муниципального образования городской округ город-курорт Сочи Краснодарского края (далее – Политика) разработана на основании:

– Приказа Федеральной службы по техническому и экспортному контролю России от 11 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных система»;

– Методического документа от 11 февраля 2014 года «Меры защиты информации в государственных информационных системах».

Под машинными носителями в настоящей Политике понимаются следующие носители информации:

1) дискеты;

2) оптические диски (CD, DVD) однократной и многократной записи;

3) электронные накопители информации (флэш-накопитали, внешние жесткие диски и иные внешние носители информации);

4) портативные вычислительные устройства и устройства связи с возможностью обработки информации (например: ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные средства).

1.1. Требования настоящей Политики распространяются на всех должностных лиц и муниципальных служащих администрации муниципального образования городской округ город-курорт Сочи Краснодарского края, а также должностных лиц и муниципальных служащих отраслевых (функциональных) и территориальных органов администрации муниципального образования городской округ город-курорт Сочи Краснодарского края являющихся пользователями информационной системы (далее – пользователи ИС).

1.2. Внесение изменений в настоящую Политику осуществляется на периодической и внеплановой основе:

– пересмотр положений настоящей Политики должен осуществляться не реже одного раза в 12 месяцев;

– внеплановое внесение изменений может проводиться в случае приобретения новых средств защиты, существенно изменяющих порядок работы с ними, либо по результатам контрольных мероприятий.

1.3. Ответственным за внесение изменений в настоящую Политику является администратор информационной безопасности.

1.4. Ответственность за выполнение положений настоящей Политики несут все пользователи ИС. Ответственность пользователей ИС за несоблюдение требований настоящей Политики, повлекших за собой разглашение или утрату информации ограниченного доступа, определяется законодательством Российской Федерации, а также должностными инструкциями муниципальных служащих.

1.5. Ответственность за общий контроль выполнения требований данной Политики возлагается на управление информатизации и связи администрации муниципального образования городской округ город-курорт Сочи Краснодарского края.

1.6. Ответственность за контроль, обеспечение безопасного использования съемных носителей информации возлагается на отдел технического сопровождения систем информационной безопасности МКУ «Электронный Сочи».

2. Порядок использования носителей информации

2.1. Под использованием носителей информации в ИС понимается их подключение к инфраструктуре ИС с целью хранения, обработки, приема/передачи информации между ИС и носителями информации.

2.2. В ИС допускается использование только учтенных носителей информации, которые являются собственностью администрации муниципального образования городской округ город-курорт Сочи Краснодарского края и подвергаются регулярной ревизии и контролю.

2.3. Носители информации предоставляются пользователям ИС по инициативе руководителей отраслевых (функциональных), территориальных органов администрации муниципального образования городской округ город-курорт Сочи Краснодарского края в случаях возникновения у пользователей ИС производственной необходимости.

3. Порядок учета, хранения и обращения со съемными носителями информации

3.1. Все находящиеся на хранении и в обращении съемные носители с информацией подлежат учёту.

3.2. Учет и выдачу съемных носителей информации осуществляет отдел технического сопровождения систем информационной безопасности МКУ «Электронный Сочи». Выдача съемного носителя информации осуществляется по карточке учета выдачи машинных носителей информации.

3.3. Любое взаимодействие (обработка, прием/передача информации), инициированное муниципальным служащим между ИС и неучтенными (личными) носителями информации, рассматривается как несанкционированное

(за исключением случаев, оговоренных с администратором информационной безопасности заранее).

3.4. Информация об использовании пользователями ИС машинных носителей информации в ИС протоколируется и, при необходимости, может быть предоставлена руководителям отраслевых (функциональных), территориальных органов администрации муниципального образования городской округ город-курорт Сочи Краснодарского края.

3.5. В случае выявления фактов несанкционированного и/или нецелевого использования носителей информации инициализируется служебная проверка, проводимая комиссией, состав которой определяется распоряжением администрации муниципального образования городской округ город-курорт Сочи Краснодарского края.

3.6. По факту выясненных обстоятельств составляется акт и передается руководителю отраслевого (функционального), территориального органова для принятия мер согласно нормативным актам администрации муниципального образования городской округ город-курорт Сочи Краснодарского края и действующему законодательству.

3.7. Информация, хранящаяся на носителях информации, подлежит обязательной проверке на отсутствие вредоносного ПО.

3.8. При отправке или передаче информации адресатам на съемные носители записываются только предназначенные адресатам данные.

3.9. В случае утраты или уничтожения съемных носителей информации либо разглашения, содержащихся в них сведений, немедленно ставится в известность руководитель соответствующего отраслевого (функционального), территориального органа администрации муниципального образования городской округ город-курорт Сочи Краснодарского края, а также начальник управления информатизации и связи муниципального образования городской округ город-курорт Сочи Краснодарского края. На утраченные носители составляется акт. Соответствующие отметки вносятся в форму учета съемных носителей информации.

3.10. Съемные носители информации, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей с информацией осуществляется комиссией, утверждаемой распоряжением администрации муниципального образования городской округ город-курорт Сочи Краснодарского края. По результатам уничтожения носителей составляется акт и вносятся соответствующие отметки в форму учета съемных носителей информации.

3.11. В случае увольнения или перевода муниципального служащего в другой отраслевой (функциональный), территориальный органов, выданные носители информации возвращаются.

3.12. Должно быть обеспечено уничтожение (стирание) информации с носителей информации после их приобретения, при первичном подключении к ИС, при использовании в сторонних ИС, при передаче для постоянного использования от одного пользователя другому пользователю, после возвращения из ремонта.

3.13. Для предотвращения восстановления удаленных файлов применяются меры по уничтожению (стиранию) информации на машинных носителях, реализуемые включением функции автоматического затирания удаляемой информации случайной числовой последовательностью, средством защиты информации Secret Net Studio.

4. Учет машинных носителей информации

4.1. Администратором ИБ должен быть обеспечен учет машинных носителей информации, используемых в информационной системе для хранения и обработки информации.

4.2. Учету подлежат:

– съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства);

– портативные вычислительные устройства, имеющие встроенные носители информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные аналогичные по функциональности устройства);

– машинные носители информации, встроенные в корпус средств вычислительной техники (накопители на жестких дисках).

4.3. Учет машинных носителей информации включает присвоение (регистрационных) учетных номеров носителям. В качестве регистрационных номеров используются идентификационные (серийные) номера машинных носителей, присвоенные производителями этих машинных носителей информации.

4.4. Учет съемных машинных носителей информации ведется в электронном виде на портале ib.sochiadm.ru в разделе «Учет МНИ».

4.5. Учет встроенных в портативные или стационарные технические средства машинных носителей информации ведется в электронном виде на портале ib.sochiadm.ru в разделе «Учет АРМ».

4.6. Регистрационные или иные номера подлежат занесению в электронные журналы учета с указанием пользователей, которым разрешен доступ к машинным носителям информации.

5. Порядок регистрации выдачи съемных машинных носителей информации

Выдача съемных машинных носителей информации осуществляется по карточке учета выдачи машинных носителей информации, в которой указывается маркировка носителя, дата, фамилия, имя и отчество должностного лица, получившего машинный носитель информации, его роспись. В случае возврата пользователем машинного носителя в карточке учета выдачи машинных носителей информации должностным лицом ответственным за учет и выдачу МНИ проставляется отметка о возврате с указанием даты и росписи принимающей стороны.

6. Управление доступом к машинным носителям информации

6.1. Администратором ИБ должны быть реализованы следующие функции по управлению доступом к машинным носителям информации, используемым в информационной системе:

– должностные лица, получают физический доступ к машинным носителям информации только после реализации заявки на доступ к защищаемым ресурсам, а именно к следующим:

- съемным машинным носителям информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства);
- портативным вычислительным устройствам, имеющим встроенные носители информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные аналогичные по функциональности устройства);
- машинным носителям информации, стационарно устанавливаемым в корпус средств вычислительной техники (например, накопители на жестких дисках);

– предоставление физического доступа к машинным носителям информации только тем лицам, которым он необходим для выполнения своих должностных обязанностей (функций), прописанных в должностных инструкциях.

7. Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения или стирания

7.1. Должностными лицами отдела технического сопровождения систем информационной безопасности МКУ «Электронный Сочи» должно обеспечиваться уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) информации.

7.2. Уничтожение (стирание) информации на машинных носителях должно исключать возможность восстановления защищаемой информации при передаче машинных носителей между пользователями, в сторонние организации для ремонта или утилизации.

7.3. Уничтожению (стиранию) подлежит информация, хранящаяся на цифровых и нецифровых, съемных и несъемных машинных носителях информации.

7.4. Процедуры уничтожения (стирания) информации на машинных носителях, а также контроля уничтожения (стирания) информации должны выполняться с помощью сертифицированных средств защиты информации и содержать следующие действия, исключающие возможность восстановления защищаемой информации:

– полная многократная перезапись машинного носителя информации специальными битовыми последовательностями, зависящими от типа накопителя и используемого метода кодирования информации;

– очистка всего физического пространства накопителя, включая сбойные и резервные элементы памяти специализированными программами или утилитами производителя.

8. Защита мобильных технических средств

8.1. Должностными лицами отдела технического сопровождения систем информационной безопасности МКУ «Электронный Сочи» должна осуществляться защита применяемых в информационной системе мобильных технических средств.

8.2. Защита мобильных технических средств включает:

– очистку (удаление) информации в мобильном техническом средстве после завершения сеанса удаленного доступа к защищаемой информации или принятие иных мер, исключающих несанкционированный доступ к хранимой защищаемой информации;

– уничтожение съемных машинных носителей информации, которые не подлежат очистке;

– выборочные проверки мобильных технических средств (на предмет их наличия) и хранящейся на них информации (например, на предмет отсутствия информации, не соответствующей маркировке носителя информации);

– запрет возможности автоматического запуска (без команды пользователя) в информационной системе программного обеспечения на мобильных технических средствах.

9. Обязанности пользователей при использовании съемных носителей

9.1. При использовании муниципальными служащими носителей информации необходимо:

– соблюдать требования настоящей Политики;

– использовать носители информации исключительно для выполнения своих служебных обязанностей;

– ставить в известность администратора ИБ о любых фактах нарушения требований настоящей Политики;

– бережно относиться к носителям информации;

– обеспечивать физическую безопасность носителей информации всеми разумными способами;

– извещать администратора ИБ о фактах утраты (кражи) носителей информации.

9.2. При использовании носителей информации запрещено:

– использовать носители информации в личных целях;

– передавать носители информации другим лицам;

– хранить съемные носители с информацией на рабочих столах либо оставлять их без присмотра или передавать на хранение другим лицам;

– выносить съемные носители с информацией из служебных помещений для работы с ними на дому и т. д.

Начальник управления информатизации
и связи администрации муниципального
образования городской округ
город-курорт Сочи Краснодарского края Н.Р.Лавриенко

Приложение № 11
к распоряжению администрации
муниципального образования городской
округ город-курорт Сочи
Краснодарского края
от 16.08.2021 № 300-р

ПОЛИТИКА
контроля защищенности в информационных системах администрации муниципального образования городской округ город-курорт Сочи Краснодарского края, а также в отраслевых (функциональных) и территориальных органах администрации муниципального образования городской округ город-курорт Сочи Краснодарского края

1. Общие положения

Политика контроля защищенности информации в информационных системах администрации муниципального образования городской округ город-курорт Сочи Краснодарского края (далее – Политика) разработана в соответствии с методическим документом «Меры защиты информации в государственных информационных системах» утвержден Федеральной службой по техническому и экспортному контролю России 11 февраля 2014 года

Настоящая Политика определяет порядок действий администратора информационной безопасности (далее – ИБ) и администратора информационных систем (далее – ИС).

2. Выявление, анализ и устранение уязвимостей информационных систем

Уязвимость – это недостаток информационных систем или системы защиты информации, который может привести к реализации угрозы безопасности информации, обрабатываемой в информационных системах администрации муниципального образования городской округ город-курорт Сочи Краснодарского края (далее – администрация города Сочи), а также в отраслевых (функциональных) и территориальных органах администрации города Сочи.

Периодичность плановых процедур выявления, анализа и устранения уязвимостей ИС составляет 3 месяца. Внеплановые процедуры выявления, анализа и устранения уязвимостей ИС проводят в случае необходимости по распоряжению администратора ИБ. Необходимость внеплановой процедуры определяется на основе анализа журналов событий безопасности.

При выявлении (поиске), анализе и устранении уязвимостей в ИС должны проводиться:

– выявление (поиск) уязвимостей, связанных с ошибками кода в программном (микропрограммном) обеспечении (общесистемном, прикладном, специальном), а также программном обеспечении (далее – ПО) средств защиты информации (далее – СЗИ), правильностью установки и настройки СЗИ,

технических средств и ПО, а также корректностью работы СЗИ при их взаимодействии с техническими средствами и ПО.

По результатам проведения процедуры выявления, анализа и устранения уязвимостей ИС должно быть обеспечено:

– анализ отчетов средств защиты информации о результатах поиска уязвимостей;

– устранение выявленных уязвимостей, в том числе путем установки обновлений ПО СЗИ, общесистемного ПО, прикладного ПО или микропрограммного обеспечения технических средств;

– информирование уполномоченных лиц о результатах поиска уязвимостей и оценки достаточности реализованных мер защиты информации.

В качестве источников информации об уязвимостях должны быть использованы опубликованные данные разработчиков СЗИ, общесистемного, прикладного и специального ПО, технических средств, а также другие базы данных уязвимостей.

Непосредственным исполнителем мероприятий по выявлению и анализу уязвимостей ИС является администратор ИБ. В целях устранения выявленных уязвимостей ИС, администратор ИБ имеет право привлекать администратора ИС.

В случае невозможности устранения выявленных уязвимостей путем установки обновлений ПО СЗИ, общесистемного ПО, прикладного ПО или микропрограммного обеспечения технических средств необходимо предпринять действия (настройки СЗИ, изменение режима и порядка использования информационной системы), направленные на устранение возможности использования выявленных уязвимостей.

В целях выявления уязвимостей ИС администратором ИБ должны применяться сканеры безопасности, имеющие стандартизованные (унифицированные) описание и перечни программно-аппаратных платформ, уязвимостей ПО, ошибочных конфигураций, правил описания уязвимостей, проверочных списков, процедур тестирования и языка тестирования ИС на наличие уязвимостей, оценки последствий уязвимостей, имеющих возможность оперативного обновления базы данных выявляемых уязвимостей.

Доступ к консоли управления сканером безопасности должен предоставляться только администратору ИБ.

3. Контроль работоспособности, параметров настройки и правильности функционирования ПО и СЗИ

Администратором ИБ должен проводиться контроль работоспособности, параметров настройки и правильности функционирования ПО и СЗИ.

Контроль работоспособности, параметров настройки и правильности функционирования ПО и СЗИ проводится администратором ИБ с периодичностью не менее одного раза в месяц.

Администратор ИБ должен осуществлять проверку конфигурации и настроек ПО и СЗИ ИС на соответствие требованиям эксплуатационной

документации на СЗИ и подсистему информационной безопасности ИС, а также требованиям к защите информации.

Администратор ИБ должен осуществлять проверку:

– наличия и сроков лицензий на установленное ПО и СЗИ;

– наличия последних обновлений используемого ПО и СЗИ (обновления вирусных баз, обновлений баз уязвимостей).

4. Контроль состава технических средств, ПО и СЗИ

В ИС должно осуществляться реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти.

Администратором ИБ должен проводиться контроль состава технических средств, ПО и СЗИ, применяемых в ИС с периодичностью не реже одного раза в месяц.

Администратор ИБ должен проводить анализ перечня событий безопасности за период контроля, связанных с отказами и неисправностями технических средств ИС.

В ИС должна обеспечиваться регистрация событий безопасности, связанных с изменением состава технических средств, ПО и СЗИ.

Обнаруженные в ходе контроля отклонения от конфигурации ИС устраняет администратор ИБ и администратор ИС. При обнаружении технических средств с низкой надежностью, частыми выходами из строя администратор ИБ принимает меры по ремонту или замене этих технических средств. В случае, если технические средства, подлежащие ремонту или замене, входят в состав аттестованной ИС, администратор ИБ обязан оповестить орган по аттестации о таких изменениях в конфигурации ИС.

5. Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в ИС

Администратором ИБ должен проводиться контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в ИС с периодичностью не реже одного раза в месяц.

В ИС должна обеспечиваться регистрация событий, связанных со сменой паролей пользователей, заведением и удалением учетных записей пользователей, изменением правил разграничения доступом и полномочий пользователей.

6. Выявление, анализ и устранение организационно-технических недостатков

Администратор ИБ совместно с лицом, ответственным за обработку и защиту персональных данных должны проводить:

– проверку состояния и актуальности организационно-распорядительной документации (далее – ОРД) по защите информации, обрабатываемой в ИС;

– проверку заполнения рабочих документов ОРД (записи в журналах, перечнях, актах и других формах по требованиям ОРД);

– проверку соответствия выполнения правил генерации и смены паролей пользователей принятым требованиям;

– проверка соответствия выполнения правил заведения и удаления учетных записей пользователей принятым требованиям;

– проверку соответствия выполнения правил разграничения доступа к информации и ресурсам ИС принятым требованиям;

– проверку соответствия полномочий пользователей принятым требованиям;

– проверку наличия документов, подтверждающих правомерность изменений учетных записей пользователей, их параметров, правил разграничения доступом и полномочий пользователей;

– проверку состояния физической защиты ИС (средства охраны и физического доступа в контролируемой зоне ИС);

– проверку знания и соблюдения пользователями ИС основных нормативно-правовых актов в области защиты информации и требований ОРД.

7. Контроль за обеспечением уровня защищенности информации, содержащейся в информационной системе

В ходе контроля за обеспечением уровня защищенности информации, содержащейся в информационной системе, осуществляются:

– контроль (анализ) защищенности информации с учетом особенностей функционирования информационной системы;

– анализ и оценка функционирования информационной системы и ее системы защиты информации, включая анализ и устранение уязвимостей и иных недостатков в функционировании системы защиты информации информационной системы;

– документирование процедур и результатов контроля за обеспечением уровня защищенности информации, содержащейся в информационной системе;

– принятие решения по результатам контроля за обеспечением уровня защищенности информации, содержащейся в информационной системе, о необходимости доработки (модернизации) ее системы защиты информации.

Контроль за обеспечением уровня защищенности информации (далее – периодический контроль), содержащейся в информационной системе, проводится администрацией города Сочи самостоятельно и (или) с привлечением организации, имеющей лицензию на деятельность по технической защите информации ограниченного доступа. В случае самостоятельного проведения периодического контроля создается специальная комиссия или возлагается проведение периодического контроля на комиссию из состава работников организации, имеющей лицензию на деятельность по технической защите информации.

Периодичность проведения контроля за обеспечением уровня защищенности информации, содержащейся в информационной системе, устанавливается не реже 1 раза в два года.

Периодический контроль проводится в соответствии с разрабатываемой программой и методикой контроля за обеспечением уровня защищенности информации (при этом за основу может быть взята программа и методика аттестационных испытаний ранее аттестованных информационных систем, в соответствии с установленными классами защищенности новых информационных систем).

Указанная программа и методики должна содержать:

– описания контрольных мероприятий (проверок, испытаний), проводимых при периодическом контроле, необходимых и достаточных для оценки функционирования и установления соответствия требованиям безопасности информации информационной системы и ее системы защиты;

– средства инструментального контроля, необходимые для проведения периодического контроля;

– требования к документированию периодического контроля.

По результатам периодического контроля комиссия принимает решение о необходимости доработки (модернизации) ее системы защиты информации.

Начальник управления информатизации
и связи администрации муниципального
образования городской округ город-
курорт Сочи Краснодарского края Н.Р.Лавриенко

Приложение № 12
к распоряжению администрации
муниципального образования городской
округ город-курорт Сочи
Краснодарского края
от 16.08.2021 № 300-р

ПОЛИТИКА
контроля и управления доступом к информационным системам и ресурсам администрации муниципального образования городской округ город-курорт Сочи Краснодарского края

1. Общие положения

1.1. Политика контроля и управления доступом к информационным системам и ресурсам администрации муниципального образования городской округ город-курорт Сочи Краснодарского края, а также отраслевых (функциональных) и территориальных органов администрации муниципального образования городской округ город-курорт Сочи Краснодарского края (далее – Политика) разработана на основе:

– Приказа Федеральной службы по техническому и экспортному контролю России от 11 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных система»;

– Методического документа от 11 февраля 2014 года «Меры защиты информации в государственных информационных системах».

1.2. Настоящая политика определяет:

– требования по обеспечению защиты информации в информационных системах администрации муниципального образования городской округ город-курорт Сочи Краснодарского края, а также отраслевых (функциональных) и территориальных органов администрации муниципального образования городской округ город-курорт Сочи Краснодарского края (далее – ИС) от несанкционированного доступа;

– порядок предоставления, прекращения и изменения доступа пользователей к ИС, включая сетевые сервисы (сервис печати, электронная почта, Web-серверы и т. д.), разделяемые сетевые файловые ресурсы (файлы, каталоги, диски, рабочие станции, периферия), серверы баз данных и т.п.;

– порядка изменения прав доступа пользователей к ИС при переходе на другую должность, изменении должностных обязанностей и т.п.;

– требования, предъявляемые к муниципальным служащим, в случае предоставления им доступа к ИС;

– ответственность муниципальных служащих.

1.3. Настоящая политика распространяется на все информационные процессы ИС и обязательна для применения всеми работниками и муниципальными служащими отраслевых (функциональных) и территориальных органов администрации муниципального образования

городской округ город-курорт Сочи Краснодарского края, а также представителями сторонних организаций, имеющими доступ к ИС.

1.4. Мероприятия по обеспечению информационной безопасности, выполняемые с целью реализации требований настоящей политики, утверждаются внутренними нормативными документами в соответствии с установленным порядком.

1.5. Внесение изменений в настоящую Политику осуществляется на периодической и внеплановой основе:

– пересмотр положений настоящей Политики должен осуществляться не реже одного раза в 12 месяцев;

– внеплановое внесение изменений может проводиться по результатам проведения контрольных мероприятий.

1.6. Ответственным за внесение изменений в настоящую Политику является администратор информационной безопасности.

1.7. Ответственность за выполнение положений настоящей Политики несут все работники и муниципальные служащие отраслевых (функциональных) и территориальных органов администрации муниципального образования городской округ город-курорт Сочи Краснодарского края (далее – пользователи ИС).

1.8. Ответственность пользователей ИС за несоблюдение требований настоящей Политики, повлекших за собой разглашение или утрату информации ограниченного доступа, определяется законодательством Российской Федерации, а также должностными инструкциями.

1.9. Ответственность за общий контроль выполнения требований данной Политики возлагается на администратора ИБ.

2. Общие положения по организации контроля и управления доступом к ресурсам корпоративной сети

2.1. Доступ к ИС может быть предоставлен только муниципальным служащим и работникам подведомственных учреждений, с которыми заключены трудовые отношения.

2.2. Доступ к ИС иных организаций может быть осуществлен на основании заключаемых договоров и (или) соглашений при условии выполнения требований к защите информации.

2.3. Для предоставления муниципальным служащим и работникам подведомственных учреждений доступа к ИС должна осуществляться процедура их регистрации в качестве пользователей ИС, в результате которой для каждого муниципального служащего и работника подведомственного учреждения создается одна или несколько учётных записей, используемых для получения доступа к локальному компьютеру и сетевым сервисам (сервис печати, электронная почта, Web-серверы и т.д.), разделяемым сетевым файловым ресурсам (файлы, каталоги, диски, рабочие станции, периферия), серверам баз данных и т. п.

2.4. При доступе в ИС должна осуществляться идентификация и аутентификация пользователей и процессов, запускаемых от имени этих пользователей, а также процессов, запускаемых от имени системных учетных записей.

2.5. Пользователи ИС должны однозначно идентифицироваться и аутентифицироваться для всех видов доступа, кроме тех видов доступа, которые определяются как действия, разрешенные до идентификации и аутентификации.

2.6. Аутентификация пользователя осуществляется с использованием паролей.

2.7. В ИС должна быть обеспечена возможность однозначного сопоставления идентификатора пользователя с запускаемыми от его имени процессами.

2.8. Учётные записи пользователя включают в себя данные, однозначно идентифицирующие данного пользователя, и служат для определения пользовательских полномочий по доступу к ИС, а также осуществления контроля над действиями пользователей.

2.9. Не допускается использование учётных записей других пользователей для осуществления доступа к ИС.

2.10. Всем пользователям ИС присваивается уникальное имя и предлагается выбрать пароль. При регистрации в системе пользователю необходимо ввести свое уникальное имя. Пароль служит доказательством того, что пользователь является именно тем, за кого себя выдает. Пароль пользователи обязаны держать в секрете и никому не сообщать.

2.11. При выборе, хранении и использовании паролей пользователи должны руководствоваться «Политикой идентификации и аутентификации пользователей в информационных системах администрации муниципального образования городской округ город-курорт Сочи Краснодарского края».

2.12. Доступ к ИС должен осуществляться зарегистрированными пользователями при предъявлении доказательств их подлинности (аутентификации). Используемая схема аутентификации должна исключать возможность несанкционированного доступа к ИС.

2.13. Механизмы доступа к ресурсам ИС настраиваются в соответствии с Матрицей доступа.

2.14. В ИС должна осуществляться защита аутентификационной информации в процессе ее ввода для аутентификации от возможного использования лицами, не имеющими на это полномочий. Защита обратной связи «система - субъект доступа» в процессе аутентификации обеспечивается исключением отображения для пользователя действительного значения аутентификационной информации и (или) количества вводимых пользователем символов аутентификационной информации. Вводимые символы пароля могут отображаться условными знаками «*», «•» или иными знаками.

2.15. Все запросы на предоставление или изменение прав доступа к ИС должны регистрироваться в системе электронного документооборота.

3. Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных

3.1. В ИС до начала информационного взаимодействия (передачи защищаемой информации от устройства к устройству) должна осуществляться идентификация и аутентификация устройств (технических средств).

3.2. В ИС должен быть определен перечень типов устройств, используемых в ИС и подлежащих идентификации и аутентификации до начала информационного взаимодействия.

3.3. Идентификация устройств в ИС обеспечивается по логическим именам (имя устройства и (или) ID), логическим адресам (например, IP-адресам) и (или) по физическим адресам (например, MAC-адресам) устройства или по комбинации имени, логического и (или) физического адресов устройства.

3.4. Аутентификация устройств в ИС обеспечивается с использованием соответствующих протоколов аутентификации или с применением в соответствии с законодательством Российской Федерации криптографических методов защиты информации.

4. Порядок предоставления муниципальным служащим доступа к ИС администрации муниципального образования городской округ город-курорт Сочи Краснодарского края

4.1. Права доступа к ИС предоставляются пользователю на время и в объеме, необходимом для выполнения им своих должностных обязанностей.

4.2. Первоначальный доступ к ИС предоставляется пользователю только после ознакомления с настоящей Политикой, а также другими документами, регламентирующими правила работы пользователей в сети и их подписания при оформлении муниципального служащего на работу.

4.3. Доступ к ИС должен предоставляться муниципальному служащему в соответствии с «Правилами по внесению изменений в списки пользователей и наделению их полномочиями доступа к ресурсам информационных систем администрации муниципального образования городской округ город-курорт Сочи Краснодарского края».

4.4. Для предоставления доступа к конкретным ресурсам ИС инициатор заявки в обязательном порядке предоставляет требуемые согласующие подписи руководителей подразделений, владеющих этими ресурсами.

4.5. Администратор ИБ устанавливает и реализует следующие функции управления идентификаторами пользователей и устройств в ИС:

– определение должностного лица, ответственного за создание, присвоение и уничтожение идентификаторов пользователей;

– формирование идентификатора, который однозначно идентифицирует пользователя и (или) устройство;

– присвоение идентификатора пользователю;

– предотвращение повторного использования идентификатора пользователя и (или) устройства в течение не менее одного года;

– блокирование идентификатора пользователя после 90 дней неиспользования.

4.6. Администратор ИБ устанавливает и реализует следующие функции управления учетными записями пользователей, в том числе внешних пользователей:

– определение типа учетной записи (пользователь ИС, администратор ИС, администратор ИБ);

– объединение учетных записей в группы (при необходимости);

– верификацию пользователя (проверка личности пользователя, его должностных (функциональных) обязанностей) при заведении учетной записи пользователя;

– заведение, активация, блокирование и уничтожение учетных записей пользователей;

– пересмотр и, при необходимости, корректировка учетных записей пользователей;

– порядок заведения и контроля использования гостевых (анонимных) и временных учетных записей пользователей, а также привилегированных учетных записей администраторов;

– оповещение администратора, осуществляющего управление учетными записями пользователей, об изменении сведений о пользователях, их ролях, обязанностях, полномочиях, ограничениях;

– уничтожение временных учетных записей пользователей, предоставленных для однократного (ограниченного по времени) выполнения задач в ИС;

– предоставление пользователям прав доступа к объектам доступа ИС, основываясь на задачах, решаемых пользователями в ИС и взаимодействующими с ней информационными системами.

4.7. Временная учетная запись может быть заведена для пользователя на ограниченный срок для выполнения задач, требующих расширенных полномочий, или для проведения настройки, тестирования ИС, для организации гостевого доступа (посетителям, сотрудникам сторонних организаций, стажерам и иным пользователям с временным доступом к ИС).

4.8. Руководители отраслевых (функциональных), территориальных органов администрации муниципального образования городской округ город-курорт Сочи Краснодарского края несут ответственность за предоставление их подчиненным доступа к ИС в строгом соответствии с их должностными обязанностями.

5. Порядок блокирования, изменения прав доступа увольняемых муниципальных служащих к ИС

5.1. Департамент муниципальной службы и кадровой политики администрации муниципального образования городской округ город-курорт Сочи Краснодарского края, а также отраслевые (функциональные) и территориальные органы администрации муниципального образования

городской округ город-курорт Сочи Краснодарского края, обладающие правом юридического лица, должны своевременно извещать управление информатизации и связи администрации муниципального образования городской округ город-курорт Сочи Краснодарского края (далее – УИС) о фактах увольнения, перевода на новую должность, а также выхода в отпуск по уходу за ребенком подчиненных должностных лиц.

5.2. При получении информации УИС обеспечивает блокирование или корректировку доступа пользователей к ресурсам ИС.

5.3. Специалист отдела технического обеспечения систем информационной безопасности МКУ «Электронный Сочи» обязан произвести блокировку (удаление) всех пользовательских учётных записей уволенного пользователя (в сетевых доменах, почтовых системах, приложениях, сервере удаленного доступа, серверах баз данных и т.п.).

5.4. Расширение прав доступа пользователей к ИС должно производиться в соответствии с Порядком предоставления доступа, описанным в соответствующем разделе настоящей Политики.

6. Идентификация и аутентификация пользователей, не являющихся муниципальными служащими администрации муниципального образования городской округ город-курорт Сочи Краснодарского края (далее - внешние пользователи) (для ИС)

6.1. Администратором ИБ в ИС должна осуществляться однозначная идентификация и аутентификация внешних пользователей и/или процессов, запускаемых от имени этих пользователей.

6.2. К внешним пользователям, относятся все пользователи ИС, с которыми не заключены трудовые отношения. Примером внешних пользователей являются граждане, на законных основаниях через сеть Интернет получающие доступ к информационным ресурсам портала Государственных услуг Российской Федерации «Электронного правительства» или официальным сайтам в сети Интернет органов государственной власти и местного самоуправления.

6.3. Внешние пользователи ИС должны однозначно идентифицироваться и аутентифицироваться для всех видов доступа, кроме тех видов доступа, которые определяются как действия, разрешенные до идентификации и аутентификации.

6.4. Идентификация и аутентификация внешних пользователей в целях предоставления государственных услуг осуществляется в том числе с использованием единой системы идентификации и аутентификации, созданной в соответствии с постановлением Правительства Российской Федерации от 28 ноября 2011 года № 977 «О федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме».

7. Реализация необходимых методов управления доступом (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа

7.1. Администратором ИБ в ИС для управления доступом субъектов доступа к объектам доступа должны быть реализованы методы управления доступом, назначены типы доступа субъектов к объектам доступа и реализованы правила разграничения доступа субъектов доступа к объектам доступа.

7.2. Методы управления доступом реализуются в зависимости от особенностей функционирования ИС, с учетом угроз безопасности информации и должны включать один или комбинацию следующих методов:

– дискреционный метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе идентификационной информации субъекта и для каждого объекта доступа – списка, содержащего набор субъектов доступа (групп субъектов) и ассоциированных с ними типов доступа;

– ролевой метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе ролей субъектов доступа (совокупность действий и обязанностей, связанных с определенным видом деятельности);

– мандатный метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе сопоставления классификационных меток каждого субъекта доступа и каждого объекта доступа, отражающих классификационные уровни субъектов доступа и объектов доступа, являющиеся комбинациями иерархических и неиерархических категорий.

7.3. Типы доступа должны включать операции по чтению, записи, удалению, выполнению и иные операции, разрешенные к выполнению пользователем (группе пользователей) или запускаемому от его имени процессу при доступе к объектам доступа.

7.4. Правила разграничения доступа реализуются на основе установленных списков доступа или матриц доступа и должны обеспечивать управление доступом пользователей (групп пользователей) и запускаемых от их имени процессов при входе в систему, доступе к техническим средствам, устройствам, объектам файловой системы, запускаемым и исполняемым модулям, объектам систем управления базами данных, объектам, создаваемым прикладным и специальным программным обеспечением, параметрам настройки средств защиты информации, информации о конфигурации системы защиты информации и иной информации о функционировании системы защиты информации, а также иным объектам доступа.

8. Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации

8.1. Администратором ИБ реализуются следующие функции управления средствами аутентификации (аутентификационной информацией) пользователей и устройств в ИС:

– изменение аутентификационной информации (средств аутентификации), заданных их производителями и (или) используемых при внедрении системы защиты информации ИС;

– выдача средств аутентификации пользователям;

– генерация и выдача начальной аутентификационной информации (начальных значений средств аутентификации);

– установление в Политике идентификации и аутентификации пользователей в информационных системах администрации муниципального образования городской округ город-курорт Сочи Краснодарского края характеристик пароля:

а) задание минимальной сложности пароля с определяемыми требованиями к регистру, количеству символов, сочетанию букв верхнего и нижнего регистра, цифр и специальных символов;

б) задание минимального количества измененных символов при создании новых паролей;

в) задание максимального времени действия пароля;

г) задание минимального времени действия пароля;

д) запрет на использование пользователями определенного числа последних использованных паролей при создании новых паролей;

– блокирование (прекращение действия) и замена утерянных, скомпрометированных или поврежденных средств аутентификации;

– назначение необходимых характеристик средств аутентификации (в том числе механизма пароля);

– обновление аутентификационной информации (замена средств аутентификации);

– защита аутентификационной информации от неправомерного доступа к ней и модифицирования.

9. Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами ИС

9.1. Должностными лицами МКУ «Электронный Сочи» должно осуществляться управление информационными потоками при передаче информации между устройствами, включающее:

– фильтрацию информационных потоков в соответствии с правилами управления потоками, установленными администратором ИБ;

– разрешение передачи информации в ИС системе только по маршруту, установленному администратором ИБ;

– изменение (перенаправление) маршрута передачи информации в случаях, установленных администратором ИБ;

9.2. Управление информационными потоками должно обеспечивать разрешенный (установленный администратором ИБ) маршрут прохождения информации между пользователями, устройствами, сегментами в рамках ИС, а также между ИС или при взаимодействии с сетью Интернет (или другими информационно-телекоммуникационными сетями международного информационного обмена) на основе правил управления информационными потоками, включающих контроль конфигурации ИС, источника и получателя передаваемой информации, структуры передаваемой информации, характеристик информационных потоков и (или) канала связи (без анализа содержания информации). Управление информационными потоками должно блокировать передачу защищаемой информации через сеть Интернет (или другие информационно-телекоммуникационные сети международного информационного обмена) по незащищенным линиям связи, сетевые запросы и трафик, несанкционированно исходящие из ИС и (или) входящие в ИС.

10. Регламентация и контроль использования в ИС технологий беспроводного доступа

10.1. Администратор ИБ обеспечивает контроль использования в ИС технологий беспроводного доступа пользователей к объектам доступа (стандарты коротковолновой радиосвязи, спутниковой и пакетной радиосвязи), направленные на защиту информации в ИС.

10.2. Регламентация и контроль использования технологий беспроводного доступа включают:

– ограничение на использование технологий беспроводного доступа (беспроводной передачи данных, беспроводного подключения оборудования к сети, беспроводного подключения устройств к средству вычислительной техники) в соответствии с задачами (функциями) ИС, для решения которых такой доступ необходим, и предоставление беспроводного доступа;

– предоставление технологий беспроводного доступа только тем пользователям, которым он необходим для выполнения установленных должностных обязанностей (функций);

– мониторинг и контроль применения технологий беспроводного доступа на предмет выявления несанкционированного использования технологий беспроводного доступа к объектам доступа ИС;

– контроль беспроводного доступа пользователей (процессов запускаемых от имени пользователей) к объектам доступа ИС до начала информационного взаимодействия с ИС;

– аутентификацию подключаемых с использованием технологий беспроводного доступа устройств;

– запрет возможности изменения пользователем точек беспроводного доступа информационной системы.

11.Регламентация и контроль использования в ИС мобильных технических средств

11.1. Администратор ИБ обеспечивает контроль использования в ИС мобильных технических средств, направленный на защиту информации в ИС.

11.2. В качестве мобильных технических средств рассматриваются съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства), портативные вычислительные устройства и устройства связи с возможностью обработки информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные устройства).

11.3. Регламентация и контроль использования мобильных технических средств включают:

– установление (в том числе документальное) видов доступа (беспроводной, проводной (коммутируемый), широкополосный и иные виды доступа), разрешенных для доступа к объектам доступа ИС с использованием мобильных технических средств, входящих в состав ИС;

– использование в составе ИС для доступа к объектам доступа мобильных технических средств (служебных мобильных технических средств), в которых реализованы меры защиты информации;

– ограничение на использование мобильных технических средств в соответствии с задачами (функциями) ИС, для решения которых использование таких средств необходимо, и предоставление доступа с использованием мобильных технических средств;

– мониторинг и контроль применения мобильных технических средств на предмет выявления несанкционированного использования мобильных технических средств для доступа к объектам доступа ИС;

– запрет возможности запуска без команды пользователя в ИС программного обеспечения (программного кода), используемого для взаимодействия с мобильным техническим средством;

– запрет использования в ИС, не входящих в ее состав (находящихся в личном использовании) съемных машинных носителей информации;

– запрет использования в ИС съемных машинных носителей информации, для которых не определен владелец (пользователь, организация, ответственные за принятие мер защиты информации).

12.Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)

12.1. Администратором ИБ должно быть обеспечено управление взаимодействием с внешними информационными системами, включающими информационные системы и вычислительные ресурсы (мощности)

уполномоченных лиц, информационные системы, с которыми установлено информационное взаимодействие на основании заключенного договора (соглашения), а также с иными информационными системами, информационное взаимодействие с которыми необходимо для функционирования ИС.

12.2. Управление взаимодействием с внешними информационными системами должно включать:

– предоставление доступа к информационной системе только авторизованным (уполномоченным) пользователям;

– определение типов прикладного программного обеспечения информационной системы, к которым разрешен доступ авторизованным (уполномоченным) пользователям из внешних информационных систем;

– определение системных учетных записей, используемых в рамках данного взаимодействия;

– определение порядка предоставления доступа к информационной системе авторизованными (уполномоченным) пользователями из внешних информационных систем;

– определение порядка обработки, хранения и передачи информации с использованием внешних информационных систем.

12.3. Управление взаимодействием с внешними информационными системами в целях межведомственного электронного взаимодействия, исполнения государственных и муниципальных функций, формирования базовых государственных информационных ресурсов осуществляется в том числе с использованием единой системы идентификации и аутентификации, созданной в соответствии с постановлением Правительства Российской Федерации от 28 ноября 2011 года № 977 «О федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме».

12.4. Администратор ИБ предоставляет доступ к ИС авторизованным (уполномоченным) пользователям внешних информационных систем или разрешает обработку, хранение и передачу информации с использованием внешней информационной системы при выполнении следующих условий:

– при наличии договора (соглашения) об информационном взаимодействии с обладателем (владельцем) внешней информационной системы;

– при наличии подтверждения выполнения во внешней информационной системе предъявленных к ней требований о защите информации (наличие аттестата соответствия требованиям по безопасности информации или иного подтверждения).

13.Обеспечение доверенной загрузки средств вычислительной техники

13.1. Отделом технического сопровождения систем информационной безопасности МКУ «Электронный Сочи» должно обеспечиваться исключение

несанкционированного доступа к программным и (или) техническим ресурсам средства вычислительной техники информационной системы на этапе его загрузки.

13.2. Доверенная загрузка должна обеспечивать:

– блокирование попыток несанкционированной загрузки нештатной операционной системы (среды) или недоступность информационных ресурсов для чтения или модификации в случае загрузки нештатной операционной системы;

– контроль доступа пользователей к процессу загрузки операционной системы.

13.3. В ИС применяется доверенная загрузка на разных уровнях (уровня базовой системы ввода-вывода, уровня платы расширения и уровня загрузочной записи).

14.Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения

14.1. Администратором ИС должны быть реализованы следующие функции по управлению установкой (инсталляцией) компонентов программного обеспечения ИС:

– определение компонентов программного обеспечения (состава и конфигурации), подлежащих установке в ИС после загрузки операционной системы;

– настройка параметров установки компонентов программного обеспечения, обеспечивающая исключение установки компонентов программного обеспечения, использование которых не требуется для реализации информационной технологии информационной системы (например, при запуске установщика можно выбрать или не выбрать определенные опции и, тем самым, разрешить или запретить установку соответствующих компонентов программного обеспечения);

– выбор конфигурации устанавливаемых компонентов программного обеспечения (в том числе конфигурации, предусматривающие включение в домен, или не включение в домен);

– контроль за установкой компонентов программного обеспечения (состав компонентов, параметры установки, конфигурация компонентов);

– определение и применение параметров настройки компонентов программного обеспечения, включая программные компоненты средств защиты информации, обеспечивающих реализацию мер защиты информации, а также устранение возможных уязвимостей ИС, приводящих к возникновению угроз безопасности информации.

15.Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов

15.1. Администратором ИС должна быть обеспечена установка (инсталляция) только разрешенного к использованию в ИС программного обеспечения и (или) его компонентов.

15.2. Установка (инсталляция) в ИС программного обеспечения (вида, типа, класса программного обеспечения) и (или) его компонентов осуществляется с учетом перечня программного обеспечения и (или) его компонентов, разрешенных к установке («белый список»), и (или) перечнем программного обеспечения и (или) его компонентов, запрещенных к установке («черный список»). Указанные перечни программного обеспечения и (или) его компонентов разрабатываются для ИС в целом или для всех ее сегментов или устройств в отдельности и фиксируются в организационно-распорядительной документации по защите информации (документируются).

15.3. Установка (инсталляция) в ИС программного обеспечения и (или) его компонентов должна осуществляться только от имени администратора.

15.4. Администратором ИС должен обеспечиваться периодический контроль установленного (инсталлированного) в ИС программного обеспечения на предмет соответствия его перечню программного обеспечения, разрешенному к установке в ИС, а также на предмет отсутствия программного обеспечения, запрещенного к установке.

Начальник управления информатизации
и связи администрации муниципального
образования городской округ
город-курорт Сочи Краснодарского края Н.Р.Лавриенко

Департамент муниципальной службы и кадровой политики

Приложение № 13
к распоряжению администрации
муниципального образования городской
округ город-курорт Сочи
Краснодарского края
от 16.08.2021 № 300-р

ПОЛИТИКА
обеспечения безопасности удаленного доступа к информационным системам администрации муниципального образования городской округ город-курорт Сочи Краснодарского края

1. Общие положения

1.1. Политика обеспечения безопасности удаленного доступа к информационным системам администрации муниципального образования городской округ город-курорт Сочи Краснодарского края (далее – Политика) разработана на основе:

– Методического документа «Меры защиты информации в государственных информационных системах», утвержденного Федеральной службой технического и экспортного контроля России 11 февраля 2014 года;

– Постановления Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

1.2. Требования настоящей Политики распространяются на всех должностных лиц и муниципальных служащих администрации муниципального образования городской округ город-курорт Сочи Краснодарского края (далее – администрация города Сочи), являющихся пользователями информационных систем (далее – ИС).

1.3. Внесение изменений в настоящую Политику осуществляется на периодической и внеплановой основе:

– пересмотр положений настоящей Политики должен осуществляться не реже одного раза в 24 месяца;

– внеплановое внесение изменений может проводиться в случае приобретения новых средств защиты, существенно изменяющих порядок работы с ними, либо по результатам контрольных мероприятий.

1.4. Ответственным за внесение изменений в настоящую Политику является ответственный за обеспечение безопасности информационных систем.

1.5. Ответственность за выполнение положений настоящей Политики возлагается на администратора ИБ. Ответственность за несоблюдение требований настоящей Политики, повлекших за собой разглашение или утрату информации ограниченного доступа, определяется законодательством Российской Федерации, а также должностными инструкциями муниципальных служащих администрации города Сочи.

1.6. Ответственность за общий контроль выполнения требований данной Политики возлагается на ответственного за обработку и защиту персональных данных.

2. Обеспечение безопасности удаленного доступа

2.1. Под удаленным доступом к ресурсам ИС администрации города Сочи понимаются все виды доступа, осуществляемые по внешним каналам связи и с использованием устройств доступа, расположенных за пределами контролируемой зоны.

2.2. Решение о предоставлении удаленного доступа муниципальному служащему администрации города Сочи должно быть обосновано служебной необходимостью.

2.3. Удаленный доступ к ресурсам ИС предоставляется муниципальным служащим администрации города Сочи на основании заявки (приложение № 1).

2.4. Удаленный доступ к ресурсам ИС администрации города Сочи предоставляется муниципальным служащим администрации города Сочи только после прохождения ими специального инструктажа, проводимого администратором ИБ.

2.5. Муниципальные служащие администрации города Сочи, которым предоставляется удаленный доступ, несут персональную ответственность за использование предоставляемого доступа только по назначению с соблюдением требований безопасности, устанавливаемых настоящей Политикой и иными внутренними нормативными документами администрации города Сочи.

2.6. Муниципальные служащие, получившие удалённый доступ, обязаны принимать меры по недопущению использования своих компьютеров посторонними лицами для осуществления удаленного доступа к ресурсам ИС администрации города Сочи.

2.7. Для подтверждения подлинности удаленных пользователей должны использоваться надежные схемы аутентификации, предусматривающие использование одноразовых паролей или криптографических ключей и защищенные от прослушивания сетевых каналов потенциальными злоумышленниками.

3. Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети

3.1. Администрацией города Сочи должна обеспечиваться защита информации при доступе пользователей (процессов запускаемых от имени пользователей) и (или) иных субъектов доступа к объектам доступа ИС через информационно-телекоммуникационные сети, в том числе сети связи общего пользования, с использованием стационарных и (или) мобильных технических средств (защита удаленного доступа).

3.2. Защита удаленного доступа должна обеспечиваться при всех видах доступа (беспроводной, проводной (коммутируемый), широкополосный и иные виды доступа) и включает:

– установление (в том числе документальное) видов доступа, разрешенных для удаленного доступа к объектам доступа ИС;

– ограничение на использование удаленного доступа в соответствии с задачами (функциями) ИС, для решения которых такой доступ необходим, и предоставление удаленного доступа для каждого разрешенного вида удаленного доступа;

– предоставление удаленного доступа только тем пользователям, которым он необходим для выполнения установленных должностных обязанностей (функций);

– мониторинг и контроль удаленного доступа на предмет выявления несанкционированного удаленного доступа к объектам доступа ИС;

– контроль удаленного доступа пользователей (процессов запускаемых от имени пользователей) к объектам доступа ИС до начала информационного взаимодействия с ИС (передачи защищаемой информации).

Начальник управления информатизации
и связи администрации муниципального
образования городской округ город-
курорт Сочи Краснодарского края Н.Р.Лавриенко

Приложение № 1
к Политике обеспечения безопасности
удаленного доступа к информационным
системам администрации
муниципального образования городской
округ город-курорт Сочи
Краснодарского края

_____

ЗАЯВКА
на предоставление удаленного доступа

Прошу предоставить удаленный доступ к информационным ресурсам

_____
_____
(перечень информационных ресурсов)

для решения задач:

_____
_____
_____
_____

следующим пользователям:

_____
_____
_____
(фамилия, имя, отчество)

_____ _____
(наименование должности) (наименование отдела)

«___» _____ 20__ г. _____ _____
(подпись) (Фамилия, инициалы)

Приложение № 14
к распоряжению администрации
муниципального образования городской
округ город-курорт Сочи
Краснодарского края
от 16.08.2021 № 300-р

ПРАВИЛА
организации антивирусной защиты в информационных системах администрации муниципального образования городской округ город курорт Сочи Краснодарского края

1. Общие положения

1.1. Настоящие правила определяют требования к организации защиты информации в информационных системах администрации муниципального образования городской округ город курорт Сочи Краснодарского края, а также отраслевых (функциональных) и территориальных органов администрации муниципального образования городской округ город курорт Сочи Краснодарского края (далее – ИС) от разрушающего воздействия компьютерных вирусов и устанавливают ответственность работников, эксплуатирующих и сопровождающих информационные системы, за их выполнение.

1.2. Настоящие правила разработаны на основании:

– Приказа Федеральной службы по техническому и экспертному контролю России (далее – ФСТЭК России) от 11 февраля 2013 года № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

– Методического документа от 11 февраля 2014 года «Меры защиты информации в государственных информационных системах».

1.3. К использованию в ИС допускаются только сертифицированные антивирусные средства с действующим сертификатом соответствия ФСТЭК России и/или Федеральной службы безопасности России.

1.4. В случае необходимости использования сторонних антивирусных средств, их применение необходимо согласовывать с администратором информационной безопасности (далее – ИБ).

1.5. Установка средств антивирусного контроля на АРМ и сервера ИС осуществляется уполномоченными работниками. Контроль настройки параметров средств антивирусного контроля осуществляет администратор ИБ в соответствии с руководствами по применению конкретных антивирусных средств.

2. Применение средств антивирусного контроля

2.1. Антивирусный контроль всех дисков и файлов ИС должен проводиться в автоматическом режиме по заданному расписанию (периодическое сканирование или мониторинг).

2.2. Файлы, помещенные в электронный архив должны в обязательном порядке проходить антивирусный контроль.

2.3. Периодически, раз в неделю, должен проводиться полный антивирусный контроль всех дисков и файлов ИС (сканирование).

2.4. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая информация на съемных носителях (CD-диск, flash-носители и т.п.). Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

2.5. В случае установки (изменения) программного обеспечения компьютера должна быть выполнена антивирусная проверка жестких дисков ИС лицом, установившим (изменившим) программное обеспечение.

3. Действия работников при подозрении наличия компьютерного вируса

3.1. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь самостоятельно или вместе с администратором ИБ должен провести внеочередной антивирусный контроль АРМ или серверов ИС. При необходимости он должен привлечь администратора ИБ для определения факта наличия или отсутствия компьютерного вируса.

3.2. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан:

– приостановить работу;

– немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя подразделения и администратора ИБ, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;

– совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;

– провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта привлечь администратора ИБ);

– в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, передать зараженный вирусом файл на съемном носителе администратору ИБ для дальнейшей передачи его в организацию-производитель антивирусных средств;

– по факту обнаружения зараженных вирусом файлов составить служебную записку администратору ИБ, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного

файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.

4. Порядок обновления антивирусных баз

4.1. Обновление антивирусных баз должно проводиться регулярно, в автоматическом режиме, по мере выхода новых антивирусных баз.

4.2. При согласовании с администратором ИБ ответственные за установку, модификацию и техническое обслуживание программного обеспечения могут отложить процедуру обновления антивирусных баз.

5. Ответственность

5.1. Ответственность за проведение мероприятий антивирусного контроля в подразделении и соблюдение требований настоящие правила возлагается на администратора ИБ, администратора ИС и всех пользователей ИС.

5.2. Периодический контроль за состоянием антивирусной защиты в ИС, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящих правил работниками отраслевых (функциональных), территориальных органов администрации муниципального образования городской округ город-курорт Сочи Краснодарского края осуществляется администратором ИБ.

Начальник управления информатизации
и связи администрации муниципального
образования городской округ
город-курорт Сочи Краснодарского края Н.Р.Лавриенко

Приложение № 15
к распоряжению администрации
муниципального образования городской
округ город-курорт Сочи
Краснодарского края
от 16.08.2021 № 300-р

ПРАВИЛА
по внесению изменений в списки пользователей и наделению их полномочиями доступа к ресурсам информационных систем администрации муниципального образования городской округ город-курорт Сочи Краснодарского края

1. Порядок использования учетных записей пользователей

1.1. С целью соблюдения принципа персональной ответственности за свои действия каждому работнику администрации муниципального образования городской округ город-курорт Сочи Краснодарского края, допущенному к работе с информационными системами (далее – ИС), должно быть сопоставлено персональное уникальное имя (учетная запись пользователя ИС), под которым он будет работать в системе. В случае производственной необходимости, некоторым работникам могут быть сопоставлены несколько уникальных имен (учетных записей).

1.2. Использование несколькими работниками при самостоятельной работе в ИС одного и того же имени пользователя запрещено.

2. Процедура регистрации учетных записей пользователей

2.1. Процедура регистрации (создания учетной записи) пользователя и предоставления (или прекращения) ему прав доступа к конкретным ресурсам ИС инициируется распоряжением о назначении муниципального служащего на должность и/или заявкой руководителя отраслевого (функционального), территориального органа администрации муниципального образования городской округ город-курорт Сочи Краснодарского края, в котором работает данный работник, на имя начальника управления информатизации и связи администрации муниципального образования городской округ город-курорт Сочи Краснодарского края (приложение № 1).

2.2. В заявке указывается:

– должность (с указанием отраслевого (функционального), территориального органа);

– фамилия, имя и отчество работника;

– основание для предоставления (прекращения) доступа (приказ, распоряжение);

– имя компьютера с которого будет осуществляться доступ к информационным ресурсам;

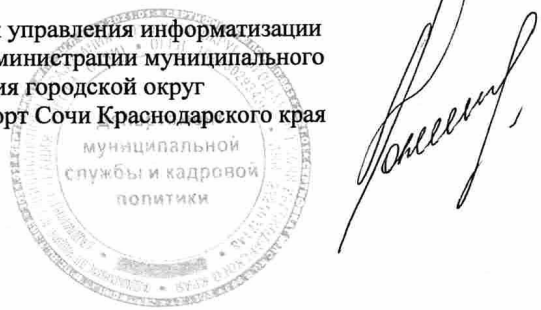
– содержание запрашиваемых изменений.

Заявку подписывает руководитель отраслевого (функционального), территориального органа администрации муниципального образования городской округ город-курорт Сочи Краснодарского края, утверждая тем самым производственную необходимость допуска (изменения прав доступа) данного работника к необходимым ресурсам ИС для решения им указанных задач.

На основании заявки (задания) ответственный за создание учетных записей производит необходимые операции по созданию (отключению) учетной записи пользователя, присвоению ему начального значения пароля и заявленных прав доступа к ресурсам ИС, включению его в соответствующие задачам группы пользователей и другие необходимые действия. Для всех пользователей должен быть установлен режим принудительного запроса смены пароля в соответствии с правилами по парольной защите.

Работнику, зарегистрированному в качестве нового пользователя системы, сообщается имя соответствующего ему пользователя, при необходимости выдается персональный аппаратный идентификатор и начальное значение пароля, которое он обязан сменить при первом входе в систему.

Начальник управления информатизации
и связи администрации муниципального
образования городской округ
город-курорт Сочи Краснодарского края Н.Р.Лавриенко



Приложение № 1
к Правилам по внесению изменений в
списки пользователей и наделению их
полномочиями доступа к ресурсам
информационных систем администрации
муниципального образования городской
округ город-курорт Сочи
Краснодарского края

Пример заявки на внесение изменений в списки пользователей

ЗАЯВКА
на доступ, прекращение доступа к информационным ресурсам
администрации муниципального образования городской округ город-курорт
Сочи Краснодарского края

_____
(должность с указанием отраслевого (функционального), территориального органа)
_____
(фамилия имя и отчество работника)
_____
(Основание (приказ, распоряжение))
_____
(Имя компьютера с которого будет осуществляться доступ к информационным ресурсам)

Наименование конкретной информационной системы (ресурса):

Допустить:
1. _____
2. _____
3. _____
4. _____
5. _____
6. _____

для решения задач: _____
_____
_____
_____

Прекратить доступ:
1. _____
2. _____
3. _____
4. _____
5. _____
6. _____

Директор департамента
(Начальник управления) ФИО

Приложение № 16
к распоряжению администрации
муниципального образования городской
округ город-курорт Сочи
Краснодарского края
от 16.08.2021 № 300-р

ПОЛИТИКА
управления изменениями программного обеспечения и технических средств в информационных системах администрации муниципального образования городской округ город-курорт Сочи Краснодарского края

1. Общие положения

1.1. Политика управления изменениями программного обеспечения и технических средств в информационной системе администрации муниципального образования городской округ город-курорт Сочи Краснодарского края (далее – Политика) разработана на основе:

– Приказа Федеральной службы по техническому и экспертному контролю России (далее – ФСТЭК России) от 11 февраля 2013 года № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

– Методического документа от 11 февраля 2014 года «Меры защиты информации в государственных информационных системах».

1.2. Настоящая Политика определяет организационно-техническое обеспечение процессов проведения работ по установке, модификации и техническому обслуживанию программного обеспечения (далее – ПО) и технических средств (далее – ТС) в информационной системе администрации муниципального образования городской округ город-курорт Сочи Краснодарского края.

1.3. Настоящей Политикой в своей работе должны руководствоваться все пользователи ИС.

1.4. Внесение изменений в настоящую Политику осуществляется на периодической и внеплановой основе:

– пересмотр положений настоящей Политики должно осуществляться не реже одного раза в 12 месяцев;

– внеплановое внесение изменений может проводиться по результатам проведения контрольных мероприятий.

1.5. Ответственным за внесение изменений в настоящую Политику является администратор информационной безопасности (далее – ИБ).

1.6. Ответственность за выполнение положений настоящей Политики несут все пользователи ИС. Ответственность муниципального служащего администрации муниципального образования городской округ город-курорт Сочи Краснодарского края за несоблюдение требований настоящей политики, повлекших за собой разглашение или утрату информации ограниченного

доступа, определяется законодательством Российской Федерации, а также должностными инструкциями муниципальных служащих администрации муниципального образования городской округ город-курорт Сочи Краснодарского края.

1.7. Контроль за выполнением требований данной Политики осуществляет ответственный администратор ИБ путем проведения регулярных контрольных мероприятий.

2. Порядок учета технических средств ВТ

2.1. В ИС осуществляется учет технических средств вычислительной техники (далее – средства ВТ).

2.2. Учет средств ВТ ведется по Перечням муниципального имущества вычислительной техники отдельно на каждый отраслевой (функциональный) орган администрации муниципального образования городской округ город-курорт Сочи Краснодарского края (далее – Перечень имущества ВТ).

2.3. Перечни имущества ВТ отрабатываются отделом информационно-технического сопровождения МКУ «Электронный Сочи» совместно с представителем отраслевого (функционального) органа администрации муниципального образования город-курорт Сочи Краснодарского края, в котором размещаются технические средства вычислительной техники и утверждаются руководителем соответствующего отраслевого (функционального) органа муниципального образования городской округ город-курорт Сочи Краснодарского края.

Перечень имущества ВТ отрабатывается в 2-х экземплярах на каждый отраслевой (функциональный) орган администрации муниципального образования город-курорт Сочи Краснодарского края. Первый экземпляр хранится в отраслевом (функциональном) органе муниципального образования городской округ город-курорт Сочи Краснодарского края, второй экземпляр передается в отдел информационно-технического сопровождения МКУ «Электронный Сочи» (приложение № 1).

2.4. Уточнение Перечней имуществ ВТ проводится ежегодно в период проведения инвентаризации, а также при перемещении (поставке (приобретении) или списании) любого оборудования входящего в состав имущества ВТ.

3. Порядок закрепления за пользователем и списания с пользователя средств ВТ

3.1. В ИС устанавливается персональная ответственность пользователей за сохранность используемых ими средств ВТ.

3.2. При приеме на работу работника отраслевого (функционального) органа администрации муниципального образования городской округ город-курорт Сочи Краснодарского края (далее – пользователь) и в случае, если должностной инструкцией по занимаемой им должности предусматривается работа на персональном компьютере за пользователем закрепляются средства ВТ.

3.3. Прием-передача средств ВТ оформляется актом, который составляется в двух экземплярах, первый выдается пользователю, получившему средства ВТ, второй хранится в отделе информационно-технического сопровождения МКУ «Электронный Сочи» (приложение № 2).

3.4. При увольнении пользователя (переводе на другую должность) отметка о сдаче средств ВТ производится в том же акте, и средства ВТ списываются с пользователя.

3.5. Пользователь получивший средства ВТ несет персональную ответственность за сохранность вверенных ему средств ВТ.

4. Порядок управления изменениями программного обеспечения и состава технических средств ВТ

4.1. В ИС определены типы возможных изменений программного обеспечения и технических средств.

4.2. Все изменения программного обеспечения и технических средств должны быть санкционированы, проводиться только на основании заявок руководителей отраслевых (функциональных), территориальных органов администрации муниципального образования городской округ город-курорт Сочи Краснодарского края, согласованных с администратором ИБ.

4.3. Если изменяемые ПО и ТС входят в состав аттестованных по требованиям безопасности информации ИС, необходимо уведомить об осуществленных изменениях производившую аттестацию организацию, которая принимает решение о необходимости проведения контроля эффективности объекта информатизации.

4.4. Все изменения конфигурации технических и программных средств, входящих в состав аттестованных по требованиям безопасности ИС, отражаются в Техническом паспорте объекта информатизации.

4.5. Процедура перемещения (изменения состава) технических средств инициируется производственной необходимостью и заявкой начальника подразделения, от которого (к которому) перемещаются технические средства, на имя начальника управления информатизации и связи администрации муниципального образования городской округ город-курорт Сочи Краснодарского края (приложение № 3).

4.6. В заявке указывается:

– место расположения АРМ, с указанием ответственного пользователя;

– состав АРМ до переезда;

– место нового расположения АРМ, с указанием нового ответственного пользователя;

– состав АРМ после переезда;

– содержание запрашиваемых изменений.

Заявку подписывает руководитель органа администрации муниципального образования городской округ город-курорт Сочи Краснодарского края, в котором расположен АРМ утверждая тем самым производственную необходимость перемещения АРМ.

На основании заявки специалист отдела информационно-технического сопровождения МКУ «Электронный Сочи» совместно с новым пользователем АРМ производит необходимые операции по перемещению и переименованию АРМ. Специалистом отдела технического сопровождения систем информационной безопасности МКУ «Электронный Сочи» вносятся соответствующие изменения в раздел «Учет АРМ» и проверка наличия и правильности настройки средств защиты информации, после чего АРМ допускается к обработке информации новым пользователем.

4.7. Право внесения изменений в конфигурацию аппаратно-программных средств ИС администрации муниципального образования городской округ город-курорт Сочи Краснодарского края предоставляется администраторам ИС, администратором ИБ. Изменение конфигурации аппаратно-программных средств рабочих станций и серверов кем-либо без согласования с администратором ИБ запрещено.

4.8. Любые изменения программного обеспечения и технических средств должны производиться в соответствии с эксплуатационной документацией.

4.9. Установка (обновление) ПО на средствах вычислительной техники производится с эталонных копий программных средств, хранящихся у администратора ИС.

4.10. Все добавляемые программные и аппаратные компоненты должны быть предварительно проверены на работоспособность, а также отсутствие вредоносного программного кода.

4.11. Любые действия по изменению программного обеспечения и состава технических средств должны быть документированы.

4.12. Пользователи, нарушившие требования настоящих правил, несут ответственность, в соответствии с действующим законодательством Российской Федерации и локальными нормативными актами администрации муниципального образования городской округ город-курорт Сочи Краснодарского края.

Начальник управления информатизации
и связи администрации муниципального
образования городской округ
город-курорт Сочи Краснодарского края Н.Р.Лавриенко

Приложение № 1
к Политике управления изменениями программного обеспечения и технических средств в информационной системе администрации муниципального образования городской округ город-курорт Сочи Краснодарского края

Экз. № ___

УТВЕРЖДАЮ
Руководитель отраслевого (функционального) органа администрации муниципального образования городской округ город-курорт Сочи Краснодарского края

_____ И.О. Фамилия
«____» _____ 2021 г

Перечень муниципального имущества вычислительной техники расположенного по адресу: _____, находящегося в оперативном управлении муниципального казенного учреждения города Сочи «Электронный Сочи»:

№ п\п	Тип технических средств и систем	Наименование технических средств и систем объекта информатизации	Инвентарный номер
ул. Советская д. 26 каб. 2			
Sov26-2-001			
1	Монитор	МОНИТОР 23.8" Acer EK240YAbi Black	MZ6516
	Системный блок	Системный блок Micro Lana i5 / 8GB DDR4/ SSD 480GB	MZ6643
	Принтер	CANON 2900 (A4/ 12стр/мин. 600qpi. USB2.0)	A00662
Sov26-2-002			
2	Монитор	МОНИТОР Samsung 24	2016101340000041
	Системный блок	Системный блок Micro Lana i5 / 8GB DDR4/ SSD 480GB	MZ6644
Количество автоматизированных рабочих мест (АРМ) в кабинете: 2 шт.			
ул. Советская д. 26 каб. 3			
Sov26-3-001			
1	Монитор	МОНИТОР 23.8" Acer EK240YAbi Black	MZ6516
	Системный блок	Системный блок Micro Lana i5 / 8GB DDR4/ SSD 480GB	MZ6643
	Принтер	CANON 2900 (A4/ 12стр/мин. 600qpi. USB2.0)	A00662
Sov26-2-002			

№ п\п	Тип технических средств и систем	Наименование технических средств и систем объекта информатизации	Инвентарный номер
2	Монитор	МОНИТОР Samsung 24	2016101340000041
	Системный блок	Системный блок Micro Lana i5 / 8GB DDR4/ SSD 480GB	MZ6644
Sov26-2-003			
3	Монитор	Монитор 22 HP LA2245wg	MZ2343
	Системный блок	Системный блок Micro Lana i5 / 8GB DDR4/ SSD 480GB	MZ6645
	МФУ	МФУ Brother MFC-L2740DWR	2020101340000172
Количество автоматизированных рабочих мест (АРМ) в кабинете: 3 шт.			
Количество автоматизированных рабочих мест (АРМ) в отраслевом (функциональном) органе: 5 шт.			

Оборудование находится в исправном состоянии.

Представитель отраслевого (функционального) органа муниципального образования городской округ город-курорт Сочи Краснодарского края

_____ И.О. Фамилия

Ответственный работник
МКУ «Электронный Сочи»

_____ И.О. Фамилия

Приложение № 2
к Политике управления изменениями программного обеспечения и технических средств в информационной системе администрации муниципального образования городской округ город-курорт Сочи Краснодарского края

Экз. № ___

Акт
приема-передачи средств вычислительной техники

г. Сочи **«___» _____ 20 ___ г.**

Настоящий акт составлен в том, что **[указать должность ФИО (работника МКУ)]** передал, а **[указать должность ФИО(пользователя)]** принял средства ВТ установленные в _____ в составе:
(адрес с указанием номера кабинета)

№ п\п	Тип технических средств и систем	Наименование технических средств и систем объекта информатизации	Инвентарный (серийный) номер
		Sov26-2-001	
1	Монитор	МОНИТОР 23.8" Acer EK240YAbi Black	MZ6516
	Системный блок	Системный блок Micro Lana i5 / 8GB DDR4/ SSD 480GB	MZ6643
	ЖМД	WD 240GB Green	2L0529SHD6NY
	Клавиатура	Logitech	б/н
	Мышь	Logitech	б/н
	Принтер	CANON 2900 (A4/ 12стр/мин. 600qpi. USB2.0)	A00662

Оборудование находится в исправном состоянии.

Несогласованное внесение изменений в состав средств ВТ **ЗАПРЕЩЕНО!!!**

Несогласованное перемещение средств ВТ за пределы кабинета **ЗАПРЕЩЕНО!!!**

Сдал:
Ответственный работник
МКУ «Электронный Сочи»
_____ И.О. Фамилия

Принял:
Пользователь отраслевого (функционального) органа
муниципального образования городской округ город-курорт
Сочи Краснодарского края
_____ И.О. Фамилия

Отметка об обратном приеме:
Ответственный работник
МКУ «Электронный Сочи»
«___» _____ 20___ г. _____ И.О. Фамилия

Приложение № 3
к Политике управления изменениями программного обеспечения и технических средств в информационной системе администрации муниципального образования городской округ город-курорт Сочи Краснодарского края

Пример заявки на перемещение АРМ

Уважаемый….

[Наименование органа] в связи с производственной необходимостью просит Вас согласовать перемещение автоматизированных рабочих мест (далее – АРМ) пользователей в количестве __ шт, с адреса: **[Указать адрес месторасположения АРМ с точностью до этажа и кабинета]** в составе, указанным в таблице № 1.

Таблица № 1 – Состав АРМ до переезда

№ п\п	Наименование (модель) технических средств и систем объекта информатизации		Заводской (серийный) или инвентарный номер	ФИО пользователя АРМ
	[Имя АРМ]			
1	Системный блок	**[Указать наименование модели]**	**[Указать заводской/инвентарный номер]**	**[Указать ФИО пользователя АРМ]**
2	Монитор	**[Указать наименование модели]**	**[Указать заводской/инвентарный номер]**	
3	Клавиатура	**[Указать наименование модели]**	**[Указать заводской/инвентарный номер]**	
4	Мышь	**[Указать наименование модели]**	**[Указать заводской/инвентарный номер]**	
5	Монитор	**[Указать наименование модели]**	**[Указать заводской/инвентарный номер]**	
6	МФУ/Принтер	**[Указать наименование модели]**	**[Указать заводской/инвентарный номер]**	

АРМ планируется переместить по адресу: **[Указать адрес месторасположения АРМ с точностью до этажа и кабинета]**. В процессе перемещения состав программного обеспечения АРМ (том числе средства защиты информации, установленные на АРМ) изменению не подлежит.

[Выбрать один из вариантов]

В процессе перемещения, состав АРМ не изменится и будет соответствовать составу, указанному в таблице № 1.

В процессе перемещения, состав АРМ подлежит изменению и будет соответствовать составу, указанному в таблице № 2.

Таблица №2 – Состав АРМ после переезда

№ п\п	Наименование (модель) технических средств и систем объекта информатизации		Заводской (серийный) или инвентарный номер	ФИО пользователя АРМ
[Имя АРМ]				
1	Системный блок	**[Указать наименование модели]**	**[Указать заводской/инвентарный номер]**	**[Указать ФИО нового пользователя АРМ]**
2	Монитор	**[Указать наименование модели]**	**[Указать заводской/инвентарный номер]**	
3	Клавиатура	**[Указать наименование модели]**	**[Указать заводской/инвентарный номер]**	
4	Мышь	**[Указать наименование модели]**	**[Указать заводской/инвентарный номер]**	
5	Монитор	**[Указать наименование модели]**	**[Указать заводской/инвентарный номер]**	
6	МФУ/Принтер	**[Указать наименование модели]**	**[Указать заводской/инвентарный номер]**	

Директор департамента
(Начальник управления) ФИО

Приложение № 17
к распоряжению администрации муниципального образования городской округ
город-курорт Сочи Краснодарского края от 16.08.2021 № 300-р

ПЛАН

мероприятий по защите информации в информационных системах администрации муниципального образования городской округ город-курорт Сочи Краснодарского края

№ п/п	Наименование мероприятия	Срок выполнения	Ответственный за выполнение	Примечание
1	Классификация информационных систем	3 квартал 2021 года	Начальник управления информатизации и связи администрации муниципального образования городской округ город-курорт Сочи Краснодарского края Н.Р. Лавриенко	Проводится при создании информационной системы, при выявлении в информационных системах наличия защищаемой информации (в том числе персональных данных), при изменении состава, структуры самой информационной системы или технических особенностей ее построения
2	Выявление угроз безопасности и разработка модели угроз	3 квартал 2021 года	Заместитель начальника управления информатизации и связи администрации муниципального образования городской округ город-курорт Сочи Краснодарского края, начальник отдела информатизации и информационной безопасности управления информатизации и связи администрации муниципального образования городской округ город-курорт Сочи Краснодарского края Е.Н. Осипова	

№ п/п	Наименование мероприятия	Срок выполнения	Ответственный за выполнение	Примечание
3	Проверка сведений, содержащихся в уведомлении	ежеквартально	Заместитель начальника управления информатизации и связи администрации муниципального образования городской округ город-курорт Сочи Краснодарского края, начальник отдела информатизации и информационной безопасности управления информатизации и связи администрации муниципального образования городской округ город-курорт Сочи Краснодарского края Е.Н. Осипова	По необходимости, в Роскомнадзор отправляется измененная версия уведомления
4	Документальное регламентирование работы с защищаемой информацией	3 квартал 2021 года	Заместитель начальника управления информатизации и связи администрации муниципального образования городской округ город-курорт Сочи Краснодарского края, начальник отдела информатизации и информационной безопасности управления информатизации и связи администрации муниципального образования городской округ город-курорт Сочи Краснодарского края Е.Н. Осипова	Необходимо разработать документы, распределяющие и закрепляющие ответственность за обработку защищаемой информации

№ п/п	Наименование мероприятия	Срок выполнения	Ответственный за выполнение	Примечание
5	Проведение первичного инструктажа по вопросам обработки персональных данных с работниками, принимаемыми на работу в администрацию муниципального образования городской округ город-курорт Сочи Краснодарского Края с осуществлением ознакомления работников с положениями законодательства Российской Федерации о персональных данных	Постоянно	Заместитель начальника отдела кадров департамента муниципальной службы и кадровой политики администрации муниципального образования городской округ город-курорт Сочи Краснодарского края Н.А. Раева	Необходимо проводить отдельный инструктаж по обработке персональных данных с принимающимися на работу работниками
6	Обучение работников, непосредственно осуществляющих обработку защищаемой информации, правилам работы с ней	Ежегодно	Заместитель начальника управления информатизации и связи администрации муниципального образования городской округ город-курорт Сочи Краснодарского края, начальник отдела информатизации и информационной безопасности управления информатизации и связи администрации муниципального образования городской округ город-курорт Сочи Краснодарского края Е.Н. Осипова	Необходимо проводить отдельный инструктаж по обработке защищаемой информации с принимаемыми на работу работниками
7	Оценка соответствия эффективности принимаемых мер по обеспечению безопасности персональных данных в ИС администрации муниципального образования городской округ город-курорт Сочи Краснодарского края в форме аттестации	4 квартал 2021 года	Начальник управления информатизации и связи администрации муниципального образования городской округ город-курорт Сочи Краснодарского края Н.Р. Лавриенко	Проводится организацией – лицензиатом ФСТЭК России

№ п/п	Наименование мероприятия	Срок выполнения	Ответственный за выполнение	Примечание
8	Пересмотр договоров с субъектами и контрагентами в части обработки персональных данных, получение письменного согласия субъекта на обработку персональных данных	Постоянно, при заключении новых договоров	Начальник управления муниципальных закупок администрации муниципального образования городской округ город-курорт Сочи Краснодарского края К.Г. Ярыш	В договоры должны быть включены согласия субъекта на обработку и передачу его персональных данных
9	Уничтожение персональных данных и иной защищаемой информации	При достижении целей обработки персональных данных	Ответственные лица отраслевых (функциональных), территориальных органов администрации муниципального образования городской округ город-курорт Сочи Краснодарского края	
10	Сопровождение заявок на предоставление доступа к ресурсам информационных систем	Постоянно	Директор МКУ «Электронный Сочи» С.А. Лугачев	
11	Повышение квалификации работников в области защиты информации	Раз в пять лет	Начальник управления информатизации и связи администрации муниципального образования городской округ город-курорт Сочи Краснодарского края Н.Р. Лавриенко	Работники, ответственные за организацию защиты информации и обеспечение безопасности информационных систем – не менее одного раза в два года. Повышение осведомленности работников, обрабатывающих защищаемую информацию – постоянно (обучение может проводить ответственный за организацию защиты информации)

№ п/п	Наименование мероприятия	Срок выполнения	Ответственный за выполнение	Примечание
12	Контроль эффективности защиты информации	Раз в два года	Начальник управления информатизации и связи администрации муниципального образования городской округ город-курорт Сочи Краснодарского края Н.Р. Лавриенко	

Начальник управления информатизации
и связи администрации муниципального
образования городской округ город-
курорт Сочи Краснодарского края Н.Р.Лавриенко

Приложение № 18
к распоряжению администрации
муниципального образования городской
округ город-курорт Сочи
Краснодарского края
от 16.08.2021 № 300-р

ПОЛИТИКА
защиты технических средств информационных систем администрации муниципального образования городской округ город-курорт Сочи Краснодарского края

1. Общие положения

1.1. Политика защиты технических средств администрации муниципального образования городской округ город-курорт Сочи Краснодарского края, а также должностных лиц и муниципальных служащих отраслевых (функциональных) и территориальных органов администрации муниципального образования городской округ город-курорт Сочи Краснодарского края (далее – Политика) разработана в соответствии с:

– Приказом Федеральной службы по техническому и экспертному контролю России (далее – ФСТЭК России) от 11 февраля 2013 года № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

– Методическим документом от 11 февраля 2014 года «Меры защиты информации в государственных информационных системах».

1.2. Требования настоящей Политики распространяются на всех должностных лиц и муниципальных служащих администрации муниципального образования городской округ город-курорт Сочи Краснодарского края, должностных лиц и муниципальных служащих отраслевых (функциональных) и территориальных органов администрации муниципального образования городской округ город-курорт Сочи Краснодарского края (далее – пользователи), являющихся пользователями информационных систем (далее – ИС).

1.3. Внесение изменений в настоящую Политику осуществляется на периодической и внеплановой основе:

– пересмотр положений настоящей Политики должен осуществляться не реже одного раза в 12 месяца;

– внеплановое внесение изменений может проводиться в случае приобретения администрацией муниципального образования городской округ город-курорт Сочи Краснодарского края новых средств защиты, существенно изменяющих порядок работы с ними, либо по результатам контрольных мероприятий.

1.4. Ответственным за внесение изменений в настоящую Политику является ответственный за обеспечение безопасности информации – администратор информационной безопасности (далее – ИБ).

1.5. Ответственность за выполнение положений настоящей Политики возлагается на администратора ИБ. Ответственность за несоблюдение требований настоящей Политики, повлекших за собой разглашение или утрату информации ограниченного доступа, определяется законодательством РФ, а также должностными инструкциями работников администрации муниципального образования городской округ город-курорт Сочи Краснодарского края.

1.6. Ответственность за общий контроль выполнения требований данной Политики возлагается на администратора ИБ.

2. Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования

2.1. В ИС должна обеспечиваться контролируемая зона, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования.

2.2. Контролируемая зона включает пространство (территорию, здание, часть здания), в котором исключено неконтролируемое пребывание муниципальных служащих (сотрудников) администрации муниципального образования городской округ город-курорт Сочи Краснодарского края и лиц, не имеющих постоянного допуска на объекты информационной системы, а также транспортных, технических и иных материальных средств.

2.3. Границами контролируемой зоны могут являться периметр охраняемой территории, ограждающие конструкции охраняемого здания или охраняемой части здания, если оно размещено на неохраняемой территории. Границы контролируемой зоны устанавливаются в организационно-распорядительных документах по защите информации.

2.4. Для одной информационной системы (ее сегментов) может быть организовано несколько контролируемых зон.

3. Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены

3.1. В ИС должны обеспечиваться контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам

обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены.

3.2. Контроль и управление физическим доступом должны предусматривать:

– определение лиц, допущенных к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены;

– санкционирование физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены;

– учет физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены.

4. Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр

4.1. В ИС должно осуществляться размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр.

4.2. В качестве устройств вывода (отображения) информации в информационной системе следует рассматривать экраны мониторов автоматизированных рабочих мест пользователей, мониторы консолей управления технических средств (серверов, телекоммуникационного оборудования и иных технических средств), видеопанели, видеостены и другие средства визуального отображения защищаемой информации, печатающие устройства (принтеры, плоттеры и иные устройства), аудиоустройства, многофункциональные устройства.

4.3. Размещение устройств вывода (отображения, печати) информации должно исключать возможность несанкционированного просмотра выводимой информации, как из-за пределов контролируемой зоны, так и в пределах контролируемой зоны. Не следует размещать устройства вывода (отображения, печати) информации напротив оконных проемов, входных дверей, технологических отверстий, в коридорах, холлах и иных местах, доступных для несанкционированного просмотра.

Начальник управления информатизации
и связи администрации муниципального
образования городской округ
город-курорт Сочи Краснодарского края Н.Р.Лавриенко

Приложение № 19
к распоряжению администрации
муниципального образования городской
округ город-курорт Сочи
Краснодарского края
от 16.08.2021 № 300-р

ИНСТРУКЦИЯ
об осуществлении контроля выполнения требований по защите персональных данных в администрации муниципального образования городской округ город-курорт Сочи Краснодарского края

1. Общие положения

Настоящая инструкция разработана в соответствии с положениями Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», «Перечнем 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», утверждённым постановлением Правительства Российской Федерации от 21 марта 2012 года № 211, и определяет порядок организации и осуществления контроля выполнения соответствия обработки персональных данных требованиям к защите персональных данных в администрации муниципального образования городской округ город-курорт Сочи Краснодарского края (далее – администрации города Сочи).

Правила обязательны для исполнения всеми должностными лицами администрации города Сочи, осуществляющими контроль состояния защиты персональных данных.

Контроль выполнения соответствия обработки персональных данных требованиям к защите персональных данных в администрации города Сочи осуществляется с целью определения наличия несоответствий между требуемым уровнем защиты персональных данных и его фактическим состоянием, правильности обработки персональных данных ответственными лицами в отраслевых (функциональных) и территориальных органах администрации муниципального образования городской округ город-курорт Сочи Краснодарского края (далее – органы), а также выработки мер по их устранению и недопущению в дальнейшем.

Контроль осуществляет ответственный за организацию обработки персональных данных в администрации города Сочи.

Контроль проводится в форме плановых и внеплановых проверок. Внеплановые проверки могут быть контрольными и по частным вопросам.

Контрольные проверки проводятся для установления полноты выполнения рекомендаций плановых проверок.

Проверки по частным вопросам охватывают отдельные направления по защите персональных данных и могут проводиться в случаях, когда стали известны факты несанкционированного доступа, утечки либо утраты

персональных данных субъектов администрации города Сочи или нарушения требований по обработке и защите персональных данных.

Проверки осуществляются ответственным за организацию обработки персональных данных в администрации города Сочи либо комиссией, образуемой главой муниципального образования городской округ город-курорт Сочи Краснодарского края.

Сроки проведения контрольных проверок доводятся руководителям проверяемых органов не позднее, чем за 24 часа до начала проверки.

Проверки по частным вопросам могут проводиться без уведомления руководителей проверяемых отраслевых (функциональных) или территориальных органов администрации города Сочи.

Периодичность и сроки проведения плановых проверок устанавливаются планом, утверждаемым главой города Сочи. Сроки проведения плановых проверок доводятся руководителям проверяемых отраслевых (функциональных) или территориальных органов администрации города Сочи не позднее, чем за 10 суток до начала проверки.

2. Порядок подготовки к проверке

Проверка проводится на основании распоряжения главы муниципального образования городской округ город-курорт Сочи Краснодарского края. Ответственный за организацию обработки персональных данных подготавливает предложения по составу комиссии, утверждаемом распоряжением администрации города Сочи.

Проверяющие лица обязаны получить у руководителей проверяемых органов информацию об условиях обработки персональных данных, необходимую для достижения целей проверки. Перед началом проверки они должны изучить материалы предыдущих проверок данного органа.

3. Порядок проведения проверки

В начале проведения проверки председатель комиссии прибывает к руководителю проверяемого органа.

Руководитель проверяемого органа обязан оказывать содействие комиссии по проверке и в случае необходимости определяет должностное лицо, ответственное за сопровождение проверки.

На период проведения контрольных мероприятий обработку персональных данных необходимо по возможности прекращать. Допуск проверяющих лиц к конкретным информационным ресурсам, защищаемым сведениям и техническим средствам должен исключать ознакомление проверяющих лиц с конкретными персональными данными.

Общий порядок проведения проверки включает следующее:

1) получение документов о распределении обязанностей по обработке и защите персональных данных, выявление ответственных за обработку и защиту персональных данных и установление факта ознакомления работников (служащих) проверяемого органа со своей ответственностью;

2) получение при содействии работников (служащих) проверяемого органа документов, касающихся обработки и защиты персональных данных в данном органе;

3) анализ полученной документации;

4) непосредственная проверка выполнения установленного порядка обработки и защиты персональных данных и требований законодательства Российской Федерации в области защиты персональных данных.

При этом согласовываются конкретные вопросы по объёму, содержанию, срокам проведения проверки, а также каких работников отраслевого (функционального), территориального органа необходимо привлечь к проверке и какие объекты следует посетить.

В ходе осуществления контроля выполнения требований по обработке и защите персональных данных в проверяемом органе рассматриваются, в частности, следующие показатели:

1) в части общей организации работ по обработке персональных данных:

а) соответствие информации, указанной в уведомлении об обработке персональных данных органа, реальному положению дел;

б) соответствие обрабатываемой и собираемой информации (персональных данных), их полнота, в соответствии с нормативными правовыми актами и локальными актами, принятыми в органе;

в) наличие нормативных документов по защите персональных данных;

г) знание нормативных документов работниками (служащими), имеющими доступ к персональным данным;

д) полнота и правильность выполнения требований нормативных документов органа работниками (служащими), имеющими доступ к персональным данным;

е) наличие документов, определяющих состав работников (служащих), ответственных за организацию защиты персональных данных в подразделении, соответствие этих документов реальному штатному составу подразделения, а также подтверждение факта ознакомления ответственных работников (служащих) с данными документами;

ж) уровень подготовки работников (служащих), ответственных за организацию защиты персональных данных в органе;

з) наличие согласий на обработку персональных данных субъектов персональных данных. Соответствие объёма персональных данных и сроков обработки целям обработки персональных данных.

2) в части защиты персональных данных в информационных системах персональных данных (далее – ИСПДн):

а) соответствие средств вычислительной техники ИСПДн показателям, указанным в документации на ИСПДн;

б) структура и состав локальных вычислительных сетей, организация разграничения доступа пользователей к сетевым информационным ресурсам, порядок защиты охраняемых сведений при передаче (обмене) персональных данных в сети передачи данных;

в) соблюдение установленного порядка использования средств вычислительной техники ИСПДн;

г) наличие и эффективность применения средств и методов защиты персональных данных, обрабатываемых на средствах вычислительной техники;

д) соблюдение требований, предъявляемых к паролям на информационные ресурсы;

е) соблюдение требований и правил антивирусной защиты средств вычислительной техники;

ж) контроль учёта носителей персональных данных;

з) тестирование реализации правил фильтрации межсетевого экрана, процесса регистрации, процесса идентификации и аутентификации запросов, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления настроек межсетевого экрана.

3) в части защиты информационных ресурсов и помещений:

а) правильность отнесения обрабатываемой информации к персональным данным;

б) правильность установления уровня защищенности персональных дынных в информационной системе;

в) закрепление гражданско-правовой ответственности в сфере информационной безопасности и соблюдения режима конфиденциальности персональных данных в правилах внутреннего трудового распорядка, положениях об органе и (или) подведомственных учреждений, должностных инструкциях работников (служащих) и трудовых договорах;

г) порядок передачи персональных данных органам государственной власти, местного самоуправления и сторонним организациям (контрагентам);

д) действенность принимаемых мер по защите охраняемых сведений в ходе подготовки материалов к открытому опубликованию и при изготовлении рекламной продукции;

е) состояние конфиденциального делопроизводства, соблюдение установленного порядка подготовки, учёта, использования, хранения и уничтожения документов, содержащих персональные данные.

Более подробно вопросы, подлежащие проверке, могут раскрываться в отдельных документах (методических рекомендациях, технологических картах, памятках и т.п.).

Во время проведения проверки, выявленные нарушения требований по обработке и защите персональных данных должны быть по возможности устранены. Проверяющие лица могут дать рекомендации по устранению на месте отмечаемых нарушений и недостатков.

Недостатки, которые не могут быть устранены на месте, включаются в итоговый документ по результатам проверки.

4. Оформление результатов проверки

Результаты проверки оформляются:

1) актом - при проведении проверки комиссией;

2) служебной запиской - при проведении проверки назначенными специалистами.

Акт и/или служебная записка составляется в двух экземплярах и подписывается членами комиссии.

Один экземпляр хранится у ответственного за обработку персональных данных в отраслевом (функциональном) или территориальном органе администрации города Сочи. Второй экземпляр хранится у администратора ИБ. Копия акта о проверке остается в проверяемом отраслевого (функционального), территориального органа администрации города Сочи.

Результаты проверок органов периодически обобщаются ответственным за организацию обработки персональных данных в администрации города Сочи и доводятся до руководителей отраслевых (функциональных), территориальных органов администрации города Сочи. При необходимости принятия решений по результатам проверок отраслевого (функционального), территориального органа администрации города Сочи на имя главы муниципального образования городской округ город-курорт Сочи Краснодарского края готовятся соответствующие служебные записки.

Начальник управления информатизации и связи администрации муниципального образования городской округ город-курорт Сочи Краснодарского края — Н.Р.Лавриенко

Приложение № 20
к распоряжению администрации
муниципального образования городской
округ город-курорт Сочи
Краснодарского края
от 16.08.2021 № 300-р

ПОРЯДОК
доступа служащих администрации муниципального образования городской округ город-курорт Сочи Краснодарского края в помещения, в которых ведётся обработка персональных данных

1. Общие положения

Настоящий порядок разработан в целях обеспечения безопасности персональных данных, средств вычислительной техники информационных систем персональных данных, материальных носителей персональных данных, а также обеспечения внутриобъектового режима.

Документ устанавливает правила доступа в помещения в рабочее и нерабочее время, а также в нештатных ситуациях.

Объектами охраны администрации муниципального образования городской округ город-курорт Сочи Краснодарского края (далее – администрация города Сочи) являются:

1) помещения, в которых происходит обработка персональных данных как с использованием средств автоматизации, так и без таковых, в том числе серверные помещения;

2) помещения, в которых хранятся материальные носители персональных данных и резервные копии персональных данных;

3) помещения, в которых установлены криптографические средства, предназначенные для шифрования персональных данных, в том числе носители ключевой информации (далее – спецпомещения).

Бесконтрольный доступ посторонних лиц в указанные помещения исключён.

Посторонними лицами считаются работники (служащие) администрации города Сочи, не допущенные к обработке персональных данных и лица, не являющиеся работниками (служащими) администрации города Сочи.

К спец-помещениям, предъявляются дополнительные требования по безопасности, указанные в разделе 4.

Ответственность за соблюдение положений настоящего порядка несут работники (служащие) отраслевых (функциональных), территориальных органов администрации города Сочи, допущенные в помещения, являющиеся объектами охраны, а также их руководители.

Контроль соблюдения требований настоящей инструкции обеспечивает руководитель отраслевого (функционального), территориального органа, в котором происходит обработка персональных данных в администрации города Сочи.

Ограждающие конструкции объектов охраны должны предполагать существенные трудности для нарушителя по их преодолению. Например, металлические решётки на окнах, металлическая дверь, система контроля и управления доступа и так далее.

2. Правила доступа в помещения, в которых ведётся обработка персональных данных

Доступ посторонних лиц в помещения, в которых ведется обработка персональных данных, а также хранятся материальные носители персональных данных и резервные копии персональных данных, должен осуществляется только ввиду служебной необходимости и под контролем сопровождающего лица, из числа работников (служащих), допущенных к обработке персональных данных.

При этом должны быть приняты меры, исключающие ознакомление посторонних лиц с персональными данными. Например, мониторы повернуты в сторону от посетителей, документы убраны в стол, либо находятся в непрозрачной папке (накрыты чистыми листами бумаги).

При возникновении чрезвычайных ситуаций природного и техногенного характера, аварий, катастроф, стихийных бедствий, а также ситуаций, которые могут создавать угрозу жизни и здоровью граждан, в целях оказания помощи гражданам, предотвращения, ликвидации предпосылок и последствий нештатной ситуации, может осуществляться доступ в помещения, в которых ведется обработка персональных данных лиц из числа работников (служащих) администрации города Сочи, не допущенных к обработке персональных данных.

В нерабочее время все окна и двери в помещениях (в том числе в смежные помещения), в которых ведется обработка персональных данных, должны быть надежно закрыты, материальные носители персональных данных должны быть убраны в запираемые шкафы (сейфы), компьютеры выключены либо заблокированы.

3. Правила доступа в серверные помещения

Доступ в серверные помещения, в которых ведется обработка персональных данных, осуществляется в соответствии со списком, утверждённым главой муниципального образования городской округ город-курорт Сочи Краснодарского края.

Уборка серверных помещений происходит только под контролем лица, из указанных в утверждённом списке.

Доступ в серверные помещения посторонних лиц допускается по согласованию с администратором ИБ в администрации города Сочи.

Нахождение в серверных помещениях посторонних лиц без сопровождающего запрещено.

При возникновении чрезвычайных ситуаций природного и техногенного характера, аварий, катастроф, стихийных бедствий, а также других ситуаций, которые могут создавать угрозу жизни и здоровью граждан, доступ в серверные помещения, в целях оказания помощи гражданам, предотвращения, ликвидации

предпосылок и последствий нештатной ситуации, может осуществляться без согласования с ответственным за обеспечение безопасности информационных систем персональных данных.

4. Правила доступа в спецпомещения

Спецпомещения выделяют с учётом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к средствам криптографической защиты информации (далее – СКЗИ). Помещения должны иметь прочные входные двери с замками, гарантирующими надёжное закрытие помещений в нерабочее время. Окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в спецпомещения посторонних лиц, необходимо оборудовать металлическими решётками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в спецпомещения.

Расположение спецпомещения, специальное оборудование и организация режима в спецпомещениях должны исключить возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

Для предотвращения просмотра извне спецпомещений их окна должны быть защищены.

Спецпомещения должны быть оснащены входными дверьми с замками. Должно быть обеспечено постоянное закрытие дверей спецпомещений на замок и открытие только для санкционированного прохода, а также оборудование спецпомещений соответствующими техническими устройствами, сигнализирующими о несанкционированном входе в спецпомещения.

Доступ в спецпомещения осуществляется в соответствии с перечнем лиц, имеющих право доступа в помещения, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ, утверждённым распоряжением администрации города Сочи.

Доступ иных лиц в спецпомещения может осуществляться под контролем лиц, имеющих право допуска в спецпомещения.

При возникновении чрезвычайных ситуаций природного и техногенного характера, аварий, катастроф, стихийных бедствий, а также ситуаций, которые могут создавать угрозу жизни и здоровью граждан, в целях оказания помощи гражданам, предотвращения, ликвидации предпосылок и последствий нештатной ситуации, может осуществляться доступ в спецпомещения иных лиц их числа работников (служащих) администрации города Сочи.

Представители органов МЧС и аварийных служб, врачи «скорой помощи» допускаются в спецпомещения для ликвидации нештатной ситуации, иных чрезвычайных ситуаций или оказания медицинской помощи в сопровождении работников, имеющих право доступа в спецпомещения.

При утрате ключа от входной двери в спецпомещение замок необходимо

заменить или переделать его секрет с изготовлением к нему новых ключей с документальным оформлением.

Нахождение в спецпомещениях посторонних лиц в нерабочее время запрещается.

Начальник управления информатизации и связи администрации муниципального образования городской округ город-курорт Сочи Краснодарского края Н.Р.Лавриенко

Приложение № 21
к распоряжению администрации
муниципального образования городской
округ город-курорт Сочи
Краснодарского края
от 16.08.2021 № 300-р

ПОЛОЖЕНИЕ
по работе с инцидентами информационной безопасности в администрации муниципального образования городской округ город-курорт Сочи Краснодарского края

1. Общие положения

Положение о работе с инцидентами информационной безопасности в администрации муниципального образования городской округ город-курорт Сочи Краснодарского края (далее – Положение) разработано в соответствии с:

1) Федеральным законом Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

2) Федеральным законом Российской Федерации от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

3) требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119;

4) приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

5) политикой обработки персональных данных.

Работа с инцидентами включает в себя следующие направления:

1) определение лиц, ответственных за выявление инцидентов и реагирование на них;

2) обнаружение, идентификация и регистрация инцидентов;

3) своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами;

4) анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий;

5) принятие мер по устранению последствий инцидентов;

6) планирование и принятие мер по предотвращению повторного возникновения инцидентов.

Для анализа инцидентов, в том числе определения источников и причин возникновения инцидентов, а также оценки их последствий; планирования и принятия мер по предотвращению повторного возникновения инцидентов, назначается постоянно действующая комиссия по работе с инцидентами в

соответствии с распоряжением администрации муниципального образования городской округ город-курорт Сочи Краснодарского края.

2. Ответственные за выявление инцидентов и реагирование на них

2.1. В информационных системах (далее – ИС) администрации муниципального образования городской округ город-курорт Сочи Краснодарского края (далее – администрация города Сочи).

Ответственными за выявление инцидентов в ИС являются:

1) лица, имеющие право доступа к ИС;

2) ответственный за техническое обслуживание ИС;

3) администратор информационной безопасности ИС.

Ответственными за реагирование на инциденты в ИС являются:

1) лица, имеющие право доступа к ИС;

2) руководитель отраслевого (функционального) или территориального органа администрации города Сочи, в котором выявлен инцидент;

3) ответственный за техническое обслуживание ИС;

4) администратор ИС;

5) администратор информационной безопасности ИС;

6) ответственный за организацию обработки персональных данных в администрации города Сочи;

7) председатель комиссии по работе с инцидентами.

2.2. Вне информационных систем администрации города Сочи.

Ответственными за выявление инцидентов вне ИС являются все работники (служащие) администрации города Сочи.

Ответственными за реагирование на инциденты вне ИС являются:

1) работник отраслевого (функционального) или территориального органа администрации города Сочи, обнаруживший инцидент;

2) руководитель отраслевого (функционального) или территориального органа администрации города Сочи, в котором выявлен инцидент;

3) ответственный за организацию обработки персональных данных в администрации города Сочи, в случае если существует угроза безопасности персональных данных;

4) председатель комиссии по работе с инцидентами.

3. Обнаружение, идентификация и регистрация инцидентов

3.1. Работа по обнаружению инцидентов в области информационной безопасности включает в себя мероприятия, направленные на:

1) выявление инцидентов в области информационной безопасности с помощью технических средств;

2) выявление инцидентов в области информационной безопасности в ходе контрольных мероприятий;

3) выявление инцидентов с помощью работников (служащих) администрации города Сочи.

3.2. Работа по идентификации инцидентов в области информационной безопасности включает в себя мероприятия, направленные на доведение до

работников (служащих) администрации города Сочи информации, позволяющей идентифицировать инциденты.

4. Информирование о возникновении инцидентов

Муниципальный служащий администрации города Сочи (пользователь ИС), обнаруживший инцидент в ИС, должен незамедлительно, любым доступным способом, сообщить об инциденте непосредственному руководителю, администратору ИС, администратору информационной безопасности, ответственному за организацию обработки персональных данных в администрации города Сочи (в случае если ИС является ИСПДн), председателю комиссии по работе с инцидентами.

Администратор ИС, в случае необходимости, информирует пользователей ИС о возникновении инцидента и дает указания по дальнейшим действиям.

5. Анализ инцидентов, а также оценка их последствий

Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценку их последствий осуществляет комиссия по работе с инцидентами информационной безопасности.

5.1. Источниками и причинами возникновения инцидентов в области информационной безопасности являются:

1) действия организаций и отдельных лиц враждебные интересам администрации города Сочи;

2) отсутствие персональной ответственности работников (служащих) администрации города Сочи и их руководителей за обеспечение информационной безопасности, в том числе персональных данных;

3) недостаточная работа с персоналом по обеспечению необходимого режима соблюдения конфиденциальности, в том числе персональных данных;

4) отсутствие дисциплинарной мотивации соблюдения правил и требований информационной безопасности;

5) недостаточная техническая оснащённость подразделений, ответственных за обеспечение информационной безопасности;

6) совмещение функций по разработке и сопровождению или сопровождению и контролю за информационными системами;

7) наличие привилегированных бесконтрольных пользователей в информационной системе;

8) пренебрежение правилами и требованиями информационной безопасности работниками (служащими) администрации города Сочи;

9) и иные события, выявляемые в результате поиска источников и причин возникновения инцидентов.

5.2. Оценка последствий инцидента производится на основании потенциально возможного или фактического ущерба.

6. Принятие мер по устранению последствий инцидентов

Меры по устранению последствий инцидентов включает в себя мероприятия, направленные на:

1) определение границ инцидента и ущерба от реализации угроз информационной безопасности;

2) ликвидацию последствий инцидента и полное либо частичное возмещение ущерба.

7. Планирование и принятие мер по предотвращению инцидентов

7.1. Планирование и принятие мер по предотвращению возникновения инцидентов осуществляет комиссия по работе с инцидентами информационной безопасности и основывается на:

1) планомерной деятельности по повышению уровня осознанности информационной безопасности руководством и работниками (служащими) администрации города Сочи;

2) проведении мероприятий по обучению работников (служащих) администрации города Сочи правилам и способам работы со средствами защиты информационных систем;

3) доведении до работников (служащих) норм законодательства, внутренних документов администрации города Сочи, устанавливающих ответственность за нарушение требований информационной безопасности;

4) разъяснительной работе с увольняющимися работниками (служащими) и работниками (служащими), принимаемыми на работу;

5) своевременной модернизации системы обеспечения информационной безопасности, с учетом возникновения новых угроз информационной безопасности, либо в случае изменения требований руководящих документов по организации обеспечения информационной безопасности;

6) своевременном обновлении программного обеспечения, в том числе баз сигнатур антивирусных средств.

Начальник управления информатизации и связи администрации муниципального образования городской округ город-курорт Сочи Краснодарского края — Н.Р.Лавриенко

Департамент муниципальной службы и кадровой политики