АДМИНИСТРАЦИЯ ГОРОДА СОЧИ

ПОСТАНОВЛЕНИЕ

от 28.07.2016 № 1773

город Сочи

Об утверждении Политики информационной безопасности в администрации города Сочи

В соответствии с Федеральным законом от 27 июля 2006 года №152-ФЗ «О персональных данных», Федеральным законом от 27 июля 2006 года №149-ФЗ «Об информации, информационных технологиях и о защите информации» и иными документами, регламентирующими защиту информации в Российской Федерации, органах государственной власти, органах местного самоуправления, ПОСТАНОВЛЯЮ:

1. Утвердить Политику информационной безопасности в администрации города Сочи (прилагается).

2. Руководителям отраслевых (функциональных) и территориальных органов администрации города Сочи ознакомить служащих с утвержденной Политикой информационной безопасности в администрации города Сочи (далее – Политика) и отметить индивидуальную ответственность за нарушение положений Политики под роспись. Срок ознакомления установить: 30 дней со дня вступления в силу настоящего постановления.

3. Руководителям отраслевых (функциональных) органов, не обладающих правом юридического лица, а также территориальных органов администрации города Сочи организовать работу по регистрации носителей информации в соответствии с Инструкцией по пользованию съемными носителями информации (Приложение №12 к Политике).

4. Департаменту муниципальной службы и кадровой политики администрации города Сочи (Владимирская) организовать работу по ознакомлению с Политикой информационной безопасности служащих при приёме на работу.

5. Полномочия по контролю за выполнением положений Политики информационной безопасности возложить на управление информационных ресурсов администрации города Сочи (Похлебаев).

6. Управлению информационных ресурсов администрации города Сочи разместить настоящее постановление на официальном сайте администрации города Сочи в информационно-коммуникационной сети Интернет.

7.Контроль за выполнением настоящего постановления возложить на заместителя Главы города Сочи С.П.Юрина.

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

Глава города Сочи А.Н. Пахомов

024602

Приложение
к постановлению
администрации города Сочи
от 28.07.2016 № 1773

ПОЛИТИКА
информационной безопасности в администрации города Сочи

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Политика информационной безопасности (далее – Политика) разработана на основании Конституции Российской Федерации, Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», Федерального закона от 27 июля 2006 года №149-ФЗ «Об информации, информационных технологиях и о защите информации» и других нормативно-правовых актов Российской Федерации.

1.2. Настоящей Политикой определяется порядок обработки информации, т.е. действия (операции) с персональными данными служащих администрации города Сочи (далее - Администрация) и служащих (далее служащих) отраслевых (функциональных) органов (далее – Подразделений) и иных лиц, не являющихся служащими Администрации, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных с использованием средств автоматизации или без использования таких средств.

1.3. Целью настоящей Политики является организация обработки и обеспечения безопасности персональных данных служащих Администрации, а также персональных данных иных лиц в соответствии с законодательными и нормативными правовыми актами Российской Федерации, и иной информации ограниченного доступа при их обработке в информационных системах Администрации.

1.4. Основные термины и определения, применяемые в настоящей Политике:

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

1.4.2. **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.

1.4.3. **Распространение персональных данных** – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

1.4.4. **Использование персональных данных** – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

1.4.5. **Блокирование персональных данных** – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

1.4.6. **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.

1.4.7. **Обезличивание персональных данных** – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

1.4.8. **Информационная система персональных данных** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

1.4.9. **Информационные системы Администрации** - государственные информационные системы, обрабатывающие конфиденциальную информацию, и информационные системы персональных данных.

1.4.10. **Конфиденциальная информация (информация ограниченного доступа)** – информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации и представляет собой коммерческую, служебную или личную тайны, охраняющиеся её владельцем.

1.4.11. **Конфиденциальность персональных данных** – обязательное для соблюдения оператором, или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

1.4.12. **Общедоступные персональные данные** – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

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.

Сведения о субъекте персональных данных могут быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта или по решению главы города Сочи, либо по решению суда или иных уполномоченных государственных органов.

1.4.13. **Служащие** – лица, имеющие трудовые отношения с Администрацией, либо кандидаты на вакантную должность, вступившие в отношения по поводу приема на работу, либо служащие отраслевых (функциональных) органов.

1.4.14. **Оператор** –муниципальный орган, самостоятельно или совместно с другими лицами организующий и (или) осуществляющий обработку персональных данных, а также определяющий цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

1.5. **К субъектам персональных данных** (далее – субъекты) относятся лица-носители персональных данных, персональные данные которых переданы Администрации (как на добровольной основе, так и в рамках выполнения требований нормативно-правовых актов) для обработки (в том числе передачи), в том числе:

– служащие Администрации, включая совместителей, а также лица, выполняющие работы по договорам гражданско-правового характера;

– иные лица, предоставляющие персональные данные Администрации.

1.6. Обработка персональных данных субъекта без его письменного согласия не допускается, если иное не определено законом. Персональные данные относятся к информации ограниченного доступа, не составляющей государственную тайну.

1.7. Должностные лица Администрации, в обязанности которых входит обработка персональных данных субъектов, обязаны обеспечить каждому субъекту возможность ознакомления со своими персональными данными, если иное не предусмотрено законом.

1.8. Персональные данные не могут быть использованы в целях:

– причинения имущественного и морального вреда гражданам;

– затруднения реализации прав и свобод граждан Российской Федерации.

1.9. Настоящая Политика и изменения к ней утверждаются Постановлением администрации города Сочи, являются обязательным для исполнения всеми служащими, имеющими доступ к персональным данным субъектов персональных данных Администрации. Администрацией должен быть обеспечен неограниченный доступ к настоящей Политике путем ее размещения на веб-сайте www.sochiadm.ru или иным образом во исполнение пункта 2 статьи 18.1 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

2. ПРИНЦИПЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1.Обработка персональных данных в Администрации осуществляется на основе следующих принципов:

– осуществления обработки персональных данных на законной и справедливой основе;

– ограничения достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, не совместимых с целями сбора персональных данных;

– недопустимости объединения созданных для несовместимых между собой целей баз данных, содержащих персональные данные;

– соответствия содержания и объема персональных данных целям их обработки, а также недопустимости обработки персональных данных, избыточных по отношению к заявленным целям;

– обеспечения точности, достаточности, а в необходимых случаях и актуальности персональных данных по отношению к целям обработки персональных данных.

2.2.Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

2.3.Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, информативным и сознательным.

3. ПОНЯТИЕ И СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1.Под персональными данными субъектов персональных данных понимается любая информация, относящаяся к данному субъекту персональных данных.

3.2. Перечень обрабатываемых персональных данных приведен в приложении № 1 к настоящей Политике.

3.3.Операторы 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.

4. ПОЛУЧЕНИЕ, ОБРАБОТКА И ХРАНЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1.Администрация получает сведения о персональных данных субъектов персональных данных непосредственно от самих субъектов, из общедоступных источников, от третьих лиц. Субъект персональных данных обязан представлять Администрации достоверные сведения о себе. Администрация имеет право проверять достоверность указанных сведений в порядке, не противоречащем законодательству Российской Федерации.

4.2.Администрация руководствуется конкретными, заранее определенными целями обработки персональных данных, в соответствии с которыми персональные данные были предоставлены субъектом, Конституцией Российской Федерации, Трудовым кодексом Российской Федерации и иными федеральными законами при определении состава обрабатываемых персональных данных субъектов.

4.3.Обработка персональных данных в Администрации осуществляется в целях:

– обеспечения бухгалтерского и кадрового учета;

– обеспечения рассмотрения, обработки и анализа обращений граждан.

4.4.Как правило, персональные данные субъекта Администрация получает непосредственно от субъекта. Служащий, ответственный за документационное обеспечение производственной деятельности, принимает от субъекта материальные носители персональных данных (документы, копии документов), сверяет копии документов с подлинниками.

4.5.Если персональные данные субъекта возможно получить исключительно у третьей стороны, то субъект должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие (приложение № 3). Администрация сообщает субъекту о целях, предполагаемых источниках и способах получения персональных данных, а также о составе подлежащих получению персональных данных и последствиях отказа субъекта представить письменное согласие на их

получение (приложение №3). В случае если субъект уже дал письменное согласие на передачу своих персональных данных третьим лицам, дополнительное уведомление не требуется.

4.6.Условием обработки персональных данных субъекта персональных данных является его письменное согласие (приложение №5). Письменное согласие субъекта на обработку его персональных данных должно включать в себя:

– фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

– фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя;

– наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;

– цель обработки персональных данных;

– перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

– наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;

– перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

– срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;

– подпись субъекта персональных данных.

4.7.Согласие на обработку персональных данных может быть отозвано субъектом персональных данных.

4.8.Согласия субъекта на обработку его персональных данных не требуется в следующих случаях:

– обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;

– обработка персональных данных необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;

– обработка персональных данных необходима для предоставления

государственной или муниципальной услуги в соответствии с Федеральным законом от 27 июля 2010 года № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», для обеспечения предоставления такой услуги, для регистрации субъекта персональных данных на едином портале государственных и муниципальных услуг;

– обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

– обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

– обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

– обработка персональных данных необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных;

– обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением целей продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также целей политической агитации, при условии обязательного обезличивания персональных данных;

– осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе;

– осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

4.9.В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных в письменной форме 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.

4.10. В случае если оператор на основании договора поручает обработку персональных данных другому лицу, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке. Ответственность перед субъектом персональных данных за действия указанного лица несет оператор. Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед оператором.

4.11.Администрация не имеет права осуществлять обработку специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, за исключением, если:

– субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;

– персональные данные сделаны общедоступными субъектом персональных данных;

– обработка персональных данных необходима в связи с реализацией международных договоров Российской Федерации о реадмиссии;

– обработка персональных данных осуществляется в соответствии с Федеральным законом от 25 января 2002 года N 8-ФЗ "О Всероссийской переписи населения";

– обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта персональных данных невозможно;

– обработка персональных данных осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну;

– обработка персональных данных необходима для установления или осуществления прав субъекта персональных данных или третьих лиц, а равно и в связи с осуществлением правосудия;

– обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-розыскной деятельности, об исполнительном производстве, уголовно-исполнительным законодательством Российской Федерации;

– обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации, государственными органами, муниципальными органами или организациями в целях устройства детей, оставшихся без попечения родителей, на воспитание в семьи граждан.

В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со ст. 24 Конституции Российской Федерации работодатель вправе получать и обрабатывать данные о частной жизни субъекта только с его письменного согласия.

Обработка специальных категорий персональных данных должна быть незамедлительно прекращена, если устранены причины, вследствие которых осуществлялась обработка.

4.12. Защита персональных данных субъекта от неправомерного их использования или утраты должна быть обеспечена оператором за счет его средств в порядке, установленном федеральным законодательством Российской Федерации.

4.13. Основными источниками, содержащими персональные данные служащих, являются их личные дела.

Личные дела хранятся уполномоченным лицом на бумажных носителях. Помимо этого, персональные данные могут храниться в виде электронных документов, баз данных. Личное дело пополняется на протяжении всей трудовой деятельности служащего в Администрации.

Письменные доказательства получения оператором согласия субъекта персональных данных на их обработку хранятся в личном деле.

4.14. При обработке персональных данных руководитель Администрации вправе утверждать способы обработки, документирования, хранения и защиты персональных данных на базе современных информационных технологий.

4.15. Перечень лиц, допущенных к обработке персональных данных, определяется Постановлением администрации города Сочи.

4.16. Обработка персональных данных, осуществляется уполномоченными должностными лицами Администрации, определенными Постановлением главы города Сочи, которые действуют на основании инструкций, предусматривающих выполнение комплекса мероприятий по организации обработки и обеспечению безопасности персональных данных.

4.17. Контроль выполнения требований по обработке и обеспечению безопасности персональных данных организуется оператором самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации, и проводится не реже 1 раза в 3 года в сроки, определяемые оператором.

4.18. Обеспечение техническими средствами обработки (ПЭВМ, серверами и т.д.) и их исправной работы происходит Администратором ИС и

Администратором ИБ. Помещения, в которых обрабатываются и хранятся персональные данные субъектов, оборудуются надежными замками. Должно быть исключено бесконтрольное пребывание посторонних лиц в этих помещениях.

4.19. Для хранения материальных носителей персональных данных используются специально оборудованные шкафы или сейфы, которые запираются на ключ.

4.20. Помещения, в которых обрабатываются и хранятся персональные данные субъектов, в рабочее время при отсутствии в них служащих должны быть закрыты.

4.21. Проведение уборки помещений, в которых хранятся персональные данные, должно производиться в присутствии соответствующих служащих.

5. ПРАВА И ОБЯЗАННОСТИ СТОРОН В ОБЛАСТИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1.Субъект персональных данных обязан:

– передать Администрации или ее представителю комплекс достоверных, документированных персональных данных, состав которых установлен трудовым законодательством, иными законами Российской Федерации, включая сведения об образовании, специальных знаниях, стаже работы, отношении к воинской обязанности, гражданстве, месте жительства и др.

– своевременно сообщать оператору об изменении своих персональных данных.

5.2.Субъект персональных данных имеет право:

– на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

а) подтверждение факта обработки персональных данных оператором;

б) правовые основания и цели обработки персональных данных;

в) цели и применяемые оператором способы обработки персональных данных;

г) наименование и место нахождения оператора, сведения о лицах (за исключением служащих оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;

д) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения,

если иной порядок предоставления таких данных не предусмотрен федеральным законом;

е) сроки обработки персональных данных, в том числе сроки их хранения;

ж) порядок осуществления субъектом персональных данных прав, предусмотренных федеральным законом;

з) информацию об осуществлении или о предполагаемой трансграничной передаче данных;

и) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;

к) иные сведения, предусмотренные федеральными законами.

– на повторное обращение к оператору или направление оператору повторного запроса в целях получения информации, касающейся обработки его персональных данных, и ознакомление с такой информацией не ранее чем через тридцать 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;

– на повторное обращение к оператору или направление повторного запроса в целях получения информации, касающейся обработки его персональных данных, а также в целях ознакомления с обрабатываемыми персональными данными до истечения тридцатидневного срока в случае, если такая информация и (или) персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения;

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

– требовать извещения оператором всех лиц, которым ранее были сообщены неверные или неполные персональные данные субъекта, обо всех произведенных в них исключениях, исправлениях или дополнениях;

– на обжалование действий или бездействий оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

Доступ к своим персональным данным предоставляется субъекту или его законному представителю при личном обращении либо при получении запроса (приложение №7).

Сведения о персональных данных должны быть предоставлены субъекту персональных данных оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных.

5.3.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 субъекта в письменной форме (приложение №5) или в случаях, предусмотренных федеральными законами, устанавливающими такие же меры по обеспечению соблюдения прав и законных интересов субъекта персональных данных.

5.4.Оператор обязан разъяснить субъекту персональных данных порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты своих прав и законных интересов.

5.5.Оператор обязан рассмотреть возражение субъекта персональных данных в течение тридцати дней со дня его получения и уведомить его о результатах рассмотрения такого возражения.

5.6.Если предоставление персональных данных является обязательным в соответствии с федеральным законом, оператор обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

5.7.Если персональные данные получены не от субъекта персональных данных (за исключением случаев, если субъект персональных данных уведомлен об осуществлении обработки его персональных данных соответствующим оператором, персональные данные были получены оператором на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника), оператор до начала обработки таких персональных данных обязан предоставить субъекту персональных данных информацию, содержащую:

– наименование либо фамилия, имя, отчество и адрес оператора или его представителя;

– цель обработки персональных данных и ее правовое основание;

– предполагаемые пользователи персональных данных;

– установленные федеральным законом права субъекта персональных данных;

– источник получения персональных данных.

5.8. Оператор обязан предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, оператор обязан внести в них необходимые изменения. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, оператор обязан уничтожить такие персональные данные. Оператор обязан уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы (приложение №7).

5.9. Оператор обязан сообщить в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение тридцати дней с даты получения такого запроса.

5.10.В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя, либо по запросу субъекта персональных данных или его представителя, либо уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки.

5.11.В случае 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 оператор обязан осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) 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.

5.12.В случае подтверждения факта неточности персональных данных оператор на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные либо обеспечить их уточнение (если

обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в течение семи рабочих дней и снять блокирование персональных данных.

5.13.В случае выявления неправомерной обработки персональных данных, осуществляемой оператором или лицом, действующим по поручению оператора, оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению оператора. В случае, если обеспечить правомерность обработки персональных данных невозможно, оператор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

5.14.В случае достижения цели обработки персональных данных оператор обязан прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати 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 оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных федеральными законами, и уведомить об этом субъекта персональных данных и уполномоченный орган по защите прав субъектов персональных данных в течение десяти рабочих дней с даты прекращения обработки персональных данных или их уничтожения (приложение №9).

5.15.В случае отзыва субъектом персональных данных согласия на обработку его персональных данных оператор обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати 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 оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных федеральными законами. Об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных (приложение №9).

5.16.До начала обработки персональных данных Администрация обязана уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных, за исключением случаев обработки персональных данных:

– обрабатываемых в соответствии с трудовым законодательством;

– полученных Администрацией в связи с заключением договора, стороной которого является субъект персональных данных, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются Администрацией исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных;

– относящихся к членам (участникам) общественного объединения или религиозной организации и обрабатываемых соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться или раскрываться третьим лицам без согласия в письменной форме субъектов персональных данных;

– сделанных субъектом персональных данных общедоступными;

– включающих в себя только фамилии, имена и отчества субъектов персональных данных;

– необходимых в целях однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в аналогичных целях;

– включенных в информационные системы персональных данных, имеющие в соответствии с федеральными законами статус государственных автоматизированных информационных систем, а также в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка;

– обрабатываемых без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к

соблюдению прав субъектов персональных данных.

5.17. Уведомление должно быть направлено в виде документа на бумажном носителе или в форме электронного документа и подписано оператором. Уведомление должно содержать следующие сведения:

– наименование (фамилия, имя, отчество), адрес оператора;

– цель обработки персональных данных;

– категории персональных данных;

– категории субъектов, персональные данные которых обрабатываются;

– правовое основание обработки персональных данных;

– перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных;

– описание мер, которые оператор обязуется осуществлять при обработке персональных данных по обеспечению безопасности персональных данных при их обработке, в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;

– дата начала обработки персональных данных;

– фамилия, имя, отчество физического лица или наименование юридического лица, ответственных за организацию обработки персональных данных, и номера их контактных телефонов, почтовые адреса и адреса электронной почты;

– срок и условия прекращения обработки персональных данных;

– сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;

– сведения о месте нахождения базы данных информации, содержащей персональные данные граждан Российской Федерации;

– сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации.

6. ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ СУБЪЕКТА И ИХ ПЕРЕДАЧА

6.1.Внутренний доступ (доступ внутри Администрации) персональным данным субъектов имеют служащие отраслевых (функциональных), территориальных органов Администрации (далее – Подразделений), которым эти данные необходимы для выполнения служебных (трудовых) обязанностей в соответствии с перечнем лиц, утвержденным Постановлением Администрации.

Право доступа к персональным данным субъекта имеют:

– Глава города Сочи;

– заместители Главы города Сочи;

– руководители Подразделений по направлению деятельности

субъекта (исключительно к персональным данным служащих данного Подразделения; за исключением сведений имущественного характера);

– Руководитель нового подразделения при переводе служащего из одного подразделения в другое (за исключением сведений имущественного характера);

– Начальник и служащие управления по вопросам семьи и детства администрации города Сочи;

– Начальник и служащие управления по работе с обращениями граждан и организаций администрации города Сочи;

– Начальник и служащие управления по образованию и науке администрации города Сочи;

– Начальник и служащие отдела по делам несовершеннолетних администрации города Сочи;

– Начальник и служащие управления бухгалтерского учета и отчетности администрации города Сочи;

– Начальник и служащие управления социальной политики администрации города Сочи;

– Начальник и служащие управления молодежной политики администрации города Сочи;

– непосредственно субъект;

– иные служащие Администрации, которые имеют доступ к персональным данным субъекта с письменного согласия самого субъекта персональных данных.

После прекращения юридических отношений с субъектом персональных данных (увольнения служащего и т.п.) документы, содержащие его персональные данные, хранятся в Администрации в течение сроков, установленных архивным и иным законодательством Российской Федерации.

6.2. Внешний доступ к персональным данным субъектов имеют массовые потребители персональных данных и контрольно-надзорные органы.

6.2.1. К числу массовых потребителей персональных данных вне Администрации относятся следующие государственные и негосударственные структуры:

– налоговые органы;

– правоохранительные органы;

– органы лицензирования и сертификации;

– органы прокуратуры и Федеральной Службы Безопасности;

– органы статистики;

– страховые агентства;

– военные комиссариаты;

– органы социального страхования;

– пенсионные фонды.

6.2.2. Надзорно-контрольные органы имеют доступ к информации исключительно в сфере своей компетенции.

6.3. Внешний доступ со стороны третьих лиц к персональным данным субъекта осуществляется с его письменного согласия, за исключением случаев, когда такой доступ необходим в целях предупреждения угрозы жизни и здоровью субъекта или других лиц, и иных случаев, установленных законодательством.

6.4. Оператор обязан сообщать персональные данные субъекта по надлежащим оформленным запросам суда, прокуратуры иных правоохранительных органов.

6.5. Сведения о работающем или уже уволенном служащем могут быть предоставлены другой организации только на основании письменного запроса на бланке организации, с приложением копии заявления служащего.

6.6. Персональные данные субъекта могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого субъекта персональных данных.

6.7. При передаче персональных данных Администрация должна соблюдать следующие требования:

– не сообщать персональные данные субъекта третьей стороне без его письменного согласия, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта персональных данных, а также в случаях, установленных федеральными законами;

– не сообщать персональные данные субъекта в коммерческих целях без его письменного согласия;

– 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, за исключением случаев, когда обмен персональными данными осуществляется в порядке, установленном федеральными законами;

– сообщать информацию о состоянии здоровья субъекта только в тех случаях, если такие сведения относятся к вопросу о выполнении служащим служебных (трудовых) обязанностей;

– передавать персональные данные субъекта представителям служащих и иных категорий субъектов персональных данных в порядке, установленном Трудовым кодексом Российской Федерации и Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», и ограничивать эту информацию только теми персональными данными, которые необходимы для выполнения указанными представителями их целей;

– разрешать доступ к персональным данным, исключительно специально уполномоченным лицам (при этом указанные лица должны иметь право получать лишь те персональные данные, которые необходимы для

выполнения конкретных целей);

– уполномоченные лица должны подписать обязательство о неразглашении персональных данных (приложение №2).

6.8. Ответы на правомерные письменные запросы других предприятий, учреждений и организаций даются с разрешения Главы города Сочи в письменной форме, в том объеме, который позволяет не разглашать излишний объем персональных данных.

6.9. Не допускается передача персональных данных по открытым каналам связи, в том числе по телефону.

6.10.Сведения, передаваемые на материальных или бумажных носителях, должны иметь пометку о конфиденциальности. В сопроводительном письме к таким документам указывается, что в прилагаемых документах содержатся персональные данные субъектов Администрации.

7. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1.Комплекс мер по защите персональных данных направлен на предупреждение нарушений доступности, целостности и конфиденциальности персональных данных и обеспечивает безопасность информации в процессе управленческой и производственной деятельности Администрации.

7.2.Администрация при обработке персональных данных обязана принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в соответствии с требованиями к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, требованиями к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных, установленными Правительством Российской Федерации.

7.3.Мероприятия по защите персональных данных определяются Политикой организации по обработке и защите персональных данных в информационных системах персональных данных, приказами, инструкциями и другими внутренними актами Администрации.

7.4.Обеспечение безопасности персональных данных достигается, в частности:

– определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

– применением организационных и технических мер по обеспечению безопасности персональных данных;

– применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

– оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

– учетом машинных носителей персональных данных;

– обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

– восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

– установлением 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;

– контролем над принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

8. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ, СВЯЗАННОЙ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ

8.1.Персональная ответственность является одним из главных требований к организации функционирования системы защиты персональных данных и обязательным условием обеспечения эффективности функционирования данной системы.

8.2.Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

8.3.Руководитель, разрешающий доступ служащего к конфиденциальному документу, несет персональную ответственность за данное разрешение.

8.4.Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

8.5.Каждый служащий Администрации, получающий для работы конфиденциальный документ, несет персональную ответственность за сохранность носителя и конфиденциальность полученной информации.

8.6.Должностные лица, в обязанность которых входит обработка персональных данных, обязаны обеспечить каждому субъекту персональных данных, возможность ознакомления со своими обрабатываемыми

персональными данными, если иное не предусмотрено законом.

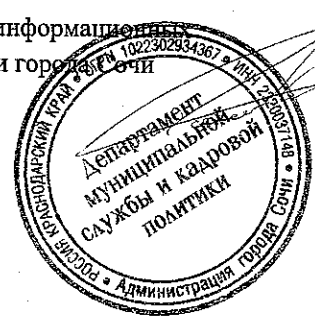
8.7.Неправомерный отказ в предоставлении собранных в установленном порядке персональных данных, либо несвоевременное их предоставление в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации влечет наложение на должностных лиц административного наказания в порядке, установленном Кодексом Российской Федерации об административных правонарушениях.

8.8.В соответствии с Гражданским кодексом Российской Федерации лица, незаконными методами получившие информацию, содержащую персональные данные, обязаны возместить причиненные убытки; такая же обязанность возлагается и на служащих, не обладающих правом доступа к персональным данным.

8.9.Уголовная ответственность за нарушение неприкосновенности частной жизни (в том числе незаконный сбор и (или) распространение сведений о частной жизни лица, составляющего его личную или семейную тайну, без его согласия), неправомерный доступ к охраняемой законом компьютерной информации, неправомерный отказ в предоставлении собранных в установленном порядке документов и сведений (если эти деяния причинили вред правам и законным интересам граждан), совершенные лицом с использованием своего служебного положения влечет наложение наказания в порядке, предусмотренном Уголовным кодексом Российской Федерации.

8.10. Неправомерность деятельности муниципальных органов местного самоуправления по сбору и использованию персональных данных может быть установлена в судебном порядке.

Начальник управления информационных ресурсов администрации города Сочи А.В.Похлебаев



Приложение № 1
к Политике информационной
безопасности в администрации
города Сочи

ПЕРЕЧЕНЬ

персональных данных, обрабатываемых в администрации города Сочи

1 СВЕДЕНИЯ, СОСТАВЛЯЮЩИЕ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Сведениями, составляющими персональные данные, в администрации города Сочи является любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе:

1.1 Фамилия, имя, отчество (в т.ч. прежние), дата и место рождения.

1.2 Паспортные данные или данные иного документа, удостоверяющего личность (серия, номер, дата выдачи, наименование органа, выдавшего документ) и гражданство.

1.3 Адрес места жительства (по паспорту и фактический) и дата регистрации по месту жительства или по месту пребывания.

1.4 Номера телефонов (мобильного и домашнего), в случае их регистрации на субъекта персональных данных или по адресу его места жительства (по паспорту).

1.5 Сведения об образовании, квалификации и о наличии специальных знаний или специальной подготовки (серия, номер, дата выдачи диплома, свидетельства, аттестата или другого документа об окончании образовательного учреждения, в том числе наименование и местоположение образовательного учреждения, дата начала и завершения обучения, факультет или отделение, квалификация и специальность по окончании образовательного учреждения, ученая степень, ученое звание, владение иностранными языками и другие сведения).

1.6 Сведения о повышении квалификации и переподготовке (серия, номер, дата выдачи документа о повышении квалификации или о переподготовке, наименование и местоположение образовательного учреждения, дата начала и завершения обучения, квалификация и специальность по окончании образовательного учреждения и другие сведения).

1.7 Сведения о трудовой деятельности (данные о трудовой занятости на текущее время с полным указанием должности, Подразделения Администрации, ИНН, адреса и телефонов, а также реквизитов других организаций с полным наименование занимаемых ранее в них

сведения).

1.8 Сведения о номере, серии и дате выдачи трудовой книжки (вкладыша в нее) и записях в ней.

1.9 Содержание и реквизиты трудового договора со служащим Администрации.

1.10 Сведения о заработной плате (номера счетов для расчета со служащими, данные зарплатных договоров, в том числе номера их спецкартсчетов, данные по окладу, надбавкам, налогам и другие сведения).

1.11 Сведения о воинском учете военнообязанных лиц и лиц, подлежащих призыву на военную службу (серия, номер, дата выдачи, наименование органа, выдавшего военный билет, военно-учетная специальность, воинское звание, данные о принятии\снятии на(с) учет(а) и другие сведения).

1.12 Сведения о семейном положении (состояние в браке, данные свидетельства о заключении брака, фамилия, имя, отчество супруга(и), паспортные данные супруга(и), данные брачного контракта, данные справки по форме 2НДФЛ супруга(и), данные документов по долговым обязательствам, степень родства, фамилии, имена, отчества и даты рождения других членов семьи, иждивенцев и другие сведения).

1.13 Сведения о номере и серии страхового свидетельства государственного пенсионного страхования.

1.14 Сведения об идентификационном номере налогоплательщика.

1.15 Сведения из страховых полисов обязательного (добровольного) медицинского страхования (в том числе данные соответствующих карточек медицинского страхования).

1.16 Сведения, указанные в оригиналах и копиях приказов по личному составу Администрации и материалах к ним.

1.17 Сведения о государственных и ведомственных наградах, почетных и специальных званиях, поощрениях (в том числе наименование или название награды, звания или поощрения, дата и вид нормативного акта о награждении или дата поощрения) служащих Администрации.

1.18 Материалы по аттестации и оценке служащих Администрации.

1.19 Материалы по внутренним служебным расследованиям в отношении служащих Администрации.

1.20 Внутренние материалы по расследованию и учету несчастных случаев на производстве и профессиональным заболеваниям в соответствии с Трудовым кодексом Российской Федерации, другими федеральными законами.

1.21 Сведения о временной нетрудоспособности служащих Администрации.

1.22 Табельный номер работника Администрации.

1.23 Сведения о социальных льготах и о социальном статусе (серия, номер, дата выдачи, наименование органа, выдавшего документ, являющийся основанием для предоставления льгот и статуса, и другие сведения).

основанием для предоставления льгот и статуса, и другие сведения).

1.24 ФИО и паспортные данные граждан, данные о финансовом и имущественном положении граждан, обращающихся в Администрацию, данные о состоянии их здоровья.

1.25 ФИО, паспортные данные, данные о семейном положении, иные идентифицирующие данные несовершеннолетних, в отделе по делам несовершеннолетних.

1.26 ФИО, паспортные данные, данные о семейном положении, иные идентифицирующие данные несовершеннолетних, а также ФИО, паспортные данные, данные о семейном положении, данные о финансовом имущественном положении их родителей, в управлении по вопросам семьи и детства.

1.27 Сведения об адресах сайтов и (или) страниц, в информационно-телекоммуникационной сети «Интернет», на которых гражданин, претендующий на замещение должности муниципальной службы, муниципальный служащий разместили общедоступную информацию, а также данные, позволяющие их идентифицировать.

2 ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1 Целями обработки указанных выше персональных данных являются:

2.1.1 организация учета служащих Администрации для обеспечения соблюдения законов и иных нормативно-правовых актов, содействия в трудоустройстве, обучении, продвижении по службе, пользования различного вида льготами в соответствии с Трудовым кодексом Российской Федерации, Налоговым кодексом Российской Федерации, федеральными законами, в частности: «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования», «О персональных данных», а также Уставом и нормативными актами Администрации.

2.1.2 выполнение работ по обеспечению рассмотрения обращений граждан

3 СРОКИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1 Сроки обработки указанных выше персональных данных определяются в соответствие со сроком действия договора с субъектом ПДн, и целями обработки персональных данных.

Начальник управления информационных ресурсов администрации города Сочи А.В.Похлебаев

Приложение № 2
к Политике информационной безопасности в администрации города Сочи

ОБЯЗАТЕЛЬСТВО

о неразглашении персональных данных

Я, _____

(должность,

_____,

фамилия, имя, отчество)

ознакомлен(а) с «Политикой информационной безопасности в администрации города Сочи» и обязуюсь не разглашать сведения, содержащие персональные данные субъектов персональных данных, ставшие мне известными в связи с исполнением мною трудовых (должностных) обязанностей. Об ответственности за разглашение указанных сведений предупрежден(а).

_____ _____ _____

дата подпись расшифровка подписи

Начальник управления информационных ресурсов администрации города Сочи А.В.Похлебаев

Приложение № 3
к Политике информационной
безопасности в администрации
города Сочи

ПИСЬМЕННОЕ СОГЛАСИЕ

субъекта персональных данных

на получение его персональных данных у третьих лиц

Я, _____,

(фамилия, имя, отчество)

согласен(на) на получение оператором (администрацией города Сочи) от _____

(фамилия, имя отчество или наименование третьего лица)

следующей информации _____

_____

(виды запрашиваемой информации и (или) документов)

_____ _____

дата подпись расшифровка подписи

Начальник управления информационных ресурсов администрации города Сочи А.В.Похлебаев

Приложение № 4
к Политике информационной
безопасности в администрации
города Сочи

УВЕДОМЛЕНИЕ

Уважаемый(ая)_____

(фамилия, имя, отчество)

В связи с _____

(указать причину)

у администрации города Сочи возникла необходимость получения следующей информации, составляющей Ваши персональные данные _____

(перечислить информацию)

Просим Вас предоставить указанные сведения _____

_____

(кому)

в течение трех рабочих дней с момента получения настоящего уведомления.

В случае невозможности предоставить указанные сведения просим в указанный срок дать письменное согласие на получение оператором (администрация города Сочи) необходимой информации из следующих источников:

_____,

(указать источники)

следующими способами: _____

(автоматизированная обработка, иные способы)

По результатам обработки указанной информации оператором планируется принятие следующих решений, которые будут доведены до Вашего сведения_____

_____

(указать решения и иные юридические последствия обработки информации)

Против принятого решения Вы имеете право заявить свои письменные возражения в _____ срок.

Информируем Вас о последствиях Вашего отказа дать письменное согласие на получение оператором указанной информации

_____

_____

(перечислить последствия)

Информируем Вас о Вашем праве в любое время отозвать свое письменное согласие на обработку персональных данных.

_____ _____ _____

дата подпись расшифровка подписи

Настоящее уведомление на руки получил(а):

_____ _____ _____

дата подпись расшифровка подписи

Начальник управления информационных ресурсов администрации города Сочи А.В.Похлебаев

Приложение № 5
к Политике информационной безопасности в администрации города Сочи

СОГЛАСИЕ СУБЪЕКТА

на обработку его персональных данных

Я, _____,

(фамилия, имя, отчество субъекта)

даю свое согласие администрации города Сочи (далее – Администрация) на обработку (включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение) моих персональных данных:

– _____;
– _____;
– _____,

а также предоставления сторонним лицам (включая органы государственного и муниципального управления) в рамках требований законодательства России.

Обработка, передача персональных данных разрешается на срок, установленный нормативно-правовыми актами РФ.

Согласие может быть отозвано мною в любое время на основании моего письменного заявления.

Подтверждаю свое согласие с «Политикой информационной безопасности в администрации города Сочи», а также ознакомление с правами и обязанностями в области защиты персональных данных.

_____ _____ _____

дата подпись расшифровка подписи

Начальник управления информационных ресурсов администрации города Сочи А.В.Похлебаев

Приложение № 6
к Политике информационной
безопасности в администрации
города Сочи

СОГЛАСИЕ СЛУЖАЩЕГО

на обработку его персональных данных

Я, _____

(фамилия, имя, отчество служащего)

документ, удостоверяющий личность _____

(вид документа)

серия, номер _____

выдан

_____

(кем и когда выдан)

проживающий(ая) по адресу _____

_____

являясь служащим администрации города Сочи (далее - Оператор), находящейся по адресу: г. Сочи, ул. Советская, д.26, своей волей и в своих интересах выражаю согласие на обработку моих персональных данных Оператором в целях информационного обеспечения для формирования общедоступных источников персональных данных (справочников, адресных книг, информации в СМИ, на сайте организации и т.д.), включая выполнение действия по сбору, систематизации, накоплению, хранению, уничтожению (обновлению, изменению), распространению (в том числе передаче) и уничтожению моих персональных данных, входящих в следующий перечень общедоступных сведений:

- фамилия, имя, отчество;

- дата рождения;

- рабочий номер телефона и адрес электронной почты;

- сведения о профессии, должности, образовании;

- иные сведения, специально предоставленные мной для размещения в общедоступных источниках персональных данных.

Для целей обеспечения соблюдения законов и иных нормативных правовых актов, содействия в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности, контроля количества и качества выполняемой работы и обеспечения сохранности имущества, оформления доверенностей, прохождения конкурсного отбора, безналичных платежей на мой счет, выражаю согласие на получение и передачу моих персональных данных путем подачи и получения запросов в отношении органов местного самоуправления, государственных органов и организаций (для этих целей дополнительно к общедоступным сведениям могут быть получены или переданы сведения о дате рождения, гражданстве, доходах, паспортных данных, сведениях о водительском удостоверении, предыдущих местах работы, идентификационном номере налогоплательщика, свидетельстве государственного пенсионного страхования, допуске к сведениям, составляющим государственную тайну, социальных льготах и выплатах, на которые я имею право в соответствии с действующим законодательством).

Вышеприведенное согласие на обработку моих персональных данных предоставлено с учетом п. 2 ст. 6 и п. 2 ст. 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», в соответствии с которыми обработка персональных данных, осуществляемая на основе федерального закона либо для исполнения договора, стороной в котором я являюсь, может осуществляться Оператором без моего дополнительного согласия.

Персональные данные подлежат уничтожению по достижению целей обработки или в случае утраты необходимости их достижения.

Настоящее согласие вступает в силу с момента его подписания на срок действия трудового договора с Оператором и может быть отозвано путем подачи Оператору письменного заявления.

_____ _____ _____

дата подпись расшифровка подписи

Начальник управления информационных ресурсов администрации города Сочи А.В.Похлебаев

Приложение № 7
к Политике информационной
безопасности в администрации
города Сочи

ЗАПРОС О ДОСТУПЕ
субъекта персональных данных к своим персональным данным

_____

(наименование и адрес оператора)

От _____

(фамилия, имя, отчество,

_____

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

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

_____.

(перечислить)

_____ _____ _____

дата подпись расшифровка подписи

Начальник управления информационных
ресурсов администрации города Сочи А.В.Похлебаев

Приложение № 8
к Политике информационной
безопасности в администрации
города Сочи

УВЕДОМЛЕНИЕ

Уважаемый(ая) _____

(фамилия, имя, отчество)

на основании _____
администрация города Сочи (Оператор), расположенная по адресу: г. Сочи, ул. Советская, д.26, получила от

_____

(наименование организации, адрес)

следующую информацию, содержащую Ваши персональные данные: _____

_____

(перечислить)

Указанная информация будет обработана и использована Оператором в целях:_____

_____

(перечислить)

Вы имеете право на полную информацию о своих персональных данных, содержащуюся у оператора, свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей Ваши персональные данные, за исключением случаев, предусмотренных действующим законодательством; требовать от Оператора уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав, получать иную информацию, касающуюся обработки Ваших персональных данных.

_____ _____ _____

дата подпись расшифровка подписи

Настоящее уведомление на руки получил(а):

_____ _____ _____

дата подпись расшифровка подписи

Начальник управления информационных
ресурсов администрации города Сочи А.В.Похлебаев

Приложение № 9
к Политике информационной
безопасности в администрации
города Сочи

УВЕДОМЛЕНИЕ ОБ УНИЧТОЖЕНИИ,

(изменении, прекращении обработки, устранении нарушений

персональных данных)

Уважаемый(ая) _____.

(фамилия, имя, отчество)

В связи с _____

_____

(недостоверностью, выявлением неправомерных действий с Вашими персональными данными, достижением цели обработки, отзывом Вами согласия на обработку, другие причины)

сообщаем Вам, что обработка следующих Ваших персональных данных:

_____

_____

(перечислить)

прекращена и указанная информация подлежит уничтожению (изменению).

_____ _____ _____

дата подпись расшифровка подписи

Настоящее уведомление на руки получил(а):

_____ _____ _____

дата подпись расшифровка подписи

Начальник управления информационных
ресурсов администрации города Сочи А.В.Похлебаев

Нештатная ситуация		Оценка ситуации (раздел Инструкции)
		Ошибка привела к нарушению работоспособности ТС и ПО (0)
Дефекты, сбои, отказы, аварии ТС, программных средств и систем ОИ		(0)
Сбои, отказы и аварии систем обеспечения ОИ		(0)
Природные явления, стихийные бедствия	Несущие угрозу жизни человека	(0)
	Не несущие угрозу жизни человека	(0)

Нештатные ситуации, которые повлекли утечку или повреждение защищаемой информации либо созданы внутренним злоумышленником

При обнаружении нештатных ситуаций, которые повлекли утечку или повреждение защищаемой информации либо созданы внутренним злоумышленником, создается комиссия.

В первую очередь администратором ИБ предпринимаются действия по сбору и обеспечению сохранности улик незаметно для злоумышленника при нештатных ситуациях, связанных с:

- разглашением защищаемой информации;
- обнаружением несанкционированно скопированной или измененной защищаемой информации;
- обнаружением подключения технических средств к средствам и системам объекта информатизации;
- обнаружением закладочных устройств;
- маскировкой под зарегистрированного пользователя внутренним злоумышленником или обнаружением факта маскировки в прошлом (как внутренним, так и внешним злоумышленником);
- использованием дефектов программного обеспечения ОИ внутренним злоумышленником или обнаружением факта их использования в прошлом (как внутренним, так и внешним злоумышленником);
- использованием программных закладок внутренним злоумышленником или обнаружением факта их использования в прошлом (как внутренним, так и внешним злоумышленником);
- хищением носителя защищаемой информации.

Комиссия, дополнительно к общему порядку действий (в соответствии с разделом 3), должна:

- если это возможно, определить организации, в которые произошла утечка защищаемой информации;
- определить возможные контрмеры, призванные уменьшить ущерб от утечки информации.

Несанкционированное копирование или изменение конфиденциальной информации в текущий момент времени со стороны лиц, имеющих право доступа к ней

В случае обнаружения злоумышленника неправомерно копирующего, либо изменяющего защищаемую информацию выполняются следующие действия.

Первоочередные действия

1. Администратор ИБ прерывает несанкционированный процесс.
2. Администратор ИБ блокирует доступ к ИС Администрации для злоумышленника.
3. Администратор ИБ совместно с ответственным за защиту информации удаляют нарушителя от средств ИС.
4. Ответственным за защиту информации совместно с администратором ИБ предпринимаются действия по сбору и обеспечению сохранности улик.

Последующие действия

Создается комиссия для расследования инцидента.

Подключение технических средств к средствам и системам ОИ в текущий момент времени

В случае обнаружения злоумышленника, производящего подключение к техническим средствам и системам ОИ в текущий момент времени, выполняются следующие действия.

Первоочередные действия

1. Администратор ИБ прерывает процесс работы нарушителя.
2. В случае если нарушитель – пользователь ИС, администратор ИБ блокирует доступ в ИС Администрации для нарушителя.

Последующие действия

Создается комиссия для расследования инцидента.

Установка закладных устройств злоумышленником в текущий момент времени

В случае обнаружения злоумышленника, устанавливающего закладочные устройства, выполняются следующие действия.

Первоочередные действия

Администратор ИБ принимает меры к задержанию злоумышленника.

Последующие действия

Создается комиссия для расследования инцидента.

Приложение № 10
к Политике информационной
безопасности в администрации
города Сочи

ИНСТРУКЦИЯ

пользователя информационных систем администрации города Сочи

1. ФУНКЦИИ И ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЕЙ

1.1. Каждый служащий Администрации, участвующий в рамках своих функциональных обязанностей в процессах обработки конфиденциальной информации (КИ) и имеющий доступ к аппаратным средствам, программному обеспечению и данным в информационных системам Администрации (далее – ИС), несет персональную ответственность за свои действия и обязан:

1.1.1. строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИС;

1.1.2. выполнять свои функциональные обязанности строго в рамках прав доступа к внутренним и внешним информационным ресурсам, техническим средствам, полученным в установленном порядке;

1.1.3. знать и строго выполнять правила работы со средствами защиты информации, установленными в ИС;

1.1.4. хранить в тайне свой пароль (пароли);

1.1.5. исполнять требования «Порядка парольной защиты в ИС», «Инструкции по организации антивирусной защиты ИС», а также других документов, регламентирующих вопросы работы в ИС и обеспечение безопасности информации в части, его касающейся;

1.1.6. немедленно ставить в известность администратора ИБ и руководителя подразделения в случае утери личных реквизитов доступа, при компрометации личных паролей, подозрении на совершение попыток несанкционированного доступа (НСД) к персональным электронно-вычислительным машинам (ПЭВМ), обнаружении несанкционированных изменений в конфигурации программных или аппаратных средств ИС;

1.1.7. немедленно ставить в известность администратора ИС при обнаружении отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию ИС, выхода из строя или неустойчивого функционирования устройств ПЭВМ (дисководов, принтера и т.п.), а также перебоев в

системе электроснабжения, некорректного функционирования установленных технических средств защиты информации;

1.1.8. при обработке на ПЭВМ защищаемой информации присутствовать при работах по внесению изменений в аппаратно-программную конфигурацию закрепленной за ним ПЭВМ в подразделении;

1.1.9. при обработке на ПЭВМ защищаемой информации и необходимости использовать носители информации, применять только учтенные носители.

1.2. Служащим ЗАПРЕЩАЕТСЯ:

1.2.1. использовать компоненты программного и аппаратного обеспечения ИС в неслужебных целях;

1.2.2. хранить и обрабатывать личную информацию на ПЭВМ и серверах ИС;

1.2.3. использовать в работе неучтенные носители информации (например, USB-flash накопители);

1.2.4. использовать для работы в сетях общего пользования (Интернет) личные USB-модемы, телефоны в режиме модема и иные личные средства обеспечения доступа в сети Интернет;

1.2.5. КАТЕГОРИЧЕСКИ запрещено передавать и обсуждать информацию ограниченного доступа при помощи мобильных и иных устройств с использованием программ-мессенджеров WhatsApp, Viber и иных аналогичных, фотографировать и пересылать документы (в том числе документы, открытые на экране ПЭВМ), содержащие информацию ограниченного доступа;

1.2.6. при работе в сетях связи общего пользования (Интернет):

1.2.6.1. использовать информационные ресурсы сети Интернет, содержание которых нарушает действующее законодательство Российской Федерации;

1.2.6.2. использовать информационные ресурсы сети Интернет для целей, не связанных с областью производственной деятельности пользователя;

1.2.6.3. использовать информационные ресурсы сети Интернет в личных целях;

1.2.6.4. вносить изменения в состав и/или процесс работы внешних информационных ресурсов, если такие изменения не санкционированы собственником (владельцем) соответствующего ресурса;

1.2.6.5. пользоваться ресурсами электронной почты на доменах, не принадлежащих администрации города Сочи (@sochiadm.ru).

1.2.7. самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ИС или устанавливать дополнительно любые программные и аппаратные средства;

1.2.8. оставлять без присмотра включенную ПЭВМ, не заблокировав её;

1.2.9. оставлять без личного присмотра на рабочем месте или где бы то ни было свои персональные реквизиты доступа;

1.2.10. оставлять без личного присмотра в легкодоступном месте на рабочем месте или где бы то ни было свои машинные носители и распечатки, содержащие сведения ограниченного распространения;

1.2.11. использовать в работе неучтенные носители информации для обработки защищаемой информации;

1.2.12. устанавливать и использовать стороннее программное обеспечение без согласования с Администратором информационных систем (ИС) и Администратором информационной безопасности (ИБ).

1.2.13. открывать скачанные из сети Интернет, либо полученные по каналам электронной почты файлы, без предварительной проверки Антивирусом, о случаях попыток пересылки файлов, зараженных вирусами, а также исполняемых файлов (приложений) по электронной почте, НЕМЕДЛЕННО сообщать Администратору ИБ и Администратору ИС, при этом ЗАПРЕЩАЕТСЯ запускать эти файлы на исполнение или открытие;

1.2.14. умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, об обнаружении такого рода ошибок – ставить в известность администратора ИБ и руководителя своего Подразделения.

2. ОТВЕТСТВЕННЫЕ ЗА ОРГАНИЗАЦИЮ И КОНТРОЛЬ ВЫПОЛНЕНИЯ ИНСТРУКЦИИ

2.1. Ответственность за соблюдение требований настоящей Инструкции пользователями возлагается на всех служащих Администрации, участвующих в обработке КИ.

2.2. Ответственность за организацию контрольных и проверочных мероприятий возлагается на Администратора ИБ.

2.3. Ответственность за общий контроль информационной безопасности возлагается на ответственного за защиту информации Администрации.

Начальник управления информационных ресурсов администрации города Сочи А.В.Похлебаев

Приложение № 11
к Политике информационной безопасности в администрации города Сочи

ИНСТРУКЦИЯ

по действиям пользователей информационных систем администрации города Сочи в нештатных ситуациях

ОБЩИЕ ПОЛОЖЕНИЯ

Настоящая инструкция по действиям пользователей информационных систем в нештатных ситуациях (далее – Инструкция) предназначена для определения порядка действий пользователей информационных систем (ИС) администрации города Сочи (далее – Администрация) при возникновении нештатных ситуаций.

Нештатными ситуациями являются:

1) разглашение информации, относящейся к конфиденциальной, в том числе персональных данных (далее – защищаемая информация), служащими Администрации, имеющими к ней право доступа, в том числе:

- разглашение информации лицам, не имеющим права доступа к защищаемой информации;
- передача (попытка передачи) защищаемой информации по открытым линиям связи;
- обработка защищаемой информации на незащищенных технических средствах обработки информации;
- опубликование защищаемой информации в открытой печати и других средствах массовой информации;
- передача носителя информации лицу, не имеющему права доступа к ней;
- утрата носителя с защищаемой информацией;

2) неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации:

- несанкционированное изменение защищаемой информации;
- несанкционированное копирование защищаемой информации.

3) несанкционированный доступ к защищаемой информации:

- подключение несанкционированных технических средств (ТС) к средствам и системам объекта информатизации (ОИ);
- использование закладных устройств;
- маскировка под зарегистрированного пользователя;
- использование дефектов программного обеспечения ОИ;
- использование программных закладок;

- применение программных вирусов;
- хищение носителя защищаемой информации;
- нарушение функционирования ТС обработки информации;
- блокирование доступа к защищаемой информации путем перегрузки ТС обработки информации ложными заявками на ее обработку;

4) дефекты, сбои, отказы, аварии ТС и систем ОИ;

5) дефекты, сбои и отказы программного обеспечения ОИ;

6) сбои, отказы и аварии систем обеспечения ОИ;

7) природные явления, стихийные бедствия:

- термические, климатические факторы (пожары, наводнения и т.д.);
- механические факторы (землетрясения и т.д.);
- электромагнитные факторы (грозовые разряды и т.д.).

В случае возникновения нештатной ситуации, порядок действий при которой не регламентирован настоящей Инструкцией, администратором информационной безопасности (ИБ), ответственным за защиту информации, вырабатывается конкретный план действий с учетом текущей ситуации.

Резервируемые в Администрации информационные ресурсы и способы их резервирования представлены в Приложении 1 к настоящей Инструкции.

Порядок оповещения должностных лиц и сроки выполнения мероприятий при нештатных ситуациях определены в приложении 2 к настоящей Инструкции.

Для эффективной реализации мероприятий по реагированию в случае нештатных ситуаций должны проводиться регулярные тренировки по различным нештатным ситуациям. По результатам тренировки в случае необходимости проводится уточнение настоящей Инструкции.

Ознакомление с требованиями Инструкции служащих Администрации осуществляет администратор ИБ под роспись с выдачей электронных копий соответствующих приложений и разделов Инструкции непосредственно для повседневного использования в работе.

ПОРЯДОК ДЕЙСТВИЙ ПРИ ОБНАРУЖЕНИИ НЕШТАТНЫХ СИТУАЦИЙ

Классификация нештатных ситуаций

Нештатные ситуации классифицируются в соответствии с оценками, представленными в таблице 1.

Таблица 1. Оценки нештатных ситуаций

Нештатная ситуация		Оценка ситуации (раздел Инструкции)
Разглашение защищаемой информации служащими, имеющими к ней право доступа		(0)
Неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации	Несанкционированное копирование защищаемой информации	Обнаружился случившийся факт (0)
		Производится в текущий момент (0)
	Несанкционированное изменение защищаемой информации	Обнаружился случившийся факт (0)
		Производится в текущий момент (0)
Несанкционированный доступ к защищаемой информации	Подключение технических средств к средствам и системам объекта информатизации (ОИ)	Обнаружился случившийся факт (0)
		Производится в текущий момент (0)
	Установка закладочных устройств	Обнаружение установленных (0)
		Устанавливаются в настоящий момент (0)
	Маскировка под зарегистрированного пользователя	Внешним злоумышленником в текущий момент (0)
		Внутренним злоумышленником либо производилась в прошлом (0)
	Использование дефектов программного обеспечения ОИ	Внешним злоумышленником в текущий момент (0)
		Внутренним злоумышленником либо производилось в прошлом (0)
	Использование программных закладок	Внешним злоумышленником в текущий момент (0)
		Внутренним злоумышленником либо производилось в прошлом (0)
	Обнаружение программных вирусов	(0)
	Хищение носителя защищаемой информации	(0)
	Нарушение функционирования ТС обработки информации злоумышленником	Производится в текущий момент (0)
		Обнаружился случившийся факт (0)
	Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку	Производится в текущий момент внешним злоумышленником (0)
		Производится в текущий момент внутренним злоумышленником (0)
		Обнаружился случившийся факт (0)
Ошибки пользователей системы при эксплуатации программных средств, ТС, средств и систем защиты информации		Ошибка повлекла утерю или повреждение защищаемой информации (0)

Маскировка под зарегистрированного пользователя внешним злоумышленником в текущий момент времени

В случае обнаружения внешнего злоумышленника, маскирующегося под зарегистрированного пользователя, выполняются следующие действия.

Первоочередные действия

Администратор ИБ блокирует доступ к ИС Администрации для злоумышленника.

Последующие действия

Создается комиссия для расследования инцидента.

Использование дефектов программного обеспечения ОИ внешним нарушителем в текущий момент времени

В случае обнаружения использования дефектов программного обеспечения ОИ внешним нарушителем в текущий момент времени выполняются следующие действия.

Первоочередные действия

Администратор ИБ блокирует доступ из внешних сетей к оборудованию, на котором используется уязвимое ПО.

Последующие действия

Создается комиссия для расследования инцидента.

Использование программных закладок внешним нарушителем в текущий момент времени

В случае обнаружения использования программной закладки внешним нарушителем в текущий момент времени выполняются следующие действия.

Первоочередные действия

Администратор ИБ блокирует доступ из внешних сетей к оборудованию, на котором установлена программная закладка.

Последующие действия

1. Администратор ИБ определяет возможный ущерб, нанесенный программной закладкой.
2. Администратор ИБ проводит мероприятия по обнаружению внедренных программных закладок и их нейтрализации, планирует и организует мероприятия по предотвращению повторения, нейтрализации последствий инцидента.
3. Составляется акт об инциденте.

Обнаружение программных вирусов

В случае обнаружения программных вирусов выполняются действия предусмотренные Инструкцией по антивирусной защите.

Нарушение функционирования ТС обработки информации в текущий момент времени злоумышленником

В случае обнаружения злоумышленника, нарушающего функционирование ТС обработки информации в текущий момент времени, выполняются следующие действия.

Первоочередные действия

1. Администратор ИБ принимает меры по немедленному удалению злоумышленника от средств вычислительной техники.
2. В случае если злоумышленник является пользователем системы, администратор ИБ блокирует доступ к ИС Администрации для злоумышленника.

Последующие действия

1. В случае наличия повреждений администратор ИБ определяет ущерб, нанесенный ТС и информации.
2. Администратор ИБ производит восстановление работоспособности системы.
3. Создается комиссия для расследования инцидента.

Обнаружение нарушения функционирования ТС обработки информации, произведенного злоумышленником

В случае обнаружения нарушений в функционировании ТС обработки информации, выполняются следующие действия.

1. Администратор ИБ определяет возможный круг лиц, причастных к нарушению функционирования ТС, определяет объем повреждений техническим и информационным ресурсам.
2. Администратор ИБ производит восстановление работоспособности системы.
3. Создается комиссия для расследования инцидента.

Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку внешним злоумышленником в текущий момент времени

В случае обнаружения внешней атаки, направленной на блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку в текущий момент времени, выполняются следующие действия.

Первоочередные действия

1. Администратор ИБ выявляет источник ложных заявок.

2. Администратор ИБ вырабатывает решение по блокированию потока ложных заявок и реализует выбранное решение.

Последующие действия

1. Администратор ИБ уведомляет провайдера, от которого идут ложные заявки, планирует и организует мероприятия по предотвращению повторения, нейтрализации последствий инцидента.

2. Администратор ИБ составляет акт об инциденте.

Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку внутренним злоумышленником в текущий момент времени

В случае обнаружения внутренней атаки, направленной на блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку в текущий момент времени, выполняются следующие действия:

1. Администратор ИБ выявляет источник ложных заявок и блокирует доступ к ИС Администрации для злоумышленника.

2. Создается комиссия для расследования инцидента.

Блокировка доступа к защищаемой информации, произошедшая в прошлом

При обнаружении факта блокировки доступа к защищаемой информации, произошедшей в прошлом, выполняются следующие действия.

1. Администратор ИБ выявляет источник ложных заявок.

2. В случае если злоумышленник является внешним, администратор ИБ уведомляет провайдера, от которого идут ложные заявки. Планирует и организует мероприятия по предотвращению повторения, нейтрализации последствий инцидента.

3. В случае если злоумышленник является внутренним, администратор ИБ составляет акт об инциденте.

4. Создается комиссия для расследования инцидента.

Ошибки пользователей системы при эксплуатации ТС, программных средств, средств и систем защиты информации, повлекшие утерю или повреждение защищаемой информации

В случае обнаружения ошибок пользователей системы при эксплуатации ТС, программных средств, средств и систем защиты информации, повлекшие утерю или повреждение защищаемой информации, выполняются следующие действия.

Первоочередные действия

1. Администратор ИБ проводит анализ и идентификацию причин инцидента.

2. В случае возможности злоумышленных действий выполняется последовательность действий, предусмотренная в соответствующем разделе Инструкции.

3. Администратор ИБ определяет ущерб, нанесенный нештатной ситуацией.

4. Администратор ИБ проводит мероприятия по восстановлению работоспособности системы и информации.

Последующие действия

1. Проводится проверка знаний пользователя, виновного в инциденте, а в случае необходимости его обучение.

2. Администратор ИБ составляет акт об инциденте, в случае необходимости выносит предложение Главе города Сочи о применении дисциплинарной меры в отношении нарушителя.

Ошибки пользователей системы при эксплуатации ТС, программных средств, средств и систем защиты информации, повлекшие нарушение работоспособности ТС и ПО

В случае обнаружения ошибок пользователей системы при эксплуатации ТС, программных средств, средств и систем защиты информации, повлекшие нарушение работоспособности ТС и ПО, выполняются следующие действия.

Первоочередные действия

1. Администратор ИБ проводит анализ и идентификацию причин инцидента.

2. В случае возможности злоумышленных действий выполняется последовательность действий, предусмотренная в соответствующем разделе Инструкции.

Последующие действия

1. Администратор ИБ определяет ущерб, нанесенный нештатной ситуацией, восстанавливают работоспособность системы.

2. Администратор ИБ составляет акт об инциденте, в случае необходимости выносит предложение Руководителю Администрация о применении дисциплинарной меры в отношении нарушителя.

3. Проводится проверка знаний пользователя виновного в инциденте, а в случае необходимости его обучение.

Дефекты, сбои, отказы, аварии ТС, программных средств и систем ОИ

В случае возникновения дефектов, сбоев, отказов, аварий ТС и систем ОИ выполняются следующие действия.

Первоочередные действия

1. Администратор ИБ выявляет возможные причины проявления дестабилизирующих факторов.

2. В случае наличия злоумышленных действий выполняется порядок действий в соответствии с Приложением 2.

Последующие действия

1. Администратор ИБ восстанавливает работоспособность систем.

2. В случае потери данных администратором ИБ по возможности проводится восстановление их из резервных копий.

3. Администратором ИБ производится составление акта.

Сбои, отказы и аварии систем обеспечения ОИ

В случае сбоев, отказов и аварий систем электроснабжения, вентиляции, других обеспечивающих инженерных систем выполняется следующая последовательность действий.

1. В случае если наблюдается продолжительное отключение электропитания. Администратором ИБ производится отключение ТС до момента истечения резервов системы бесперебойного питания.

2. Ответственным за материально-техническое обеспечение организуются работы по максимально быстрому восстановлению систем обеспечения.

3. В случае потери защищаемых данных администратором ИБ по возможности проводится восстановление их из резервных копий.

4. Администратором ИБ и ответственным за материально-техническое обеспечение производится составление акта.

Природные явления, стихийные бедствия, несущие угрозу жизни человека

В случае проявления стихийных бедствий и природных явлений, которые несут угрозу жизни человека, выполняются следующие действия:

1. Все служащие (руководители подразделений в том числе) обязаны личные реквизиты защиты (например: металлические и/или электронные ключи, карты-идентификаторы, ключевые носители, печати и пр.) собрать и упаковать в водонепроницаемый пакет (непосредственный руководитель обеспечивает заранее) и лично обеспечивать сохранность этого пакета во время эвакуации.

2. По «Списку имущества и(или) документов в личном пользовании служащего, подлежащего эвакуации в первую очередь» (разрабатываются служащими заранее и постоянно хранятся на рабочем месте) произвести сбор, упаковку, опись (в двух экз. – 1 экз. в тару) документов и технических средств в водонепроницаемую тару (обеспечивает заранее непосредственный руководитель). Упакованное имущество служащий передает под роспись (на своем экз. описи) лицам, обеспечивающим доставку имущества на эвакопункт, либо лично сопровождает груз во время его транспортировки.

3. Служащий вкладывает в вышеназванный пакет картонную табличку с указанием текущей даты, своих персональных данных (ФИО, наименование организации, номер служебного телефона) и содержащую опись содержимого пакета, заверенную собственноручной подписью.

Руководители обязаны собрать в помещениях подразделения и лично упаковать, (и далее лично хранить, как свои) реквизиты защиты и документы (согласно спискам первой очереди) тех служащих, которых на момент эвакуации нет на рабочем месте (болезнь, командировка, учеба, отпуск и т.д.).

Руководители обязаны:

- при подготовке к эвакуации проверить обеспеченность (а при отсутствии – обеспечить) служащих подразделения упаковочным материалом, списками документов, дел и имущества, подлежащих эвакуации в первую очередь;
- перед выездом в эвакопункт – проконтролировать исполнение задач эвакуации, приняв соответствующие доклады от служащих о готовности к эвакуации, провести выборочную проверку готовности (комплектности) документов, дел, имущества подразделения и/или ИС к эвакуации.

Природные явления, стихийные бедствия, не несущие угрозу жизни человека

В случае проявления стихийных бедствий и природных явлений, которые не несут угрозу жизни и/или человека, выполняются следующие действия:

1. Служащие Администрации выключают свои персональные компьютеры.

2. Администратор ИС выключает серверы и сетевое оборудование.

3. Администратор ИБ принимает меры к эвакуации резервных копий с информацией, системных блоков компьютеров, содержащих особо ценную информацию, документов и другого имущества. В первую очередь эвакуируется имущество по «Списку имущества и(или) документов в личном пользовании служащего, подлежащего эвакуации в первую очередь».

4. В случае локальных пожаров и частичных затоплений ответственным за материально-техническое обеспечение организуются работы по ликвидации нештатной ситуации и ее последствий.

ПРОВЕДЕНИЕ РАССЛЕДОВАНИЙ ОПАСНЫХ СИТУАЦИЙ

Для расследования опасных ситуаций в случаях, предусмотренных настоящей Инструкцией может создаваться комиссия. В состав комиссии должны входить:

- председатель;
- ответственный за обеспечение ЗИ;
- администратор ИБ;
- другие лица по решению председателя комиссии.

Деятельность комиссии должна по возможности происходить в режиме конфиденциальности.

В общем случае комиссия проводит:

- анализ и идентификацию причин инцидента, определение виновных;
- определение ущерба, нанесенного нештатной ситуацией;
- планирование мер для предотвращения повторения, нейтрализации последствий (если это возможно);
- анализ и сохранение доказательств, следов инцидента, улик и свидетельств;
- определение меры взыскания с виновного;
- взаимодействие, при необходимости с правоохранительными органами.

При сохранении улик, если есть возможность, администратором ИБ производится резервное копирование системной и защищаемой информации технических средств, вовлеченных в инцидент, включая логи (контрольные записи).

По результатам деятельности комиссии составляется акт с описанием ситуации. К акту прилагаются поясняющие материалы (копии экрана, распечатки журнала событий, и др.).

По результатам расследования администраторами организуются мероприятия по реализации предложенных комиссией мер для предотвращения либо уменьшения вероятности проявления, подобных инцидентов в дальнейшем.

При проведении расследований, кроме того, необходимо ответить на следующие вопросы:

- можно ли было предупредить нештатную ситуацию?
- вызвана ли она слабостью средств защиты и регистрации?
- это первая кризисная ситуация такого рода?
- достаточно ли имеющегося резерва?
- есть ли необходимость пересмотра системы защиты?

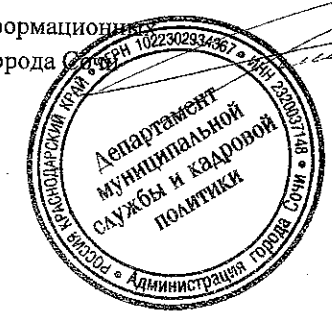
- есть ли необходимость пересмотра настоящей инструкции?

ОТВЕТСТВЕННЫЕ ЗА КОНТРОЛЬ ВЫПОЛНЕНИЯ ИНСТРУКЦИИ

Ответственными за постоянный контроль выполнения требований данной Инструкции являются:

- администратор ИБ в части задач, возложенных на него настоящей инструкцией;
- ответственный за защиту информации в части общего контроля информационной безопасности;
- ответственный за материально-техническое обеспечение, в части задач, возложенных на него настоящей инструкцией.

Начальник управления информационных ресурсов администрации города Сочи А.В.Похлебаев



Приложение № 1
к Инструкции по действиям
пользователей информационных
систем администрации города
Сочи в нештатных ситуациях

СРЕДСТВА ОБЕСПЕЧЕНИЯ НЕПРЕРЫВНОЙ РАБОТЫ И ВОССТАНОВЛЕНИЯ

Резервному копированию (РК) подлежит следующая информация:

- системные программы и наборы данных - *невозобновляемому (однократному, эталонному) РК*;
- прикладное программное обеспечение и наборы данных - *невозобновляемому РК*;
- наборы данных, генерируемые в течение рабочего дня и содержащие ценную информацию (журналы транзакций, системный журнал и т.д.) - *периодическому возобновляемому РК*.

Резервному копированию в ИС подлежат следующие программные и информационные ресурсы:

Наименование информационного ресурса	Где размещается ресурс в системе	Вид резервного копирования	Ответственный за резервное копирование (используемые технические средства)	Где хранится резервная копия	Частота периодического резервирования
Информация ИС		Периодическое, возобновляемое	Администратор ИБ		Каждую пятницу
Эталонное программное обеспечение		Невозобновляемое	Администратор ИБ		Обновляется при появлении нового ПО

Начальник управления информационных ресурсов администрации города Сочи А.В.Похлебаев

Приложение № 2
к Инструкции по действиям
пользователей информационных
систем администрации города
Сочи в нештатных ситуациях

ПЛАН
ОБЕСПЕЧЕНИЯ НЕПРЕРЫВНОЙ РАБОТЫ И ВОССТАНОВЛЕНИЯ ИНФОРМАЦИИ

Тип кризисной ситуации	Критерии кризисной ситуации	Кому [1] и в какие сроки докладывается		Срок реализации первоочередных действий	Максимальное время для выполнения всех мероприятий
		В рабочее время	В нерабочее время		
Неправомерные действия со стороны лиц допущенных к защищаемой информации					
Разглашение защищаемой информации служащими, имеющими к ней право доступа		Администратору ИБ сразу после обнаружения инцидента	Администратору ИБ как можно скорее, в дневное время, но не позднее 8 часов после инцидента		
Обнаружение несанкционированно скопированной или измененной конфиденциальной информации		Администратору ИБ сразу после обнаружения инцидента	Администратору ИБ как можно скорее, в дневное время, но не позднее 8 часов после инцидента		

[1] В случае отсутствия лиц, которые должны опсвещаться, их замещают лица, определенные в разделе «Порядок замещения ответственных лиц» настоящей Инструкции. Либо могут быть оповещены непосредственные руководители

Несанкционированное копирование или изменение конфиденциальной информации в текущий момент времени со стороны лиц имеющих право доступа к ней		Администратору ИБ сразу после обнаружения инцидента	Администратору ИБ сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	
Несанкционированный доступ к информации					
Обнаружение подключения технических средств к средствам и системам объекта информатизации		Администратору ИБ сразу после обнаружения инцидента	Администратору ИБ как можно скорее, в дневное время, но не позднее 8 часов после инцидента		
Подключение технических средств к средствам и системам ОИ в текущий момент времени		Администратору ИБ сразу после обнаружения инцидента	Администратору ИБ сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	
Обнаружение закладочных устройств		Администратору ИБ сразу после обнаружения инцидента	Администратору ИБ как можно скорее, в дневное время, но не позднее 8 часов после инцидента		
Установка закладочных устройств злоумышленником в текущий момент времени		Администратору ИБ сразу после обнаружения инцидента	Администратору ИБ сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	
Маскировка под зарегистрированного пользователя внешним злоумышленником в текущий момент времени		Администратору ИБ сразу после обнаружения инцидента	Администратору ИБ сразу после обнаружения инцидента	5 минут в рабочее время (1 час в нерабочее)	
Маскировка под зарегистрированного пользователя внутренним		Администратору ИБ сразу после обнаружения инцидента	Администратору ИБ как можно скорее, в дневное время, но не позднее 8		

злоумышленником или обнаружением факта маскировки			часов после инцидента		
Использование дефектов программного обеспечения ОИ внешним нарушителем в текущий момент времени		Администратору ИБ сразу после обнаружения инцидента	Администратору ИБ сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	
Использование программных закладок внешним нарушителем в текущий момент времени		Администратору ИБ сразу после обнаружения инцидента	Администратору ИБ сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	
Использование программных закладок внутренним злоумышленником или обнаружение факта использования		Администратору ИБ сразу после обнаружения инцидента	Администратору ИБ как можно скорее, в дневное время, но не позднее 8 часов после инцидента		
Обнаружение программных вирусов		Администратору ИБ сразу после обнаружения инцидента	Администратору ИБ как можно скорее, в дневное время, но не позднее 8 часов после инцидента		12 часов
Хищение носителя защищаемой информации		Администратору ИБ сразу после обнаружения инцидента	Администратору ИБ как можно скорее, в дневное время, но не позднее 8 часов после инцидента		
Нарушение функционирования ТС обработки информации в текущий момент времени злоумышленником	Нарушена работа одного пользователя	Администратору ИБ сразу после обнаружения инцидента	Администратору ИБ сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	2 дня
	Нарушена	Администратору ИБ	Администратору ИБ	10 минут в	1 день

	работа группы пользователей	сразу после обнаружения инцидента	сразу после обнаружения инцидента	рабочее время (1 час в нерабочее)	
Обнаружение нарушения функционирования ТС обработки информации произведенного злоумышленником	Нарушена работа одного пользователя	Администратору ИБ сразу после обнаружения инцидента	Администратору ИБ сразу после обнаружения инцидента		2 дня
	Нарушена работа группы пользователей	Администратору ИБ сразу после обнаружения инцидента	Администратору ИБ сразу после обнаружения инцидента		1 день
Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку					
Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку внешним злоумышленником в текущий момент времени		Администратору ИБ сразу после обнаружения инцидента	Администратору ИБ как можно скорее, в дневное время, но не позднее 8 часов после инцидента	20 минут в рабочее время (1 час в нерабочее)	7 дней
Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку внутренним злоумышленником в текущий момент времени		Администратору ИБ сразу после обнаружения инцидента	Администратору ИБ как можно скорее, в дневное время, но не позднее 8 часов после инцидента	20 минут в рабочее время (1 час в нерабочее)	1 день

Обнаружение произошедшего факта блокировки доступа к защищаемой информации		Администратору ИБ сразу после обнаружения инцидента	Администратору ИБ как можно скорее, в дневное время, но не позднее 8 часов после инцидента		1 день
Ошибки пользователей системы					
Ошибки пользователей системы при эксплуатации ТС, программных средств, средств и систем защиты информации, повлекшие утерю или повреждение защищаемой информации		Администратору ИБ сразу после обнаружения инцидента	Администратору ИБ как можно скорее, в дневное время, но не позднее 8 часов после инцидента	2 часа в рабочее время (12 часов в нерабочее)	1 день
Ошибки пользователей системы при эксплуатации ТС, программных средств, средств и систем защиты информации, повлекшие нарушение работоспособности ТС и ПО	Нарушена работа одного пользователя	Администратору ИБ сразу после инцидента	Администратору ИБ в первый рабочий день после инцидента	20 минут	2 дня
	Нарушена работа группы пользователей	Администратору ИБ сразу после обнаружения инцидента	Администратору ИБ сразу после обнаружения инцидента	20 минут	1 день
Объективные факторы					
Дефекты, сбои, отказы, аварии ТС, программных средств и систем ОИ	Сбой ТС и систем ОИ	Администратору ИБ сразу после инцидента	Администратору ИБ сразу после инцидента	1 час	2 дня
	Отказ ТС и систем ОИ, затронувший работу группы пользователей	Администратору ИБ сразу после обнаружения инцидента	Администратору ИБ как можно скорее, в дневное время, но не позднее 8 часов после инцидента	1 час в рабочее время (8 часов в нерабочее)	1 день

	Отказ ТС и систем ОИ, затронувший работу одного пользователя	Администратору ИБ сразу после инцидента	Администратору ИБ в первый рабочий день после инцидента	1 час	2 дня
	Авария ТС и систем ОИ	Администратору ИБ сразу после обнаружения инцидента	Администратору ИБ как можно скорее, в дневное время, но не позднее 8 часов после инцидента	1 час	1 день
Сбои, отказы и аварии систем обеспечения ОИ	Сбой систем обеспечения ОИ	Ответственному за материально-техническое обеспечение сразу после инцидента	Ответственному за материально-техническое обеспечение в первый рабочий день после инцидента		
	Отказ систем обеспечения ОИ, затронувший работу группы пользователей	Ответственному за материально-техническое обеспечение и Администратору ИБ сразу после обнаружения инцидента	Ответственному за материально-техническое обеспечение и Администратору ИБ сразу после обнаружения инцидента		1 день
	Отказ систем обеспечения ОИ, затронувший работу одного пользователя	Ответственному за материально-техническое обеспечение сразу после инцидента	Ответственному за материально-техническое обеспечение в первый рабочий день после инцидента		2 дня

	Авария систем обеспечения ОИ	Ответственному за материально-техническое обеспечение, Администратору ИБ сразу после обнаружения инцидента	Ответственному за материально-техническое обеспечение, Администратору ИБ как можно скорее, в дневное время, но не позднее 8 часов после инцидента		1 день
Природные явления, стихийные бедствия, несущие угрозу жизни человека		Руководителю, заместителям Руководителю, которые оповещают всех своих служащих сразу после получения информации	Руководителю, заместителям Руководителю, которые оповещают всех своих служащих сразу после получения информации		30 минут
Природные явления, стихийные бедствия, не несущие угрозу жизни человека		Руководителю, заместителям Руководителю, Администратору ИБ	Руководителю, заместителям Руководителю, Администратору ИБ		30 минут

Начальник управления информационных ресурсов
администрации города Сочи А.В.Похлебаев

Приложение № 3
к Инструкции по действиям
пользователей информационных
систем администрации города
Сочи в нештатных ситуациях

ЖУРНАЛ

учета нештатных ситуаций

№ п/п	Дата, ИС , ПЭВМ, описание ситуации, выполненные работы	Подпись исполнителя	Подпись администратора

Начальник управления информационных ресурсов администрации города Сочи А.В.Похлебаев

Приложение № 12
к Политике информационной
безопасности в администрации
города Сочи

ИНСТРУКЦИЯ

по использованию съемных накопителей информации в администрации города Сочи

1. ФУНКЦИИ И ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЕЙ

1.1 Каждый служащий Администрации, которому необходим доступ к использованию USB-флеш накопителей, флеш-карт, съемных жестких дисков и иных съемных носителей информации ОБЯЗАН:

– строго соблюдать установленные правила обеспечения безопасности информации при работе накопителями;

– использовать накопители исключительно в рабочих целях;

– пользоваться только учтенными установленным порядком носителями;

– при необходимости использования накопителя, известить непосредственного руководителя, и оформить заявку на регистрацию носителя в АИС Администрации;

– при каждом подключении накопителя проводить антивирусную проверку подключаемого устройства;

– немедленно ставить в известность администратора ИБ в случае обнаружения вируса на подключенном носителе;

– немедленно ставить в известность администратора ИБ при обнаружении в своем персональном компьютере (далее - ПЭВМ) незарегистрированного носителя (забытого, либо специально оставленного иными лицами);

– при транспортировке носителей с информацией ограниченного доступа, принимать все возможные меры против утери или хищения носителя, или информации в процессе транспортировки;

1.2 Служащим ЗАПРЕЩАЕТСЯ:

– хранить и обрабатывать личную информацию на учтенных носителях;

– записывать и обрабатывать информацию ограниченного доступа на съемных носителях без прямой производственной необходимости;

– запускать на исполнение исполняемые файлы (*.exe, *.msi, *.bat, *.com и т.д.) либо пользоваться автозапуском с накопителей;

– использовать в работе неучтенные и незарегистрированные носители.

2. ПОРЯДОК РЕГИСТРАЦИИ НОСИТЕЛЕЙ

Для регистрации носителя и получения разрешения на его использование на ПЭВМ Администрации руководителю Подразделения необходимо:

2.1. Назначить ответственного служащего, который соберет информацию о необходимом количестве накопителей в структурном подразделении;
2.2. Оформить заявку на регистрацию (Приложение 2 к настоящей Инструкции);
2.3. Предоставить в Управление информационных ресурсов оформленную заявку и накопители на регистрацию.
2.4. В дальнейшем, при необходимости замены/добавления носителей действовать аналогичным образом.
2.5. Первичная регистрация носителей будет происходить с 10 до 13:00 каждый рабочий день по адресу: ул.Советская, 26, кабинет 39 с в течение месяца с момента утверждения Политики информационной безопасности в администрации города Сочи.
2.6. Дальнейшая регистрация носителей будет производиться по адресу: ул.Юных Ленинцев, 23, по согласованию с ответственным за регистрацию носителей.

3. ОТВЕТСТВЕННЫЕ ЗА ОРГАНИЗАЦИЮ И КОНТРОЛЬ ВЫПОЛНЕНИЯ ИНСТРУКЦИИ

3.1. Ответственность за соблюдение требований настоящей Инструкции пользователями возлагается на всех служащих Администрации, участвующих в обработке КИ.
3.2. Ответственность за организацию контрольных и проверочных мероприятий возлагается на администратора ИБ.
3.3. Ответственность за общий контроль информационной безопасности возлагается на ответственного за защиту информации Администрации.

Начальник управления информационных
ресурсов администрации города Сочи А.В.Похлебаев

Приложение № 1
К инструкции по пользованию
съемными накопителями

ФОРМА РЕГИСТРАЦИИ НАКОПИТЕЛЕЙ ИНФОРМАЦИИ

№	Наименование и GUID	Тип носителя	Подразделение	Должность пользователя	ФИО пользователя	Дата	Подпись
1.	Kingston KVSR-12201222, GUID 1222122121212	USB-флеш накопитель	Департамент имущественных отношений	Главный специалист	Иванов И.И.		

Начальник управления информационных
ресурсов администрации города Сочи А.В.Похлебаев

Департамент муниципальной службы и кадровой политики

Приложение № 2
К инструкции по пользованию
съемными накопителями

ФОРМА ЗАЯВКИ
НА РЕГИСТРАЦИЮ НОСИТЕЛЕЙ

_____

Наименование отраслевого (функционального), территориального органа

направляет информацию о съемных носителях, которые необходимо использовать в обеспечении деятельности. Прошу зарегистрировать и разрешить к работе на ПЭВМ администрации города Сочи носители согласно прилагаемому перечню.

№	Наименование	Тип носителя	Должность пользователя	ФИО пользователя	Дата	Подпись
1.	Kingston KVSR-12201222	USB-флеш накопитель	Главный специалист	Иванов И.И.		

_____ _____ _____

дата подпись расшифровка подписи

Начальник управления информационных ресурсов администрации города Сочи А.В.Похлебаев

Приложение № 13
к Политике информационной
безопасности в администрации
города Сочи

ИНСТРУКЦИЯ

по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств информационных систем администрации города Сочи

1. ОБЩИЕ ПОЛОЖЕНИЯ

Инструкция по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств информационных систем персональных данных (далее – Инструкция) администрации города Сочи (далее – Администрация), включает в себя описание комплекса организационно-технических мер по проведению работ по установке, модификации и техническому обслуживанию (ТО) программного обеспечения (ПО) и аппаратных средств ИС.

Требования настоящей Инструкции распространяются на всех должностных лиц и служащих подразделений Администрации, использующих в работе ресурсы информационных систем (ИС), в которых осуществляется обработка информации ограниченного доступа, не составляющей государственной тайны.

Непосредственное исполнение настоящей Инструкции определяется администратором ИБ по согласованию с ответственным за защиту информации Администрации.

2. ПОРЯДОК ПРОВЕДЕНИЯ РАБОТ

Все изменения конфигурации технических и программных средств рабочих станций Администрации должны производиться только на основании заявок руководителей структурных подразделений Администрации (приложение 1), согласованных с Руководителем управления информационных ресурсов администрации города Сочи. Производственная необходимость проведения указанных в заявке изменений подтверждается подписью руководителя структурного подразделения.

Все изменения конфигурации технических и программных средств рабочих станций и серверов, входящих в состав аттестованных по требованиям безопасности ИС Администрации, должны производиться только на основании заявок руководителей структурных подразделений Администрации (приложение 1), согласованных с Главой города Сочи.

Производственная необходимость проведения указанных в заявке изменений подтверждается подписью руководителя структурного подразделения. При этом необходимо уведомить об осуществленных изменениях организацию, производившую аттестацию, которая принимает решение о необходимости проведения контроля эффективности аттестованного объекта информатизации.

Все изменения конфигурации технических и программных средств, входящих в состав аттестованных по требованиям безопасности ИС Администрации, отражаются в Техническом паспорте объекта информатизации. Запрещается изменение состава (в том числе ввод новых) программных средств, осуществляющих обработку защищаемой информации на объектах информатизации, аттестованных по требованиям безопасности информации.

В заявке указываются наименование персональной электронной вычислительной машины (ПЭВМ) и ответственный за нее служащий. После чего заявка передается администратору ИБ для исполнения работ по внесению изменений в конфигурацию ПЭВМ.

Право внесения изменений в конфигурацию аппаратно-программных средств рабочих станций ИС Администрации предоставляется администратору ИБ, а также ответственному за защиту информации. Изменение конфигурации аппаратно-программных средств рабочих станций и серверов кем-либо без согласования с администратором ИБ и/или ответственным за защиту информации, запрещено.

Установка и настройка программного средства осуществляется администратором ИБ согласно эксплуатационной документации.

Запрещается установка и использование на ПЭВМ (серверах) ПО, не входящего в перечень ПО, разрешенного к использованию в Администрации.

Руководители структурных подразделений осуществляют контроль отсутствия на ПЭВМ служащих подразделения ПО и данных, не связанных с выполнением должностных обязанностей.

Установка (обновление) ПО (системного, тестового и т.п.) на средствах вычислительной техники производится с эталонных копий программных средств, хранящихся у администратора ИС. Все добавляемые программные и аппаратные компоненты должны быть предварительно проверены на работоспособность, а также отсутствие вредоносного программного кода в соответствии с «Инструкцией по организации антивирусной защиты ИС Администрации».

После установки (обновления) ПО администратор ИБ должен произвести настройку средств управления доступом к компонентам данной задачи (программного средства) в соответствии с требованиями к системе защиты информации и, совместно с пользователем ПЭВМ, проверить правильность настройки средств защиты.

В случае обнаружения недекларированных (не описанных в документации) возможностей программного средства, служащие немедленно

докладывают руководителю своего подразделения и администратору ИБ. Использование программного средства до получения специальных указаний запрещается.

При изъятии ПЭВМ из состава рабочих станций, обрабатывающих защищаемую информацию, ее передача на склад, в ремонт или в другое подразделение для решения иных задач осуществляется только после того, как администратор ИБ снимет с данной ПЭВМ средства защиты и предпримет необходимые меры для затирания (уничтожения) защищаемой информации, которая хранилась на дисках компьютера. Факт уничтожения данных, находившихся на диске компьютера, оформляется актом за подписью администратора ИС. Форма акта приведена в приложении 2.

Допуск новых пользователей к решению задач с использованием вновь развернутого ПО (либо изменение их полномочий доступа) осуществляется согласно «Инструкции по внесению изменений в списки пользователей и наделению их полномочиями доступа к ресурсам информационных систем, обрабатывающих конфиденциальную информацию, в Администрации».

Оригиналы заявок (документов), на основании которых производились изменения в составе технических или программных средств ПЭВМ с отметками о внесении изменений в состав аппаратно-программных средств должны храниться у администратора ИБ.

3. ОТВЕТСТВЕННЫЕ ЗА ОРГАНИЗАЦИЮ И КОНТРОЛЬ ВЫПОЛНЕНИЯ ИНСТРУКЦИИ

Ответственность за организацию контрольных и проверочных мероприятий по вопросам установки, модификации технических и программных средств возлагается на администратора ИБ.

Ответственность за общий контроль информационной безопасности возлагается на ответственного за защиту информации Администрации.

Начальник управления информационных ресурсов администрации города Сочи А.В.Похлебаев

Приложение № 1
К инструкции по установке,
модификации и техническому
обслуживанию программного
обеспечения и аппаратных средств

Начальнику управления
информационных ресурсов
администрации города Сочи

А.В. Похлебаеву

ЗАЯВКА

на внесение изменений в состав *программного (аппаратного)* обеспечения

(ненужное зачеркнуть)

_____

(наименование ПЭВМ)

Прошу дать указания ответственным служащим для организации *установки (изменения настроек)*

(ненужное зачеркнуть)

_____

(перечень ПО (аппаратных средств) и необходимых настроек)

для решения задач:_____

следующим пользователям:

_____

(фамилия, имя, отчество)

Руководитель отраслевого
(функционального)
территориального органа
администрации г.Сочи

«___» _____20__ г. _____ ФИО

Оборотная сторона заявки

Изменения на ПЭВМ *произведены (не произведены)* по следующей причине:
(ненужное зачеркнуть)

_____

_____

Выполнены следующие работы:

_____

_____

Выполнены следующие изменения в настройках средств защиты:

_____

_____

Администратор ИБ

«___» _____ 20__ г. _____ А.С. Десятерик

Начальник управления информационных
ресурсов администрации города Сочи _____ А.В.Похлебаев

Департамент муниципальной службы и кадровой политики
Краснодарский край • ОГРН 1022302934367 • ИНН 2320037148 • Администрация города Сочи

Приложение № 2
К инструкции по установке,
модификации и техническому
обслуживанию программного
обеспечения и аппаратных средств

АКТ

затирания остаточной информации, хранившейся на диске компьютера

Все файлы, содержащие подлежащую защите информацию, находившиеся на НЖМД

_____,

(модель, серийный номер)

передаваемого

_____

(с какой целью)

_____

(кому: должность, Ф.И.О.)

ПЭВМ:

_____

(наименование ПЭВМ)

уничтожены (затерты) посредством программы _____.

Администратор ИБ

«___» _____ 20__ г. С.С. Десятерик

Начальник управления
информационных ресурсов
администрации города Сочи А.В.Похлебаев

Приложение № 14
к Политике информационной
безопасности в администрации
города Сочи

ПОРЯДОК

парольной защиты в информационных системах администрации города Сочи

1. ОБЩИЕ ПОЛОЖЕНИЯ

Порядок парольной защиты в информационных системах (далее – Порядок) включает в себя взаимоувязанный комплекс организационно-технических мер, регламентирующих генерацию и/или выбор, использование, хранение, уничтожение парольной информации в информационных системах администрации города Сочи (далее – Администрация).

Требования настоящего Порядка являются неотъемлемой частью комплекса мер безопасности и защиты информации в Администрации.

Требования настоящего Порядка распространяются на всех должностных лиц и служащих подразделений Администрации, использующих в работе информационные системы (ИС), а также всех видов программного обеспечения (ПО), эксплуатируемого в Администрации.

В целях закрепления знаний по вопросам практического исполнения требований Порядка, разъяснения возникающих вопросов, проводятся (при необходимости) персональные инструктажи пользователей ИС Администрации.

2. ФУНКЦИИ СЛУЖАЩИХ

Непосредственное исполнение, организация и контроль исполнения требований настоящего Порядка в Администрации осуществляется всеми пользователями ИС, а именно:

– пользователь ИС:

а) регулярная (с частотой, установленной настоящим Порядком) смена используемой в работе парольной информации;

б) выбор парольной информации с качеством, установленным настоящим Порядком;

– администратор ИБ;

а) организационно-методическое обеспечение процессов генерации, смены и удаления паролей в ИС Администрации;

б) разработка всех необходимых инструкций по вопросам парольной защиты ИС Администрации;

в) организация доведения до пользователей ИС Администрации требований по парольной защите;

г) организация периодического и выборочного контроля исполнения служащими Администрации требований настоящего Порядка;

д) согласование выдачи управляющих учетных записей к ИС;

е) текущий контроль действий персонала Администрации по работе с паролями (автоматизированный контроль качества паролей – при наличии программно-технических средств);

ж) техническое обеспечение (при наличии программно-технических средств) процессов генерации/выбора, смены и удаления паролей, соответствующая конфигурация ИС.

3. КАЧЕСТВО И ОБРАЩЕНИЕ ПАРОЛЬНОЙ ИНФОРМАЦИИ

3.1.Пароли доступа к аппаратно-программным вычислительным средствам, информационным ресурсам Администрации формируются (выбираются) пользователями этих ресурсов с учетом следующих требований к качеству парольной информации:

№ п/п	Параметр качества пароля	Администратор	Пользователь
1.	Минимальная длина пароля в символах	10	6[1]
2.	Максимальная длина пароля в символах	32	16
3.	Содержание в пароле букв верхнего и нижнего регистра	да	да
4.	Алфавит пароля	Английский алфавит с использованием цифр и специальных символов	Английский алфавит с использование м цифр и специальных символов
5.	Содержание в пароле специальных символов (@, #, $, &, * и т.п.) и цифр	обязательно	рекомендуется
6.	Минимальное отличие нового пароля от предыдущего (в позициях)	3	3
7.	Максимальный срок действия пароля	30 дней	60 дней
8.	Дополнительный (типа ТМ, eToken[2] или другие	рекомендуется	рекомендуется

[1] При использовании электронных ключей (USB, Touch Memory) не менее 6 символов.

№ п/п	Параметр качества пароля	Администратор	Пользователь
	электронные ключи) идентификатор		
9.	Пароль на заставку монитора	да	да
10.	Максимальное количество неуспешных попыток аутентификации	3	5
11.	Блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации	10 минут	5 минут

3.2.Хранение служащим (администратором, пользователем) личных паролей допускается только в личном сейфе (запираемом шкафу, ящике), либо в сейфе (запираемом шкафу, ящике) администратора, либо в сейфе (запираемом шкафу, ящике) руководителя подразделения. При этом бумажный носитель должен быть упакован в отдельный опечатанный конверт.

3.3.ЗАПРЕЩАЕТСЯ использовать в пароле личных имен, фамилий, кличек домашних животных, № телефонов, дат рождения, географических названий, именований АРМ, общепринятых сокращений (ПЭВМ, ЛВС, USER, SYSOP и т.д.);

3.4.Личные пароли и/или дополнительные идентификаторы (электронные ключи) пользователи и администраторы никому не имеют права сообщать и(или) передавать[3].

3.5.В информационной системе должны быть запрещены любые действия до прохождения пользователями процедур идентификации и аутентификации.

3.6.Внеплановая смена/удаление пароля (и при возможности учетной записи) пользователя или администратора ИБ ИС в случае прекращения его полномочий должна производиться немедленно после окончания последнего сеанса работы данного пользователя с системой.

3.7.Внеплановая полная смена паролей должна производиться в случае прекращения полномочий администратора ИБ ИС, других служащих, которым по роду работы были предоставлены либо полномочия по управлению ИС, либо полномочия по управлению подсистемой защиты информации ИС[4].

[2] При использовании электронного ключа такого типа требования вышеприведенной таблицы актуальны только по пунктам №1 и №9.

[3] Служащие Администрации раскрывают значение своего пароля и/или передают физический идентификатор только своим непосредственным руководителям в случае производственной необходимости и/или при проведении контрольно-проверочных мероприятий. По окончании производственных и/или контрольно-проверочных работ служащие производят немедленную смену значений раскрытых паролей

[4] Смена паролей производится для учетных записей систем, в которых не используется аутентификация посредством дополнительных идентификаторов (Touch Memory, eToken и т.п.)

3.8.В случае компрометации пароля доступа в ИС администратором ИБ ИС должны быть немедленно предприняты меры в зависимости от полномочий владельца скомпрометированного пароля и обстоятельств компрометации.

3.9.Все пользователи ИС Администрации обязаны по первому требованию администратора ИБ ИС предъявить значения действующего личного пароля для контроля соответствия установленным требованиям, а после проверки провести немедленную его смену.

3.10. Администратор ИБ ИС, по согласованию с ответственным за защиту информации проводит ежеквартальный выборочный контроль выполнения служащими Администрации требований Порядка с отметками в отдельном журнале. О фактах несоответствия качества паролей и/или условий обеспечения их сохранности администратор ИБ ИС докладывает ответственному за защиту информации.

4. УПРАВЛЕНИЕ ИДЕНТИФИКАТОРАМИ И УЧЕТНЫМИ ЗАПИСЯМИ

4.1.Идентификаторы к аппаратно-программным вычислительным средствам, информационным ресурсам Управления формируются (выбираются) администратором ИБ с учетом следующих требований:

– идентификатор должен однозначно идентифицировать пользователя и (или) устройство;

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

– должно быть обеспечено блокирование идентификатора пользователя не более чем через 90 дней неиспользования.

4.2.Для информационной системы определены следующие типы учетных записей:

– внутренний пользователь;

– администратор информационной системы;

– администратор информационной безопасности.

4.3.В информационной системе должно обеспечиваться блокирование сеанса доступа пользователя после 15 минут бездействия (неактивности) в информационной системе или по запросу пользователя.

5. ОБРАЩЕНИЕ ДОПОЛНИТЕЛЬНЫХ ИДЕНТИФИКАТОРОВ

5.1.В целях усиления процедур идентификации и аутентификации в ИС Администрации, пользователи ИС могут использовать дополнительные индивидуальные электронные идентификаторы (смарт-карты, eToken и т.д.) совместно с личным паролем доступа.

5.2.Дополнительные идентификаторы выдаются и учитываются в соответствии с «Инструкцией по внесению изменений в списки пользователей и наделению их полномочиями доступа к ресурсам информационных систем»:

– служащие получают дополнительные идентификаторы под роспись;

– администратор ИБ ИС, по обращению к нему служащих, регистрирует дополнительные идентификаторы в ИС Администрации и инструктирует служащих с учетом требований настоящего порядка и правил эксплуатации для дополнительных идентификаторов.

5.3.Служащие Администрации, получившие в пользование дополнительные идентификаторы, лично обеспечивают надежное круглосуточное безопасное хранение и использование идентификаторов. Оставление идентификатора без присмотра запрещается.

5.4.В случае утери дополнительного идентификатора служащие немедленно ставят об этом в известность администратора ИБ ИС и своего непосредственного руководителя. Администраторы организуют немедленную блокировку утерянных ключей в автоматизированных системах.

6. ОТВЕТСТВЕННЫЕ ЗА ОРГАНИЗАЦИЮ И КОНТРОЛЬ ВЫПОЛНЕНИЯ ПОРЯДКА

Ответственность за соблюдение требований настоящего Порядка возлагается на всех служащих Администрации, участвующих в обработке КИ.

Ответственность за организацию контрольных и проверочных мероприятий по вопросам парольной защиты возлагается на Администратора ИБ.

Ответственность за общий контроль информационной безопасности возлагается на ответственного за защиту информации Администрации.

Начальник управления информационных ресурсов администрации города Сочи А.В.Похлебаев

Приложение № 15
к Политике информационной
безопасности в администрации
города Сочи

ИНСТРУКЦИЯ

по организации антивирусной защиты информационных систем администрации города Сочи

1. ОБЩИЕ ПОЛОЖЕНИЯ

Инструкция по организации антивирусной защиты информационных систем (далее – Инструкция) администрации города Сочи (далее – Администрация) определяет требования к организации защиты информационных систем (ИС) от разрушающего воздействия компьютерных вирусов и другого вредоносного программного обеспечения (ПО) и устанавливает ответственность руководителей и служащих подразделений, эксплуатирующих и сопровождающих ИС, за их выполнение.

Требования настоящей Инструкции распространяются на всех должностных лиц и служащих подразделений Администрации, использующих в работе ИС Администрации.

В целях закрепления знаний по вопросам практического исполнения требований Инструкции, разъяснения возникающих вопросов, проводятся организуемые администратором информационной безопасности (ИБ) семинары и персональные инструктажи (при необходимости) пользователей ИС Администрации.

2. ПРИМЕНЕНИЕ СРЕДСТВ АНТИВИРУСНОЙ ЗАЩИТЫ

Антивирусный контроль дисков и файлов ИС после загрузки компьютера должен проводиться в автоматическом режиме (периодическое сканирование или мониторинг).

Периодически, не реже одного раза в неделю, должен проводиться полный антивирусный контроль всех дисков и файлов ИС (сканирование).

Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая информация по телекоммуникационным каналам связи, на съемных носителях (магнитных дисках, CD-ROM и т.п.). Разархивирование и контроль входящей информации необходимо проводить

непосредственно после ее приема. Контроль исходящей информации необходимо проводить непосредственно перед отправкой (записью на съемный носитель).

Установка (обновление и изменение) системного и прикладного программного обеспечения осуществляется в соответствии с «Инструкцией по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств ИС Администрации».

Обновление антивирусных баз должно проводиться регулярно, но не реже, чем 1 раз в неделю.

3. ФУНКЦИИ АДМИНИСТРАТОРА ИБ ПО ОБЕСПЕЧЕНИЮ АНТИВИРУСНОЙ БЕЗОПАСНОСТИ

Администратор ИБ обязан:

- проводить инструктажи пользователей ИС по вопросам применения средств антивирусной защиты;
- настраивать параметры средств антивирусного контроля в соответствии с руководствами по применению конкретных антивирусных средств;
- предварительно проверять устанавливаемое (обновляемое) ПО на отсутствие вредоносных программ;
- производить обновление антивирусных программных средств;
- производить получение и рассылку (при необходимости) обновлений антивирусных баз;
- разрабатывать инструкции по работе пользователей с программными средствами систем антивирусной защиты (САЗ);
- проводить работы по обнаружению и обезвреживанию вредоносных программ;
- участвовать в работе комиссии по расследованию причин заражения персональных электронных вычислительных машин (ПЭВМ) и серверов;
- хранить эталонные копии антивирусных программных средств;
- осуществлять периодический контроль за соблюдением пользователями ПЭВМ требований настоящей Инструкции;
- разрабатывать инструкции по работе пользователей с системой антивирусной защиты информации;
- проводить периодический контроль работы программных средств системы антивирусной защиты информации на ПЭВМ и серверах.

4. ФУНКЦИИ ПОЛЬЗОВАТЕЛЕЙ ИС

Пользователи ИС:

– получают по локально-вычислительной сети (ЛВС) или от администратора ИБ носители с обновлениями антивирусных баз (в случае отсутствия механизмов централизованного распространения антивирусных баз);

– проводят обновления антивирусных баз на ПЭВМ (в случае отсутствия механизмов централизованного распространения антивирусных баз);

– 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.) служащий подразделения самостоятельно или вместе с администратором ИБ должен провести внеочередной антивирусный контроль ПЭВМ. При необходимости пользователь должен привлечь администратора ИБ для определения факта наличия или отсутствия вредоносных программ;

– в случае обнаружения при проведении антивирусной проверки вредоносных программ служащие подразделений обязаны:

а) приостановить работу;

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

в) совместно с владельцем зараженных файлов провести анализ необходимости дальнейшего их использования;

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

д) в случае обнаружения новой вредоносной программы, не поддающейся лечению применяемыми антивирусными средствами, передать зараженный файл на съемном носителе администратору ИБ для дальнейшей передачи его в организацию, с которой заключен договор на антивирусную поддержку;

е) по факту обнаружения зараженных 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 и выполненные антивирусные мероприятия.

5. ОТВЕТСТВЕННЫЕ ЗА ОРГАНИЗАЦИЮ И КОНТРОЛЬ ВЫПОЛНЕНИЯ ИНСТРУКЦИИ

Ответственность за соблюдение требований настоящей Инструкции возлагается на всех служащих Администрации, участвующих в обработке конфиденциальной информации.

Ответственность за организацию контрольных и проверочных мероприятий по вопросам антивирусной защиты возлагается на администратора ИБ.

Ответственность за общий контроль информационной безопасности возлагается на ответственного за защиту информации.

Начальник управления информационных ресурсов администрации города Сочи А.В.Похлебаев

Департамент муниципальной службы и кадровой политики

Приложение № 1
К инструкции по организации
антивирусной защиты
информационных систем

ГРАФИК ПРОВЕРОК
файловой системы антивирусными средствами

Тип проверки	Условие проведения	Проверяемые ресурсы	Периодичность проверки	Время проверки
Частичная	При подключении носителя	Подключенный носитель	Каждый раз	Во время подключения, до начала работы с носителем
Полная		Подключаемые носители, жесткие диски ПЭВМ	Раз в неделю	В ночь с первого на второй рабочий день недели
Частичная	При включении ПЭВМ	Оперативная память, важные разделы ПЭВМ	Каждый раз при включении	Каждый раз при включении

Начальник управления информационных ресурсов администрации города Сочи А.В.Похлебаев

Приложение № 16
к Политике информационной
безопасности в администрации
города Сочи

ПРАВИЛА

работы с обезличенными персональными данными администрации города Сочи

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящие Правила работы с обезличенными персональными данными администрации города Сочи (далее – администрации города Сочи) разработаны с учетом Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» и постановления Правительства РФ от 21 марта 2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ-152 «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

1.2. Настоящие Правила определяют порядок работы с обезличенными персональными данными в администрации города Сочи.

2. УСЛОВИЯ ОБЕЗЛИЧИВАНИЯ

2.1. Обезличивание персональных данных может быть проведено с целью ведения статистических данных, снижения ущерба от разглашения защищаемых персональных данных, снижения уровня защищенности персональных данных администрации города Сочи и по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

2.2. Способы обезличивания при условии дальнейшей обработки персональных данных:

- уменьшение перечня обрабатываемых сведений;
- замена части сведений идентификаторами;
- обобщение – понижение точности некоторых сведений;
- понижение точности некоторых сведений (например, «Место жительства» может состоять из страны, индекса, города, улицы, дома и квартиры, а может быть указан только город)
- деление сведений на части и обработка в разных информационных системах;

- другие способы.

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

2.4. Для обезличивания персональных данных можно использовать любые способы явно незапрещенные законодательно.

2.5. Перечень должностей служащих администрации города Сочи, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, приведен в приложении № 1 к настоящим Правилам.

2.5.1. Глава города Сочи принимает решение о необходимости обезличивания персональных данных.

2.5.2. Руководители подразделений администрации города Сочи, непосредственно осуществляющих обработку персональных данных, готовят предложения по обезличиванию персональных данных, обоснование такой необходимости и способ обезличивания.

2.5.3. Служащие подразделений, обслуживающих базы данных с персональными данными, совместно с ответственным за организацию обработки персональных данных, осуществляют непосредственное обезличивание выбранным способом.

3. ПОРЯДОК РАБОТЫ С ОБЕЗЛИЧЕННЫМИ ПЕРСОНАЛЬНЫМИ ДАННЫМИ

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

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

3.3. При обработке обезличенных персональных данных с использованием средств автоматизации обязательно соблюдение:

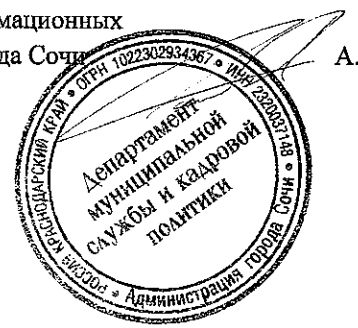
- порядка парольной защиты;
- инструкции по организации антивирусной зашиты информации;
- правил работы со съемными носителями (если они используется);
- инструкции по резервному копированию;
- порядка доступа служащих администрации города Сочи в помещения, в которых ведется обработка конфиденциальной информации;
- инструкции по действиям пользователей информационных систем администрации города Сочи в нештатных ситуациях;

- инструкции по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств информационных систем персональных данных.

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

- правил хранения бумажных носителей;
- правил доступа к ним и в помещения, где они хранятся.

Начальник управления информационных ресурсов администрации города Сочи А.В.Похлебаев



Приложение № 1
К правилам работы с
обезличенными персональными
данными

ПЕРЕЧЕНЬ ДОЛЖНОСТЕЙ
ответственных за проведение мероприятий по обезличиванию
обрабатываемых персональных данных

1) Руководители отраслевых (функциональных) территориальных органов администрации города Сочи;
2) Администратор ИБ;
3) Ответственный за защиту информации в администрации города Сочи

Начальник управления информационных
ресурсов администрации города Сочи А.В.Похлебаев

Приложение № 17
к Политике информационной
безопасности в администрации
города Сочи

ИНСТРУКЦИЯ

по внесению изменений в списки пользователей и наделению их полномочиями доступа к ресурсам информационных систем, обрабатывающих конфиденциальную информацию, в администрации города Сочи

1. ОБЩИЕ ПОЛОЖЕНИЯ

Инструкция по внесению изменений в списки пользователей и наделению их полномочиями доступа к ресурсам информационных систем персональных данных (далее – Инструкция) администрации города Сочи (далее – Администрация) устанавливает порядок изменения списка пользователей и порядок изменения их прав в информационных системах (ИС).

Непосредственное исполнение настоящей Инструкции определяется администратором ИБ, по согласованию с ответственным за защиту информации в Администрации.

2. ПОРЯДОК ИСПОЛЬЗОВАНИЯ УЧЕТНЫХ ЗАПИСЕЙ ПОЛЬЗОВАТЕЛЕЙ

С целью соблюдения принципа персональной ответственности за свои действия, каждому служащему, допущенному к работе с ИС должно быть сопоставлено персональное уникальное имя (учетная запись пользователя), под которым он будет регистрироваться и работать в системе.

В случае производственной необходимости, некоторым служащим могут быть сопоставлены несколько уникальных имен (учетных записей).

Использование несколькими служащими при самостоятельной работе в ИС одного и того же имени пользователя («группового имени») запрещено.

Использование учетных записей других служащих запрещено.

3. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ ПОЛЬЗОВАТЕЛЯМ ПРАВ ДОСТУПА К ИС

Процедура регистрации (создания учетной записи) пользователя и предоставления (изменения) ему прав доступа к ресурсам ИС инициируется на основании распоряжения о приеме на работу по заявке департамента муниципальной службы и кадровой политики администрации города Сочи. При увольнении или изменении прав доступа служащего Заявка на изменение или блокирование учетной записи готовится не позднее 2 часов с момента увольнения служащего. Заявка на создание учетной записи – в

течение 12 часов с момента подписания распоряжения о приеме на работу. Заявка согласовывается отделом информационной безопасности управления информационных ресурсов администрации города Сочи, после чего Администратором ИС в течение одного рабочего дня создается учетная запись пользователя . Форма заявки приведена в приложении 1.

В случае отсутствия особых требований, права доступа пользователя к ресурсам ИС выставляются на основании шаблона прав структурного подразделения, в которое принимается служащий.

При предоставлении служащему прав доступа к ресурсам необходимо руководствоваться принципом предоставления минимальных прав для решения требуемых задач.

В случае, если служащему требуются дополнительные права, то на основании заявки о руководителя структурного подразделения, администратор ИБ согласует изменения в правах, и Администратор ИС в течение 12 часов производит изменение прав доступа пользователя.

Начальники структурных подразделений несут ответственность за минимальную достаточность прав доступа имеющихся у пользователей их структурных подразделений. В случае наличия у пользователей избыточных для работы прав доступа начальники структурных подразделений ставят об этом в известность администратора ИБ, который вносит необходимые изменения в соответствии с настоящей Инструкцией.

Документирование прав доступа производится в электронном виде, для чего создается электронный журнал, в котором указываются следующие данные:

- фамилия, имя, отчество пользователя;
- структурное подразделение;
- учетная запись;
- контролируемый ресурс;
- права доступа;
- отметка об удалении учетной записи при увольнении.

Изменения в конфигурации механизмов защиты информации производятся только администратором ИБ и только в соответствии с документацией на средства защиты информации, применяемые в ИС.

При изменении статуса пользователя (увольнение, перевод на другую должность и т.п.) департамент муниципальной службы и кадровой политики администрации города Сочи подает заявку об изменении статуса пользователя (приложение 1 к настоящей инструкции).

4. ОТВЕТСТВЕННЫЕ ЗА ОРГАНИЗАЦИЮ И КОНТРОЛЬ ВЫПОЛНЕНИЯ ИНСТРУКЦИИ

Ответственность за соблюдение требований настоящей Инструкции пользователями возлагается на всех служащих, работающих в ИС Администрации.

Ответственность за организацию контрольных и проверочных мероприятий по вопросам управления правами пользователей возлагается на администратора ИБ.

Ответственность за общий контроль информационной безопасности возлагается на ответственного за защиту информации в Администрации.

Начальник управления информационных ресурсов администрации города Сочи А.В.Похлебаев

Приложение № 1
К инструкции по внесению
изменений в списки
пользователей

Начальнику управления информационных ресурсов администрации города Сочи

А.В. Похлебаеву

ЗАЯВКА
на внесение изменений в списки пользователей

_____

_____

(наименование автоматизированной системы, ПЭВМ)

и наделение пользователя полномочиями доступа к ресурсам системы

Прошу ___*зарегистрировать пользователем ИС (исключить из списка пользователей ИС, изменить полномочия пользователя)*

(ненужное зачеркнуть)

Подразделение_____,
Отдел_____,
Должность_____,
Руководитель_____,
ФИО_____,
Номер телефона_____,
Адрес подразделения_____,
Номер кабинета_____,

предоставив ему полномочия (лишив его полномочий), (ненужное зачеркнуть) необходимые *(х)* для решения задач:

_____

Руководитель отраслевого
(функционального)
территориального органа
администрации города Сочи

«___» _____ 20__ г. _____ ФИО

Оборотная сторона заявки

Пользователь _____ *зарегистрирован (исключен*
(фамилия, имя, отчество)

из списка пользователей, изменены полномочия пользователя).
(ненужное зачеркнуть)

Персональный идентификатор номер(при наличии) _____
выдан (изъят.

Внесены следующие изменения:

_____

_____

_____

_____

_____

_____

_____

Администратор ИБ
«___» _____ 20__ г. _____ А.С. Десятерик

Учетное имя, *персональный идентификатор* и начальные значения
(при отсутствии зачеркнуть)
паролей получил(а), о порядке смены пароля при первом входе в систему проинструктирован(а).

Пользователь _____
(подпись, фамилия, инициалы)

«___» _____ 20__ г.

Начальник управления информационных ресурсов администрации города Сочи А.В.Похлебаев