АДМИНИСТРАЦИЯ

АРТЕМОВСКОГО ГОРОДСКОГО ОКРУГА

РАСПОРЯЖЕНИЕ

16.01.2019 г. Артем № 13-ра

Об утверждении инструкций по обеспечению информационной безопасности и защиты персональных данных в администрации Артемовского городского округа

В соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказом Федеральной службы по техническому и экспортному контролю России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», постановлением администрации Артемовского городского округа от 27.12.2018 № 1084-па «О Положении об обеспечении безопасности персональных данных в администрации Артемовского городского округа», утвержденного, в целях совершенствования работы по обеспечению защиты информации в администрации Артемовского городского округа, руководствуясь Уставом Артемовского городского округа,

1. Утвердить:

1.1. Инструкцию по резервированию и восстановлению работоспособности технических средств и программного обеспечения, баз данных, средств защиты информации и средств криптографической защиты информации в администрации Артемовского городского округа (приложение 1).

1.2. Инструкцию по реагированию на инциденты информационной безопасности в администрации Артемовского городского округа (приложение 2).

1.3. Инструкцию о действиях работников администрации Артемовского городского округа в случае возникновения нештатных ситуаций в работе технических средств,

программного обеспечения, средств защиты информации (приложение 3).

1.4. Инструкцию по проведению внутренних проверок организации и состояния работ по защите информации в администрации Артемовского городского округа (приложение 4).

1.5. Инструкцию по обеспечению безопасности эксплуатации средств криптографической защиты информации в администрации Артемовского городского округа (приложение 5).

1.6. Инструкцию ответственного за обеспечение безопасности информации в органе администрации Артемовского городского округа (приложение 6).

1.7. Инструкцию пользователя информационных систем персональных данных в администрации Артемовского городского округа (приложение 7).

1.8. Инструкцию администратора безопасности информационных систем персональных данных в администрации Артемовского городского округа (приложение 8).

1.9. Инструкцию по обеспечению информационной безопасности при работе с электронной подписью в администрации Артемовского городского округа (приложение 9).

1.10. Инструкцию по организации парольной защиты информации в администрации Артемовского городского округа (приложение 10).

1.11. Инструкцию по организации антивирусной защиты информации в администрации Артемовского городского округа (приложение 11).

1.12. Инструкцию по информационной безопасности при получении доступа к информационным ресурсам администрации Артемовского городского округа с использованием мобильных устройств (приложение 12).

2. Признать утратившими силу:

распоряжение администрации Артемовского городского округа от 06.12.2017 № 859-ра «Об организации обеспечения информационной безопасности при создании и эксплуатации информационных систем администрации Артемовского городского округа»;

распоряжение администрации Артемовского городского округа от 20.12.2017 № 894-ра «Об утверждении Инструкции по обеспечению информационной безопасности при работе с электронной подписью в администрации Артемовского городского округа»;

распоряжение администрации Артемовского городского округа от 20.12.2017 № 895-ра «Об утверждении Инструкции по организации парольной защиты информации в администрации Артемовского городского округа»;

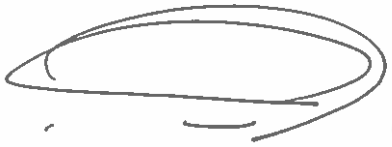
распоряжение администрации Артемовского городского округа от 20.12.2017 № 896-ра «Об утверждении Инструкции по информационной безопасности при получении доступа к информационным ресурсам администрации Артемовского городского округа с использованием мобильных устройств»;

распоряжение администрации Артемовского городского округа от 20.12.2017 № 897-ра

«Об утверждении Инструкции по организации антивирусной защиты информации в администрации Артемовского городского округа»;

распоряжение администрации Артемовского городского округа от 27.12.2017 № 913-ра «Об утверждении Инструкции ответственного за обеспечение безопасности информации в органе администрации Артемовского городского округа».

3. Контроль за исполнением настоящего распоряжения возложить на заместителя главы администрации Артемовского городского округа Салина Ю.В.

И.о. главы Артемовского городского округа  А.В. Руденко

Приложение 1

УТВЕРЖДЕНА

распоряжением администрации
Артемовского городского округа
от 16.01.2019 № 13-ра

ИНСТРУКЦИЯ
по резервированию и восстановлению работоспособности технических средств и программного обеспечения, баз данных, средств защиты информации и средств криптографической защиты информации в администрации Артемовского городского округа

1. Общие положения

1.1. Инструкция по резервированию и восстановлению работоспособности технических средств и программного обеспечения, баз данных, средств защиты информации и средств криптографической защиты информации администрации Артемовского городского округа (далее – Инструкция), определяет действия, связанные с функционированием информационных систем администрации Артемовского городского округа (далее – Администрация), меры и средства поддержания непрерывности работы и восстановления работоспособности информационных систем Администрации (далее – ИС).

1.2. Целью настоящей Инструкции является защита элементов ИС и системы защиты информации (далее – СЗИ) Администрации от предотвращения потери информации.

1.3. Задачами настоящей Инструкции являются определение мер защиты от потери информации и определение действий восстановления технических и программных средств ИС и СЗИ в случае потери информации.

1.4. Действие настоящей Инструкции распространяется на всех пользователей и администраторов ИС, имеющих доступ к информации и основным системам обеспечения непрерывности работы и восстановления информации при возникновении аварийных ситуаций.

1.5. Ответственными за реагирование на инциденты безопасности и контроль обеспечения мероприятий по предотвращению инцидентов безопасности, приводящие к потере защищаемой информации, являются работники отдела автоматизированных систем и программного обеспечения управления информации Администрации (далее – администраторы ИС).

2. Порядок реагирования на инциденты

2.1. Под инцидентом в настоящей Инструкции понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИС или СЗИ, предоставляемых

пользователям, а также потерей защищаемой информации.

2.2. Происшествие, вызывающее инцидент, может произойти в результате:

непреднамеренных действий пользователей ИС;

преднамеренных действий пользователей ИС и третьих лиц;

нарушения правил эксплуатации технических средств ИС и СЗИ;

возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

2.3. В случае возникновения инцидента в кратчайшие сроки, не превышающие одного рабочего дня, администраторы ИС предпринимают меры по восстановлению работоспособности технических средств и программного обеспечения, баз данных и СЗИ.

3. Меры и средства поддержания непрерывности работы и восстановления работоспособности информационных систем Администрации

3.1. К техническим мерам обеспечения непрерывной работы и восстановления работоспособности технических средств и программного обеспечения, баз данных, СЗИ и средств криптографической защиты информации относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения инцидентов, такие как:

системы жизнеобеспечения ИС;

системы обеспечения отказоустойчивости;

системы резервного копирования и хранения данных;

системы контроля физического доступа.

3.2. Системы жизнеобеспечения ИС включают в себя:

пожарные сигнализации и системы пожаротушения;

системы вентиляции и кондиционирования;

системы резервного питания.

3.3. Все критичные помещения Администрации (помещения, в которых размещаются элементы ИС и СЗИ) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

3.4. Для выполнения требований по эксплуатации программно-аппаратных средств ИС (температура, относительная влажность воздуха) в помещениях, где они установлены, должны использоваться системы вентиляции и кондиционирования воздуха.

3.5. Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИС, сетевое и коммуникационное оборудование должны подключаться к сети электропитания через источники бесперебойного питания.

В зависимости от необходимого времени работы ресурсов после потери электропитания могут применяться следующие методы резервного электропитания:

локальные источники бесперебойного электропитания с различным временем питания

для защиты отдельных компьютеров;

источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;

дублированные системы электропитания в устройствах (серверы, мосты и т. д.);

резервные линии электропитания в пределах комплекса зданий;

аварийные электрогенераторы.

3.6. Для защиты от отказов отдельных дисков серверов ИС, осуществляющих обработку и хранение защищаемой информации (персональных данных), используется технология RAID, которая предполагает дублирование данных, хранимых на дисках.

3.7. Система резервного копирования и хранения данных должна обеспечивать хранение защищаемой информации на твердом носителе.

3.8. Резервное копирование и хранение данных осуществляется на периодической основе:

для обрабатываемых персональных данных – не реже одного раза в неделю;

для технологической информации – не реже одного раза в месяц;

эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИС, – не реже одного раза в полгода и каждый раз при внесении изменений в эталонные копии (выход новых версий).

3.9. Резервирование данных ИС производится администраторами ИС либо работником органа Администрации, назначенным ответственным за резервирование данных.

3.10. Копирование осуществляется на специально выделенный для резервного копирования съемный носитель.

Съемные носители должны храниться:

в недоступном для посторонних лиц месте;

не менее одного года, для возможности восстановления данных.

Приложение 2

УТВЕРЖДЕНА

распоряжением администрации
Артемовского городского округа
от 16.01.2019 № 13-ра

ИНСТРУКЦИЯ
по реагированию на инциденты информационной безопасности в администрации Артемовского городского округа

1. Общие положения

1.1. Инструкция по реагированию на инциденты информационной безопасности в администрации Артемовского городского округа (далее – Инструкция) определяет порядок действия муниципальных служащих органов администрации Артемовского городского округа и работников муниципальных учреждений, учредителем которых является Артемовский городской округ (далее – работники), в случае возникновения инцидентов информационной безопасности в информационных системах (далее – ИС) администрации Артемовского городского округа (далее – Администрация).

1.2. Требования настоящей Инструкции обязательны для исполнения всеми работниками, допущенными к работе в ИС Администрации.

1.3. Общими требованиями ко всем работникам в случае возникновения инцидентов информационной безопасности (далее – инциденты ИБ) являются:

работник, обнаруживший инцидент ИБ, немедленно ставит в известность своего непосредственного руководителя и работника отдела профилактики терроризма и информационной безопасности Администрации (далее – администратор безопасности);

администратор безопасности обязан принимать меры по реагированию на инциденты ИБ, включая активизацию соответствующих защитных мер для предотвращения, уменьшения последствий и (или) восстановления после наступления негативных последствий вследствие инцидента ИБ;

в случае, если возникновение инцидентов ИБ влечет нарушение функционирования ИС и системы защиты информации (далее – СЗИ), проводятся мероприятия по выяснению причин ее проявления и проводится служебное расследование.

1.4. Инцидентом ИБ является событие, нарушающее одно из свойств защищаемой информации (целостность, доступность или конфиденциальность) или несколько таких свойств одновременно.

2. Выявление инцидента информационной безопасности

2.1. Основными источниками информации об инцидентах ИБ являются:

факты, выявленные работником, администратором безопасности;

результаты работы средств мониторинга информационной безопасности, результаты проверок и аудита (внутреннего или внешнего);

журналы и уведомления операционных систем серверов и рабочих станций, антивирусной системы, системы резервного копирования и других систем;

обращения физических и (или) юридических лиц с указанием инцидента ИБ;

запросы и предписания органов надзора за соблюдением требований по защите информации;

другие источники информации.

2.2. Основными видами инцидентов ИБ в Администрации являются:

разглашение конфиденциальной информации, в том числе персональных данных, либо угроза такого разглашения;

нарушение правил использования конфиденциальной информации, в том числе персональных данных;

несанкционированный доступ;

компрометация учетных записей или паролей;

вирусная атака или вирусное заражение;

нарушение или сбои в работе системы резервного копирования.

2.3. Работник может выявить признаки наличия инцидента ИБ путем анализа текущей ситуации на предмет ее соответствия требованиям защиты информации, установленным в Администрации. Выявленные несоответствия дают основания предполагать факт возникновения инцидента ИБ. Любые сведения об инциденте ИБ должны быть незамедлительно переданы выявившим их работником администратору безопасности.

3. Анализ исходной информации и принятие решения о проведении разбирательства

3.1. Администратор безопасности после получения информации о предполагаемом инциденте ИБ незамедлительно проводит первоначальный анализ полученных данных. В процессе анализа администратор безопасности проводит проверку наличия в выявленном факте нарушений.

3.2. По усмотрению администратора безопасности единичный инцидент ИБ, не приведший к негативным последствиям и совершенный работником впервые, фиксируется администратором безопасности в Журнале учета инцидентов информационной безопасности (форма прилагается) с присвоением статуса «Разбирательство не требуется».

3.3. В случае наличия признаков инцидента ИБ, приведшего к негативным последствиям, администратор безопасности классифицирует инцидент, определяет предварительную степень важности инцидента ИБ и принимает решение о необходимости

проведения разбирательства, информирует руководителя органа Администрации, в котором произошел инцидент ИБ, фиксирует инцидент ИБ в Журнале учета инцидентов информационной безопасности с присвоением статуса «В процессе разбирательства».

3.4. В срок не более 3 (трех) рабочих дней с момента поступления информации об инциденте ИБ, администратор безопасности инициирует первоочередные меры, направленные на локализацию инцидента ИБ и минимизацию его последствий.

4. Разбирательство инцидента информационной безопасности

4.1. Целями разбирательства инцидентов ИБ являются:

выработка организационных и технических решений, направленных на снижение рисков нарушения информационной безопасности, предотвращение и минимизацию подобных нарушений в будущем;

защита прав Администрации, установленных законодательством Российской Федерации;

защита ИС Администрации;

обеспечение безопасности конфиденциальной информации, в том числе персональных данных;

предотвращение несанкционированного доступа к конфиденциальной информации, персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации.

4.2. Разбирательство инцидента ИБ состоит из следующих этапов:

подтверждение/опровержение факта возникновения инцидента ИБ;

классификация инцидента ИБ;

подтверждение/корректировка уровня значимости инцидента ИБ;

уточнение дополнительных обстоятельств (деталей) инцидента ИБ;

получение (сбор) доказательств возникновения инцидента ИБ, обеспечение их сохранности и целостности;

минимизация последствий инцидента ИБ;

информирование и консультирование работников Администрации по действиям при обнаружении, устранении последствий и предотвращении инцидентов ИБ.

4.3. В процессе проведения разбирательства инцидента ИБ обязательными для установления являются:

дата и время совершения инцидента ИБ;

наименование органа, ФИО, должность нарушителя ИБ;

классификация инцидента ИБ;

уровень критичности инцидента ИБ;

характер и размер реального и потенциального ущерба;

обстоятельства, способствовавшие совершению инцидента ИБ.

При инциденте ИБ, затрагивающем не более одного органа Администрации, администратор безопасности информирует о факте инцидента руководителя соответствующего органа Администрации.

При инциденте ИБ, затрагивающем более одного органа Администрации, администратор безопасности информирует руководителей соответствующих органов Администрации и инициирует проведение разбирательства.

В случае проведения временного отключения прав доступа у предполагаемого нарушителя ИБ, информация об отключении прав доступа администратором безопасности направляется руководителю соответствующего органа Администрации.

4.4. Осуществляющий разбирательство администратор безопасности в процессе проведения расследования инцидента ИБ при необходимости запрашивает информацию в органах Администрации. Запрос направляется на имя руководителя органа Администрации с обязательным указанием сроков предоставления информации (с учетом необходимости ее анализа, сбора и подготовки).

После получения необходимой информации по инциденту ИБ осуществляющий разбирательство администратор безопасности проводит анализ полученных данных.

4.5. В течение 5 (пяти) рабочих дней с момента выявления инцидента ИБ администратор безопасности запрашивает у нарушителя ИБ объяснительную записку. Объяснительная записка должна быть составлена, подписана нарушителем ИБ в течение 2 (двух) рабочих дней со дня поступления запроса.

4.6. Администратор безопасности проводит оценку негативных последствий от реализации инцидента ИБ.

В ходе данной оценки учитываются:

прямой финансовый ущерб;

репутационный ущерб;

потенциальный ущерб;

косвенные потери, связанные с недоступностью сервисов ИС Администрации, потерей информации;

другие виды ущерба или аспекты негативных последствий.

4.7. С целью минимизации последствий инцидента ИБ возможно временное отключение прав доступа работника к ИС Администрации на время проведения расследования. Отключение инициируется администратором безопасности с уведомлением руководителя соответствующего органа Администрации.

4.8. В случае, если у нарушителя ИБ были отключены права доступа к ИС на время

проведения разбирательства, то по его результатам администратор безопасности принимает решение и инициирует возвращение в полном или ограниченном объеме ранее имеющихся у нарушителя ИБ прав доступа к ИС либо инициирует официальную процедуру отмены (изменения) прав доступа к ИС.

4.9. Восстановление временно отключенных у нарушителя ИБ прав доступа к ИС (разблокировка пользователя) может производиться только администратором безопасности.

5. Оформление результатов и завершение разбирательства

5.1. Собранная в процессе разбирательства инцидента ИБ информация фиксируется администратором безопасности в Журнале учета инцидентов информационной безопасности и учитывается при подготовке итогового заключения по инциденту ИБ.

5.2. Администратор безопасности формирует, согласовывает со всеми участниками разбирательства и подписывает итоговое заключение по расследованию инцидента ИБ.

Итоговое заключение по инциденту ИБ администратор безопасности направляет руководителям органов Администрации, затронутых инцидентом ИБ.

5.3. Администратор ИБ фиксирует завершение разбирательства в Журнале учета инцидентов информационной безопасности.

5.4. В случае выявления в инциденте ИБ признаков административного правонарушения или уголовного преступления, относящихся к сфере информационных технологий, администратор безопасности передает все материалы по инциденту ИБ главе Администрации для принятия решения о подаче заявления в правоохранительные органы Российской Федерации.

5.5. По завершении разбирательства инцидента ИБ администратор безопасности передает имеющиеся материалы (в объеме, достаточном для принятия решения) руководителю соответствующего органа Администрации для решения вопроса о целесообразности привлечения нарушителя ИБ к дисциплинарной ответственности.

5.6. О результатах проведенного разбирательства инцидента ИБ администратор безопасности, по необходимости, инициирует подготовку сообщения об инциденте ИБ в адрес главы Администрации.

6. Права, обязанности и ответственность

6.1. Администратор безопасности имеет право:

требовать предоставлений письменных объяснений по обстоятельствам инцидента ИБ у нарушителя ИБ;

запрашивать и получать устные и письменные разъяснения и иную информацию, необходимую для проведения разбирательства инцидента ИБ;

инициировать отключение от ИС Администрации работников, нарушивших правила

или требования ИБ, на период проведений расследования инцидента ИБ в случае, если имеется существенный риск того, что продолжение работы специалиста с ИС Администрации может повлечь значительное увеличение ущерба или новые инциденты ИБ;

по результатам расследования инцидента ИБ инициировать изменения в ИС Администрации с целью повышения их защищенности и снижения рисков инцидентов ИБ;

инициировать процедуры привлечения нарушителя ИБ к дисциплинарной ответственности согласно внутренним нормативным документам Администрации.

6.2. Администратор безопасности обязан:

определять первоочередные меры, направленные на локализацию инцидента ИБ и минимизацию негативных последствий;

фиксировать в Журнале учета инцидентов информационной безопасности всю исходную информацию об инциденте ИБ и результаты его расследования;

представлять отчеты и рекомендации по проведенным разбирательствам руководителям органов Администрации, главе Администрации;

проводить анализ обстоятельств, способствовавших совершению каждого инцидента ИБ, и на его основе разрабатывать рекомендации и предложения по снижению ущерба от подобных инцидентов ИБ и минимизации возможности их повторения в будущем.

6.3. Руководители и работники органов Администрации обязаны:

представлять по запросам администратора безопасности устные и письменные разъяснения и иную информацию в рамках своей компетенции, необходимую для проведения разбирательства инцидента ИБ;

информировать администратора безопасности о выявленных инцидентах ИБ.

6.4. Работники, виновные в нарушении норм, регулирующих получение, обработку и защиту информации, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.

6.5. Работники несут персональную ответственность за соблюдение требований по защите информации, установленных в Администрации.

Приложение

к Инструкции по реагированию на инциденты информационной безопасности в администрации Артемовского городского округа

ЖУРНАЛ

учета инцидентов информационной безопасности

Журнал начат «___»_____ 20___г.

Журнал завершен «___»_____ 20___г.

на _____ листах

№ п/п	Дата регистрации	Дата возникновения/ дата обнаружения	Информация о сообщающем лице (ФИО, должность, наименование органа администрации)	Описание события	Тип инцидента[1]	Пораженные ресурсы/ значимость[2]	Статус инцидента[3]	Разрешение инцидента[4]	Причастные лица/ описание нарушителя	Дата окончания/ дата разрешения инцидента	Привлечен-ные лица

1 – тип инцидента – действительный, попытка, подозрение, намеренный, случайный, ошибка.
2 – пораженные ресурсы – информация, аппаратура, программное обеспечение, средства связи, документация;
значимость – нарушение конфиденциальности, нарушение целостности, нарушение доступности, нарушение неотказуемости, уничтожение.
3 – статус инцидента – разбирательство не требуется, в процессе разбирательства.
4 – разрешение инцидента - описание предпринятых действий для разрешения инцидента.

Приложение 3

УТВЕРЖДЕНА

распоряжением администрации
Артемовского городского округа
от 16.01.2019 № 13-р-а

ИНСТРУКЦИЯ
о действиях работников администрации Артемовского городского округа в случае возникновения нештатных ситуаций в работе технических средств, программного обеспечения, средств защиты информации

1. Общие положения

1.1. Инструкция о действиях работников администрации Артемовского городского округа в случае возникновения нештатных ситуаций в работе технических средств, программного обеспечения и средств защиты информации (далее – Инструкция) определяет порядок действий в случае возникновения нештатных ситуаций, возникающих в процессе функционирования технических и программных средств информационных систем (далее – ИС) и системы защиты информации администрации Артемовского городского округа (далее – Администрация).

1.2. Положения настоящей Инструкции обязательны для исполнения всеми работниками Администрации, допущенными к работе в ИС Администрации.

1.3. Общие требования к работникам Администрации в случае возникновения нештатной ситуации:

1) работник Администрации, обнаруживший нештатную ситуацию, немедленно ставит в известность руководителя соответствующего органа Администрации, работников отдела профилактики терроризма и информационной безопасности Администрации и отдела автоматизированных систем и программного обеспечения управления информации Администрации;

2) работники отдела автоматизированных систем и программного обеспечения управления информации Администрации (далее – администраторы ИС) обязаны проводить анализ ситуации и локализацию угроз. Для локализации (блокирования) проявлений угроз информационной безопасности возможно привлечение пользователей ИС;

3) если возникновение нештатной ситуации повлекло нарушение функционирования ИС и системы защиты информации, проводятся мероприятия по выяснению причин ее проявления и проводится служебное расследование. Решение о проведении служебного расследования принимается главой Администрации на основании ходатайства руководителя отдела профилактики терроризма и информационной безопасности Администрации.

2. Действия работников Администрации при возникновении нештатных ситуаций

№ п/п	Нештатная ситуация	Действия
1	2	3
1.	Сбой программного обеспечения	администратор ИС выясняет причину сбоя программного обеспечения и восстанавливает его работоспособность
2.	Отключение электропитания технических средств ИС	администратор ИС проводит анализ на наличие потерь и (или) разрушения данных и программного обеспечения, а также проверяет работоспособность оборудования; при необходимости производится восстановление программного обеспечения и данных из последней резервной копии
3.	Выход из строя технических средств ИС (серверов, рабочих станций)	администратор ИС выполняет мероприятия по немедленному восстановлению работоспособности технических средств ИС; при необходимости производятся работы по восстановлению программного обеспечения и данных из резервных копий
4.	Потеря данных	администратор ИС проводит мероприятия по поиску и устранению причин потери данных (антивирусная проверка, целостность и работоспособность программного обеспечения, целостность и работоспособность оборудования); при необходимости производится восстановление программного обеспечения и данных из резервных копий
5.	Обнаружение вредоносной программы (далее – ВП) в программной среде средств автоматизации ИС	администратор ИС производит локализацию ВП с целью предотвращения ее дальнейшего распространения. При этом зараженная рабочая станция (сервер) физически отсоединяется от локальной вычислительной сети, администратором ИС проводится анализ состояния рабочей станции (сервера); в результате анализа предпринимается попытка сохранения данных, так как после перезагрузки рабочей станции (сервера) данные могут быть потеряны; после успешной ликвидации ВП сохраненные данные подвергаются повторной проверке на наличие ВП. Также проводится внеочередная проверка на всех средствах локальной вычислительной сети с применением обновленных антивирусных баз; при необходимости производится восстановление программного обеспечения и данных из резервных копий
6.	Утечка информации	в случае, если утечка информации произошла по техническим причинам, проводится анализ защищенности процессов ИС, при необходимости принимаются меры по устранению каналов утечки и предотвращению их возникновения
7.	Взлом операционной системы ИС (несанкционированное получение доступа к ресурсам операционной системы)	по возможности производится временное отключение рабочей станции (сервера) от локальной вычислительной сети для проверки на наличие ВП; администратор ИС проверяет целостность исполняемых файлов в соответствии с хэш-функциями эталонного программного обеспечения, проводится анализ состояния файлов скриптов и журналов сервера, производится смена всех паролей, имеющих отношение к данному серверу; в случае необходимости производится восстановление программного обеспечения и восстановление данных из эта-

1	2	3
		лонного архива и резервных копий; по результатам анализа ситуации проверяется вероятность проникновения несанкционированных программ в локальную вычислительную сеть, после чего проводятся аналогичные работы по проверке и восстановлению программного обеспечения и данных на других информационных узлах ИС
8.	Попытка несанкционированного доступа (далее – НСД)	администратором ИС проводится анализ ситуации на основе информации журналов регистрации попыток НСД и предыдущих попыток НСД. По результатам анализа, в случае необходимости (есть реальная угроза НСД), принимаются меры по предотвращению НСД; проводится внеплановая смена паролей; в случае появления обновлений программного обеспечения, устраняющих уязвимости системы безопасности, устанавливаются такие обновления. в случае установления факта осуществления попытки НСД со стороны внешних по отношению к ИС субъектов, принимаются меры по фиксации и документированию факта инцидента и готовятся материалы для передачи в компетентные органы дознания для проведения предварительного расследования, установления субъекта-нарушителя, определения наличия состава преступления и принятия решения о возбуждении уголовного дела
9.	Компрометация ключевой информации (паролей доступа)	администратором ИС проводится смена пароля, анализируется ситуация на наличие последствий компрометации и принимаются необходимые меры по минимизации возможного (или нанесенного) ущерба
10.	Физическое повреждение или хищение оборудования технических средств ИС	администратором ИС проводится анализ с целью оценки возможности утечки или повреждения информации; определяется причина повреждения элементов ИС и возможные угрозы информационной безопасности; администратором ИС проводится проверка программного обеспечения на целостность и на наличие ВП, а также проверка целостности данных и анализ электронных журналов; при необходимости проводятся мероприятия по восстановлению программного обеспечения и данных из резервных копий
11.	Невыполнение установленных правил информационной безопасности (далее – ИБ), правил работы в ИС, использование ИС с нарушением требований, установленных в нормативно-технической документации	администратором ИС проводится анализ с целью оценки возможности утечки или повреждения информации; определяются возможные угрозы информационной безопасности в результате инцидента
12.	Ошибки работников Администрации	администратор ИС проводит анализ с целью оценки возможности утечки или повреждения информации; определяются возможные угрозы информационной безопасности и необходимость восстановления информации,

1	2	3
		программного обеспечения и данных; при необходимости проводятся мероприятия по восстановлению программного обеспечения и данных из резервных копий
13.	Отказ в обслуживании	администратор ИС проводит анализ с целью определения причин, вызвавших отказ в обслуживании, и проверку программного обеспечения на целостность и на наличие ВП, а также проверку целостности данных и анализ электронных журналов; при необходимости администратором ИС проводятся мероприятия по восстановлению программного обеспечения и данных из резервных копий
14.	Несанкционированные изменения состава программных и аппаратных средств (конфигурации) ИС	администратором ИС проводится анализ с целью оценки возможности утечки или повреждения информации и определения возможных угроз ИБ; администратором ИС проводятся мероприятия по восстановлению программного обеспечения и данных из резервных копий, а также (при необходимости) проверка на наличие компьютерных ВП
15.	Техногенные и природные проявления нештатных ситуаций (стихийное бедствие, пожар или наводнение) грозящие уничтожением или повреждением информации (данных)	работник Администрации, обнаруживший факт возникновения нештатной ситуации, обязан: немедленно оповестить других работников Администрации и принять все меры для самостоятельной оперативной защиты помещения; немедленно позвонить в соответствующие службы помощи (пожарная охрана, служба спасения и т.д.); немедленно сообщить своему непосредственному руководителю и администратору ИС; после ликвидации нештатной ситуации решением главы Администрации назначается внутренняя комиссия по устранению последствий инцидента; комиссия определяет ущерб (состав и объем уничтоженных оборудования и информации) и причины, по которым произошло происшествие, а также выявляет виновных

3. Ответственность

3.1. Работники Администрации, виновные в нарушении норм, регулирующих получение, обработку и защиту информации ограниченного доступа, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.

3.2. Работники Администрации несут персональную ответственность за соблюдение требований по защите информации, установленных в Администрации.

Приложение 4

УТВЕРЖДЕНА

распоряжением администрации
Артемовского городского округа
от 16.01.2019 № 13-ра

ИНСТРУКЦИЯ
по проведению внутренних проверок организации и состояния работ по защите информации в администрации Артемовского городского округа

1. Общие положения

1.1. Инструкция по проведению внутренних проверок организации и состояния работ по защите информации в администрации Артемовского городского округа (далее – Инструкция) определяет цели проведения внутренних проверок организации и состояния работ по защите информации (далее – внутренняя проверка) в администрации Артемовского городского округа (далее – Администрация) и порядок проведения внутренней проверки.

1.2. Требования настоящей Инструкции обязательны для исполнения всеми муниципальными служащими администрации Артемовского городского округа и работников муниципальных учреждений, учредителем которых является Артемовский городской округ (далее – работники).

1.3. Внутреннюю проверку проводит ответственный по защите информации в Администрации, назначаемый распоряжением Администрации (далее – ответственный по защите информации).

1.4. Для проведения внутренних проверок может создаваться комиссия, состоящая из числа работников отдела профилактики терроризма и информационной безопасности Администрации и отдела автоматизированных систем и программного обеспечения управления информации Администрации.

1.5. Внутренняя проверка проводится на основании Плана внутренних проверок организации и состояния работ по защите информации в Администрации, утвержденного заместителем главы Администрации, курирующим сферу защиты информации.

2. Порядок проведения внутренних проверок

2.1. Внутренние проверки проводятся не реже одного раза в три года, но не чаще чем один раз в год в каждом органе Администрации.

2.2. Ответственный по защите информации не менее чем за 10 (десять) рабочих дней до даты начала внутренней проверки направляет письменное уведомление в органы Администрации о дате и времени предстоящей внутренней проверки данного органа Администрации.

2.3. Во время проведения внутренней проверки проводится работа по контролю эффективности проводимых мероприятий и принимаемых мер по защите:

информации, содержащей сведения, отнесенные к государственной тайне, обрабатываемой на автоматизированных рабочих местах, а также циркулирующей в выделенных помещениях;

персональных данных, обрабатываемых в информационных системах персональных данных;

конфиденциальной информации, обрабатываемой в автоматизированных системах и циркулирующей в защищаемых помещениях;

муниципальных информационных систем;

информационных систем общего доступа.

2.4. В процессе своей работы ответственный по защите информации проводит в органах Администрации:

проверку соответствия содержания документации по организации условий обработки и защиты информации требованиям действующего законодательства Российской Федерации и локальных правовых актов в области защиты информации;

контроль выполнения требований инструкций по обеспечению защиты информации, в том числе проверку знаний работниками органов Администрации инструкций по обеспечению защиты информации в Администрации;

проверку выполнения рекомендаций, указанных в актах предыдущих внутренних проверок (если такие проверки проводились в проверяемом органе Администрации);

определение направлений совершенствования и дальнейшего развития мер по защите информации.

2.5. По итогам внутренней проверки в течение 5 (пяти) рабочих дней составляется акт в количестве 2 (двух) экземпляров.

2.6. В акте отражаются:

недостатки по соблюдению требований информационной безопасности в Администрации, выявленные в органе Администрации в результате внутренней проверки;

рекомендации органу Администрации, подвергшемуся внутренней проверке, для оперативного устранения выявленных в ходе внутренней проверки недостатков по соблюдению требований информационной безопасности в Администрации.

2.7. Все экземпляры акта утверждаются заместителем главы Администрации.

Первый экземпляр акта в течение 3 (трех) рабочих дней после утверждения направляется с сопроводительным письмом в орган Администрации, подвергавшийся внутренней проверке, а второй экземпляр акта хранится у ответственного по защите информации.

3. Права и обязанности ответственного по защите информации

3.1. Ответственный по защите информации имеет право:

знакомиться с документами, техническими (программно-техническими, программными) средствами, обеспечивающими порядок обработки и защиты информации, а также осуществлять сбор в проверяемом органе Администрации необходимой информации;

привлекать к участию в проведении внутренней проверки работников, имеющих непосредственное отношение к вопросам защиты информации;

запрашивать у органов Администрации, подвергавшихся внутренней проверке, письменные отчеты об устранении замечаний и нарушений, полученных в ходе внутренней проверки, по истечении месяца со дня получения им акта проверки;

вносить главе Администрации предложения о приостановлении действий по обработке информации в органах Администрации, противоречащих действующему законодательству Российской Федерации, и локальных правовых актов в области защиты информации.

3.2. Ответственный по защите информации обязан:

соблюдать конфиденциальность в отношении сведений, полученных в ходе проведения внутренней проверки;

представлять главе Администрации отчет о состоянии информационной безопасности в Администрации по результатам выполнения годового плана внутренних проверок.

4. Ответственность

4.1. Работники, виновные в нарушении норм, регулирующих получение, обработку и защиту информации, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.

4.2. Работники несут персональную ответственность за соблюдение требований по защите информации, установленных в Администрации.

Приложение 5

УТВЕРЖДЕНА

распоряжением администрации
Артемовского городского округа
от 16.01.2019 № 13-ра

ИНСТРУКЦИЯ
по обеспечению безопасности эксплуатации средств криптографической защиты информации в администрации Артемовского городского округа

1. Общие положения

1.1. Инструкция по обеспечению безопасности эксплуатации средств криптографической защиты информации в администрации Артемовского городского округа (далее – Инструкция) разработана в соответствии с приказом Федеральной службы безопасности Российской Федерации от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)», приказом Федеральной службы безопасности Российской Федерации от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности», приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну» и в целях обеспечения безопасности эксплуатации средств криптографической защиты информации в администрации Артемовского городского округа (далее – Администрация).

1.2. Настоящая Инструкция определяет порядок учета, хранения и использования средств криптографической защиты информации (далее - СКЗИ), криптографических ключей и ключевых документов, а также порядок изготовления, смены, уничтожения и компрометации криптографических ключей в целях обеспечения безопасности эксплуатации СКЗИ.

СКЗИ – это совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем и

осуществлять криптографическое преобразование информации для обеспечения ее безопасности.

1.3. Положения Инструкции обязательны для исполнения всеми работниками Администрации, допущенными к работе с СКЗИ.

1.4. Ответственными за хранение и эксплуатацию СКЗИ являются работники отдела автоматизированных систем и программного обеспечения управления информации Администрации (далее – отдел АСПО).

1.5. Ответственный орган осуществляет:

поэкземплярный учет СКЗИ, эксплуатационной и технической документации к ним, ключевых носителей и ключевых документов;

учет пользователей СКЗИ (далее – Пользователи) и представление на утверждение списка Пользователей СКЗИ;

контроль за соблюдением условий использования СКЗИ;

расследования и составление заключений по фактам нарушения условий использования СКЗИ;

разработку и обеспечение мер по предотвращению возможных нежелательных последствий таких нарушений;

обучение Пользователей правилам работы с СКЗИ и правилам хранения СКЗИ, ключевых носителей и ключевых документов.

1.6. Пользователем СКЗИ является каждый работник Администрации, который в рамках исполнения должностных обязанностей осуществляет эксплуатацию СКЗИ.

Список Пользователей утверждается руководителем соответствующего органа Администрации.

1.7. Пользователь обязан:

не разглашать конфиденциальную информацию, к которой он допущен, в том числе сведения об СКЗИ, ключевых документах к ним и других мерах защиты;

соблюдать требования по обеспечению безопасности конфиденциальной информации при использовании СКЗИ;

хранить ключевую информацию в сейфах и помещениях, гарантирующих ее сохранность и конфиденциальность;

сообщать в отдел АСПО о попытках посторонних лиц получить сведения об СКЗИ или ключевых документах к ним;

незамедлительно уведомлять отдел АСПО о фактах утраты или недостачи СКЗИ, криптографических ключей, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых сведений конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений;

сдать СКЗИ, эксплуатационную и техническую документацию к ним, криптографические ключи в отдел АСПО, в соответствии с порядком, установленным настоящей Инструкцией, при прекращении использования СКЗИ (увольнении, переводе на другую должность и в иных подобных случаях).

2. Учет СКЗИ, хранение и передача криптографических ключей

2.1. СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы и ключевые носители подлежат поэкземплярному учету.

Программные СКЗИ учитываются совместно с аппаратными средствами, на которых осуществляется их штатная эксплуатация.

Учет осуществляется отделом АСПО в Журнале поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации (далее – Журнал, приложение 1 к настоящей Инструкции).

2.2. Единицей поэкземплярного учета ключевых документов считается отчуждаемый носитель с записанными криптографическими ключами. Если один и тот же носитель используется для записи другого криптографического ключа, его необходимо зарегистрировать снова.

2.3. Все полученные экземпляры СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы выдаются Пользователям под подпись в Журнале. Пользователи несут персональную ответственность за сохранность СКЗИ и ключевых документов.

2.4. Дистрибутивы СКЗИ, эксплуатационная и техническая документация к ним хранятся в отделе АСПО.

2.5. Ключевые носители с криптографическими ключами хранятся у Пользователей.

Хранение осуществляется в ящиках, шкафах, сейфах (хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

2.6. Ключевые носители с неработоспособными криптографическими ключами отдел АСПО принимает от Пользователя и делает соответствующую запись в Журнале.

Неработоспособные ключевые носители подлежат уничтожению.

2.7. Аппаратные средства, с которыми осуществляется штатное использование СКЗИ, а также аппаратные СКЗИ должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы). Место опечатывания (опломбирования) СКЗИ и аппаратных средств должно быть визуально контролируемым.

3. Использование СКЗИ

3.1. В Администрации СКЗИ используются с целью обеспечения конфиденциальности и целостности электронных документов и сетевого трафика. Применяемые СКЗИ должны

реализовать стойкие криптографические алгоритмы, не позволяющие в разумные сроки вычислить закрытый ключ по открытому ключу.

3.2. Для шифрования электронного документа и (или) сетевого трафика Пользователь использует свой собственный закрытый криптографический ключ и открытый криптографический ключ.

3.3. Пользователь ежедневно проверяет сохранность технических средств и целостность печатей и пломб на них.

В случае обнаружения не разрешенного программного обеспечения или факта повреждения целостности печати (пломбы) на техническом средстве с СКЗИ, работа с СКЗИ на таком техническом средстве должна быть прекращена. По данному факту проводится разбирательство в соответствии с Инструкцией по реагированию на инциденты информационной безопасности в Администрации.

3.4. Вскрытие технического средства с СКЗИ для проведения ремонта или технического обслуживания осуществляется только в присутствии работников отдела АСПО.

3.5. При работе с СКЗИ запрещается:

оставлять без присмотра (контроля) технические средства, на которых эксплуатируется СКЗИ;

самостоятельно вносить изменения в программную часть СКЗИ;

разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей, принтер и другие средства вывода информации;

использовать ключевые носители в режимах, не предусмотренных штатными функциями СКЗИ;

осуществлять несанкционированное копирование криптографических ключей;

изменять настройки или пытаться изменить настройки СКЗИ или операционной системы, сделанные ответственным органом;

использовать бывшие в работе ключевые носители для записи новой информации без предварительного гарантированного уничтожения на них ключевой информации;

осуществлять самостоятельное несанкционированное вскрытие технических средств с СКЗИ.

3.6. С целью обеспечения непрерывности работы плановая замена ключевой информации должна производиться заблаговременно.

4. Действия при компрометации криптографических ключей

4.1. Криптографические ключи считаются скомпрометированными в следующих

случаях:

потеря ключевых носителей (в том числе с последующим обнаружением);

увольнение работников, имевших доступ к ключевым носителям;

возникновение подозрений на утечку информации или ее искажение в информационной системе;

нарушение печати на хранилище с ключевыми носителями и на техническом средстве с СКЗИ;

временный бесконтрольный доступ посторонних лиц к ключевым носителям или техническим средствам с СКЗИ;

иные случаи подозрения компрометации криптографических ключей.

4.2. В случае подозрения в компрометации криптографических ключей Пользователь должен немедленно прекратить эксплуатацию СКЗИ и продолжить ее только после замены криптографических ключей.

Скомпрометированные криптографические ключи подлежат уничтожению.

5. Уничтожение криптографических ключей

5.1. Неиспользованные или выведенные из действия криптографические ключи подлежат уничтожению.

5.2. Уничтожение криптографических ключей на ключевых носителях производится комиссией в составе не менее трех человек.

5.3. Криптографические ключи, записанные на машинные ключевые носители, уничтожаются методом гарантированного стирания информации на машинном носителе в соответствии с требованиями эксплуатационной и технической документации на СКЗИ.

5.4. Криптографические ключи, записанные на бумажных носителях, уничтожаются физически (сжигание, измельчение и т. п.).

5.5. Перед уничтожением криптографических ключей и/или ключевых носителей, комиссия обязана:

установить наличие оригинала и количество копий криптографических ключей;

проверить внешнюю целостность каждого ключевого носителя;

идентифицировать каждый ключевой носитель в соответствии с Журналом;

убедиться, что криптографические ключи, находящиеся на ключевых носителях, действительно подлежат уничтожению;

произвести уничтожение криптографических ключей на оригинале и всех копиях ключевого носителя.

5.6. По факту уничтожения криптографических ключей составляется Акт уничтожения криптографических ключей (приложение 2 к настоящей Инструкции).

5.7. В Журнале делается отметка об уничтожении криптографических ключей.

5.8. Акты уничтожения криптографических ключей хранятся в отделе АСПО.

6. Требования к помещениям, в которых ведется работа с СКЗИ и (или) хранятся криптографические ключи

6.1. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены СКЗИ и (или) хранятся криптографические ключи (далее – Помещения), должны обеспечивать сохранность СКЗИ и криптографических ключей.

6.2. При оборудовании Помещения должны выполняться требования к размещению, монтажу СКЗИ, а также другого оборудования, функционирующего с СКЗИ.

6.3. Помещения должны иметь прочные входные двери с замками, гарантирующими надежную защиту от проникновения посторонних лиц в нерабочее время. Окна Помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение посторонних лиц, необходимо оборудовать средствами, препятствующими неконтролируемому проникновению в Помещения.

6.4. Мониторы рабочих станций с СКЗИ должны быть повернуты задней стороной к дверям и окнам либо должны применяться шторы, рольставни, жалюзи или другие средства для пресечения несанкционированного просмотра содержимого, отображаемого на мониторах.

6.5. Для хранения криптографических ключей, эксплуатационной и технической документации, дистрибутивов СКЗИ выделяется необходимое число надежных металлических хранилищ. Ключи от хранилищ хранятся в отделе АСПО.

6.6. По окончании рабочего дня Помещения и установленные в них хранилища должны быть закрыты на замок.

6.7. При обнаружении признаков, указывающих на возможное несанкционированное проникновение в Помещения или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено в отдел АСПО. Отдел АСПО должен оценить вероятность компрометации хранящихся криптографических ключей, составить акт и принять, при необходимости, меры к локализации последствия компрометации криптографических ключей и к их замене.

Приложение 1

к Инструкции по обеспечению безопасности эксплуатации средств криптографической защиты информации в администрации Артемовского городского округа

ЖУРНАЛ
поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним

Начат «___»_____ 20__г.

Окончен «___»_____ 20__г.

№ п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о передаче		Отметка о подключении (установке СКЗИ)			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
				От кого получены или ФИО ОКЗ, изготовившего ключевые документы	Дата и номер сопроводительного письма или дата изготовления ключевых документов и расписка в изготовлении	Ф.И.О. пользователя криптосредств	Дата и расписка в получении	ФИО специалиста ОКЗ, установившего СКЗИ	Дата установки и подписи лиц	Номера ТС, в которые установлено СКЗИ	Дата уничтожения	ФИО специалиста, уничтожившего (изъявшего) СКЗИ	Номер акта об уничтожении	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Приложение 2

к Инструкции по обеспечению
безопасности эксплуатации средств
криптографической защиты
информации в администрации
Артемовского городского округа

АКТ
об уничтожении криптографических ключей и ключевых документов

№_____ от «____» _____ 20__ г.

Комиссия в составе:

председатель комиссии: _____
(ФИО, должность)

члены комиссии: _____
(ФИО, должность)

_____
(ФИО, должность)

произвела уничтожение криптографических ключей и ключевых документов:

№ п/п	Учетный номер ключевого носителя	Номер криптографического ключа, наименование документа	Владелец ключа (документа)	Количество ключевых носителей (документов)	Номера экземпляров	Всего ключей	Примечания

Всего уничтожено _____ криптографических ключей на _____ ключевых носителях. Записи Акта сверены с записями Журнала поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов.

Уничтожение криптографических ключей выполнено путем стирания (разрушения) по технологии, принятой для ключевых носителей многократного использования в соответствии с требованиями эксплуатационной и технической документации на соответствующие СКЗИ.

Ключевые носители списаны с учета в Журнале поэкземплярного учета средств криптографической защиты информации.

Председатель комиссии: _____

Члены комиссии: _____

_____

Приложение 6

УТВЕРЖДЕНА

распоряжением администрации
Артемовского городского округа
от 16.01.2019 № 13-ра

ИНСТРУКЦИЯ
ответственного за обеспечение безопасности информации в органе администрации Артемовского городского округа

1. Общие положения

1.1. Инструкция ответственного за обеспечение безопасности информации в органе администрации Артемовского городского округа (далее – Инструкция) определяет основные обязанности и права ответственного за обеспечение безопасности информации в органе администрации Артемовского городского округа (далее – орган Администрации).

1.2. Инструкция регулирует отношения и порядок взаимодействия между ответственным за обеспечение безопасности информации в органе Администрации и муниципальными служащими и работниками, не замещающими должности муниципальной службы, органа Администрации (далее – работники), которые обрабатывают служебную информацию, в том числе персональные данные (далее - информация).

1.3. Ответственные за обеспечение безопасности информации в органах Администрации (далее – ответственный за ОБИ) назначаются распоряжением администрации Артемовского городского округа (далее – распоряжение Администрации) по ходатайству руководителя органа Администрации.

1.4. Ответственный за ОБИ руководствуется в своей деятельности действующим законодательством Российской Федерации в области защиты информации, а также принятыми в соответствии с ним распоряжениями Администрации.

1.5. Непосредственное руководство ответственным за ОБИ осуществляет руководитель органа Администрации, а методическую помощь оказывает отдел профилактики терроризма и информационной безопасности администрации Артемовского городского округа.

2. Обязанности ответственного

2.1. Ответственный за ОБИ обязан знать:

2.1.1. Правила обработки информации в органе Администрации для каждой цели обработки информации.

2.1.2. Перечень находящихся в эксплуатации органом Администрации информационных систем, в том числе информационных систем персональных данных (далее информационные системы) и применяемых средств защиты информации в органе

Администрации.

2.1.3. Перечни помещений органа Администрации, в которых ведется обработка информации и предназначенных для ее хранения материальных носителей, содержащих информацию.

2.1.4. Порядок оформления заявки на предоставление доступа работникам к информационным системам в соответствии с Инструкцией по управлению доступом к информационным ресурсам администрации Артемовского городского округа.

2.2. Ответственный за ОБИ обязан осуществлять учет:

машинных носителей информации, в том числе предназначенных для обработки персональных данных и ключевых документов, в журнале учета машинных носителей информации (приложение 1 к настоящей Инструкции);

ключевых документов по учетному номеру машинных носителей информации, содержащих ключевые документы, в журнале учета ключевых документов, руководствуясь Инструкцией по обеспечению информационной безопасности при работе с электронной подписью в администрации Артемовского городского округа.

2.3. Ответственный за ОБИ обязан:

участвовать в работе комиссии по уничтожению персональных данных и хранить акты об уничтожении персональных данных;

принимать меры для выполнения рекомендаций комиссии по проведению внутренних проверок организации и состояния работ по защите информации в органе Администрации по результатам ее работы;

проводить ознакомление работников органа Администрации с действующим законодательством Российской Федерации в области персональных данных и защиты информации, а также принятыми в соответствии с ним распоряжениями Администрации (приложение 2 к настоящей Инструкции);

сообщать немедленно руководителю органа Администрации о выявленных случаях осуществления несанкционированного доступа к персональным данным, техническим средствам из состава информационной системы и непреднамеренного уничтожения персональных данных, обрабатываемых в органе Администрации.

2.4. Ответственный за ОБИ осуществляет контроль:

за соблюдением порядка доступа работников в помещения органа Администрации, где ведется обработка персональных данных;

за ведением журнала учета обращений субъектов персональных данных или их представителей;

за выполнением постановления администрации Артемовского городского округа от 27.12.2008 № 1084-па «О Положении об обеспечении безопасности персональных данных

в администрации Артемовского городского округа»;

за порядком использования и сохранности работниками органа Администрации документов, содержащих персональные данные, и машинных носителей информации;

за выполнением работ по восстановлению информации (персональных данных), обрабатываемых органом Администрации, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

3. Права ответственного

Ответственный за ОБИ имеет право:

требовать от работников органа Администрации исполнения действующего законодательства Российской Федерации в области персональных данных и защиты информации, а также принятых в соответствии с ним распоряжений Администрации;

участвовать в выявлении недостатков, повлекших нарушения в области обработки персональных данных и защиты информации в органе Администрации, вносить предложения по устранению вышеуказанных недостатков, предупреждению таких нарушений и совершенствованию правового регулирования обработки персональных данных и защиты информации в органе Администрации.

4. Ответственность

Ответственный за ОБИ несет ответственность за нарушение требований настоящей Инструкции в соответствии с действующим законодательством Российской Федерации и должностной инструкцией.

Приложение 1

к Инструкции ответственного за обеспечение безопасности информации в органе администрации Артемовского городского округа

ЖУРНАЛ
учета машинных носителей информации

№ п/п	Дата регистрации	Учетный номер машинного носителя информации	Заводской номер машинного носителя информации	Выдача машинного носителя информации			Прием машинного носителя информации			Сведения об уничтожении машинного носителя информации (номер, дата акта)
				Дата выдачи машинного носителя информации	Ф.И.О. пользователя машинного носителя информации	Расписка в получении машинного носителя информации	Дата приема машинного носителя информации	Ф.И.О. ответственного за обеспечение безопасности информации	Расписка в приеме машинного носителя информации	
1	2	3	4	5	6	7	8	9	10	11

Приложение 2

к Инструкции ответственного за обеспечение безопасности информации в органе администрации Артемовского городского округа

ЖУРНАЛ

проведения инструктажа по информационной безопасности в органе администрации Артемовского городского округа

в _____

(наименование органа администрации Артемовского городского округа)

Журнал начат: «__» _____ 20___г.

Журнал завершен: «__» _____ 20___г.

на _____ листах

№ п/п	Инструктаж		Инструктируемый		Инструктирующий	
	дата	тема	ФИО	подпись	ФИО	подпись
1	2	3	4	5	6	7

Приложение 7

УТВЕРЖДЕНА

распоряжением администрации
Артемовского городского округа
от 16.01.2019 № 13-ра

ИНСТРУКЦИЯ
пользователя информационных систем персональных данных в администрации Артемовского городского округа

1. Общие положения

1.1. Инструкция пользователя информационных систем персональных данных в администрации Артемовского городского округа (далее – Инструкция) определяет права, обязанности и ответственность пользователя информационных систем персональных данных администрации Артемовского городского округа (далее – Администрация).

1.2. Пользователем информационных систем персональных данных в Администрации (далее – пользователь ИСПДн) является каждый работник Администрации, участвующий в рамках своих функциональных обязанностей в процессах обработки персональных данных и имеющий доступ к аппаратным средствам, программному обеспечению, персональным данным и средствам защиты информации.

1.3. Пользователь ИСПДн руководствуется в своей деятельности Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», правовыми актами Администрации в области защиты персональных данных и настоящей Инструкцией.

1.4. Методическое руководство работой пользователя ИСПДн осуществляется ответственным за обеспечение защиты персональных данных, ответственным за организацию обработки персональных данных в Администрации.

2. Права и обязанности пользователя ИСПДн

2.1. Пользователь ИСПДн обязан:

осуществлять обработку персональных данных с соблюдением требований законодательства Российской Федерации, правовых актов Администрации в области защиты персональных данных и настоящей Инструкции;

при обработке персональных данных обеспечивать их конфиденциальность и защиту от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий в соответствии с действующими законами Российской Федерации;

получать и обрабатывать данные субъекта персональных данных только с его

письменного согласия;

разрешать доступ к персональным данным только лицам, осуществляющим обработку персональных данных в соответствии с должностной инструкцией, при этом указанные лица должны иметь право получать только те персональные данные субъекта персональных данных, которые необходимы для выполнения конкретных функций;

не допускать передачу персональных данных третьей стороне без письменного согласия субъекта персональных данных, за исключением случаев, установленных законодательством Российской Федерации;

не разглашать (не использовать) в интересах организаций либо физических лиц персональные данные и сведения, затрагивающие частную жизнь, здоровье, честь и достоинство субъекта персональных данных, ставшие ему известными в связи с исполнением должностных обязанностей, в том числе и после увольнения со службы (работы);

в случае выявления недостоверных персональных данных осуществлять блокирование персональных данных, относящихся к соответствующему субъекту персональных данных, на период проверки, устранить допущенные нарушения в соответствии с Положением по обеспечению безопасности персональных данных в Администрации;

производить обработку и хранение персональных данных только в ИСПДн, оборудованных средствами защиты информации от несанкционированного доступа (средствами разграничения доступа) и от утечки по техническим каналам, с использованием взятых на учет съемных носителей информации;

осуществлять эксплуатацию ИСПДн в полном соответствии с утвержденной организационно-распорядительной и эксплуатационной документацией;

производить обмен информацией, содержащей персональные данные в электронном виде, только на учтенных носителях информации;

хранить документы и носители информации, содержащие персональные данные, в недоступном для посторонних лиц местах (запираемых и опечатываемых шкафах, ящиках, хранилищах);

ставить в известность руководителя соответствующего органа Администрации о фактах утраты документов, носителей информации с персональными данными, идентификаторов информационных систем;

в случае обнаружения неисправностей технических средств защиты информации немедленно прекратить обработку персональных данных и поставить в известность об этом своего руководителя, администратора безопасности ИСПДн;

выполнять требования администратора безопасности ИСПДн, связанные с выполнением им своих функций.

При увольнении, перед уходом в отпуск, отъездом в командировку своевременно сдать:

учтенные носители информации, идентификаторы - администратору безопасности ИСПДн;

все числящиеся за ним документы – работнику Администрации, исполняющему его обязанности на период отсутствия.

2.2. Пользователь ИСПДн имеет право:

знакомиться с документами и материалами, необходимыми для выполнения должностных обязанностей;

вносить предложения по совершенствованию системы защиты информации;

обращаться к администратору безопасности ИСПДн для получения необходимой технической и методической помощи в работе.

3. Ответственность

3.1. Пользователь ИСПДн, виновный в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несет дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.

3.2. Пользователь ИСПДн несет персональную ответственность за соблюдение требований по защите персональных данных, установленных Положением по обеспечению безопасности персональных данных в Администрации.

Приложение 8

УТВЕРЖДЕНА

распоряжением администрации
Артемовского городского округа
от 16.01.2019 № 13-ра

ИНСТРУКЦИЯ
администратора безопасности информационных систем персональных данных в администрации Артемовского городского округа

1. Общие положения

1.1. Инструкция администратора безопасности информационных систем персональных данных администрации Артемовского городского округа (далее – Инструкция) определяет права, обязанности и ответственность работников администрации Артемовского городского округа (далее – Администрация), являющихся администраторами безопасности информационных систем персональных данных (далее – администратор безопасности).

1.2. Администратор безопасности руководствуется в своей деятельности Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», правовыми актами Администрации в области защиты персональных данных и настоящей Инструкцией.

1.3. Администратором безопасности является работник Администрации, уполномоченный на проведение работ по защите информации на этапах эксплуатации и модернизации информационных систем персональных данных администрации (далее – ИСПДн) и поддержанию достигнутого уровня защищенности ее ресурсов.

1.4. Требования администратора безопасности, связанные с выполнением им своих обязанностей, обязательны для исполнения всеми пользователями ИСПДн.

2. Обязанности и права администратора безопасности

2.1. Администратор безопасности должен знать:

законодательные и нормативные правовые акты, методические и нормативные материалы по вопросам, связанным с обеспечением информационной безопасности;

структуру защищаемой системы, категории защищаемой информации, категории пользователей, работающих в системе, и их права доступа к ресурсам ИСПДн;

порядок использования, обработки и хранения информации в ИСПДн;

методы и средства контроля информации, способы выявления каналов утечки информации, способы организации противодействия угрозам информационной безопасности;

принципы функционирования, методику обслуживания и устранения неисправностей

программно-технических средств системы защиты информации;

принципы работы и форматы файлов регистрации (журналирования) операционных систем, систем управления базами данных и приложений;

основы администрирования используемых в системе защиты информации операционных систем, средств защиты информации и программного обеспечения.

2.2. Администратор безопасности обязан:

осуществлять установку, настройку и контроль функционирования средств защиты информации, применяемых на объекте информатизации, а также контроль выполнения установленного комплекса организационных мероприятий по защите информации;

контролировать целостность (неизменность), сохранность средств защиты информации, используемых в ИСПДн, а при обнаружении фактов изменения контролируемых параметров немедленно принимать меры по приведению контролируемых параметров в исходное состояние;

осуществлять оперативные действия по конфигурированию системы защиты информации и поддержке ее компонентов в работоспособном состоянии, включая:

актуализацию перечня защищаемой информации;

поддержание в актуальном состоянии перечня учётных записей пользователей и назначенных им прав доступа к ресурсам;

контролировать защищенность аппаратных средств ИСПДн;

осуществлять контроль требований защиты информации при проведении технического обслуживания и ремонта аппаратных средств ИСПДн;

не допускать использования, хранения и размножения в ИСПДн программных продуктов и носителей информации, непосредственно не связанных со служебной деятельностью на рабочем месте;

контролировать исполнение пользователями ИСПДн введенного режима безопасности, а также правильность работы с элементами ИСПДн и средствами защиты информации, в том числе исполнение парольной политики, работы в сетях общего пользования и (или) международного обмена;

уточнять в установленном порядке обязанности пользователей ИСПДн по обработке защищаемой информации, в том числе поддерживать в актуальном состоянии таблицу разграничения прав доступа (матрицу доступа) к ИСПДн;

вести контроль над процессом осуществления резервного копирования защищаемой информации;

анализировать состояние защиты ИСПДн и ее отдельных подсистем, записи журнала учета событий, регистрируемых средствами защиты, с целью выявления возможных нарушений;

оказывать помощь пользователям ИСПДн в части применения средств защиты информации и консультировать по вопросам введенного режима защиты информации;

2.3. Администратор безопасности имеет право:

участвовать в разработке организационных мероприятий по обеспечению защиты информации;

запрашивать и получать от работников Администрации информацию и материалы, необходимые для надлежащего исполнения своих должностных прав и обязанностей;

осуществлять взаимодействие с руководителями органов Администрации в процессе организации работ по вопросам защиты информации;

получать доступ к аппаратным средствам ИСПДн и в помещения, в которых они расположены, полный доступ к журналам регистрации событий.

3. Ответственность

3.1. Администратор безопасности, виновный в нарушении требований федерального законодательства в области защиты информации, несет ответственность, предусмотренную законодательством Российской Федерации.

3.2. Администратор безопасности несет персональную ответственность за качество проводимых им работ по контролю действий пользователей ИСПДн при работе в ИСПДн Администрации, за состояние и поддержание установленного уровня защищенности ИСПДн Администрации.

Приложение 9

УТВЕРЖДЕНА

распоряжением администрации
Артемовского городского округа
от 16.01.2019 № 13-ра

ИНСТРУКЦИЯ
по обеспечению информационной безопасности при работе с электронной подписью в администрации Артемовского городского округа

1. Общие положения

1.1. Инструкция по обеспечению информационной безопасности при работе с электронной подписью в администрации Артемовского городского округа (далее – Инструкция) определяет порядок обеспечения информационной безопасности при работе с государственными информационными системами по каналам связи информационно-телекоммуникационной сети Интернет и ведении электронного документооборота в администрации Артемовского городского округа (далее – Администрация) с использованием средств электронной подписи (далее – ЭП) и ключевых документов.

1.2. Муниципальные служащие и работники Администрации, не замещающие должности муниципальной службы (далее – работники), при работе с ЭП на автоматизированных рабочих местах (далее – АРМ) применяют ключевые документы в электронной форме, для хранения которых используются съемные машинные носители информации (далее – МНИ): USB-flash-накопители, e-Token, рутокены, смарт-карты.

2. Правила обеспечения информационной безопасности при работе на АРМ

2.1. Для обеспечения информационной безопасности при эксплуатации АРМ необходимо:

осуществлять установку средств ЭП на АРМ в соответствии с эксплуатационной документацией на средства ЭП;

применять специальные средства защиты информации (средства доверенной загрузки и антивирусной защиты информации, межсетевые экраны), имеющие сертификаты соответствия уполномоченного органа по сертификации средств защиты информации;

применять принудительную блокировку АРМ, защищенную паролем;

учитывать требования Инструкции по информационной безопасности при получении доступа к информационным системам администрации Артемовского городского округа с использованием мобильных устройств, если в качестве АРМ для работы с ЭП планируется использовать мобильное устройство;

удалять с АРМ средства ЭП и всю информацию о работе с ЭП в случае передачи АРМ

в другой орган Администрации, сдачи его в ремонт или списания.

2.2. Установка и обслуживание на АРМ технических средств, программного обеспечения, средств защиты информации, а также средств ЭП осуществляется специалистами отдела автоматизированных систем и программного обеспечения управления информации Администрации.

2.3. Для подготовки МНИ, предназначенных для записи ключевых документов, ответственный за обеспечение безопасности информации в органе Администрации:

форматирует МНИ, если МНИ являются USB-flash-накопителями;

маркирует и регистрирует МНИ в журнале учета машинных носителей информации;

выдает МНИ работникам органа Администрации под подпись в журнале учета машинных носителей информации.

2.4. Ответственный за обеспечение безопасности информации в органе Администрации после получения ключевых документов в удостоверяющем центре:

регистрируют ключевые документы по учетным номерам МНИ, содержащих ключевые документы, в журнале учета ключевых документов (приложение 1 к настоящей Инструкции) после каждой проведенной записи ключевых документов на МНИ, если они многократно используются;

выдают ключевые документы на ключевых носителях работникам органа Администрации под подпись в журнале учета ключевых документов.

2.5. Работники Администрации при работе с ключевыми документами на МНИ (далее - ключевые носители) обязаны:

получать ключевые документы под подпись в журнале учета ключевых документов;

обеспечивать конфиденциальность ключевых документов, в том числе с использованием средств защиты информации, установленных на АРМ;

хранить ключевые носители в местах, недоступных посторонним лицам: в шкафу или ящике стола, запираемых на ключ;

следить за сроком действия сертификата ключевого документа и заблаговременно сообщать о времени его окончания ответственному за обеспечение безопасности информации органа Администрации;

вставлять ключевые носители только в считывающее устройство АРМ и только на время работы на средствах ЭП;

исключить в рабочее время несанкционированный доступ в помещение, где установлен АРМ и (или) хранятся ключевые носители (далее – помещение), посторонних лиц, не допущенных к работе в помещении;

сдать МНИ в случае увольнения или перевода в другой орган Администрации;

оповещать отдел профилактики терроризма и информационной безопасности

Администрации о фактах совершения попытки постороннего лица получить сведения об используемых средствах ЭП или доступ к ключевым документам, а также о компрометации ключевых документов или утрате ключевых носителей.

2.6. Работникам Администрации при работе с ключевыми документами на МНИ запрещается:

снимать копии с ключевых документов;

знакомить с ключевыми документами или передавать ключевые носители лицам, к ним не допущенным;

записывать на ключевые носители постороннюю информацию, в том числе рабочие или личные файлы;

оставлять ключевые носители на рабочем месте без присмотра;

использовать МНИ для записи информации, не связанной с ЭП, без предварительного уничтожения на них ключевых документов средствами гарантированного стирания информации и выполнения соответствующей записи в журнале учета ключевых документов;

пересылать ключевые документы по открытым каналам Администрации и информационно-телекоммуникационной сети Интернет.

2.7. Единовременное уничтожение большого объема ключевых документов в случае истечения срока действия ключевых документов, прекращения полномочий владельца ключевых документов, выхода из строя ключевого носителя или компрометации ключевых документов оформляется актом об уничтожении ключевых документов (приложение 2 к настоящей Инструкции).

Приложение 1

к Инструкции по обеспечению информационной безопасности при работе с электронной подписью в администрации Артемовского городского округа

ЖУРНАЛ
учета ключевых документов

№ п/п	Регистрационный номер машинного носителя информации, содержащего ключевые документы	Отметка о получении ключевых документов		Отметка о выдаче ключевых документов			Отметка об изъятии (уничтожении) ключевых документов		
		От кого получен ключевой документ	Дата и номер сопроводительного письма	Фамилия, имя, отчество владельца ключевых документов	Дата получения ключевых документов	Подпись владельца ключевых документов	Дата изъятия ключевых документов	Фамилия, имя, отчество лица, производившего изъятие (уничтожение) ключевых документов	Номер акта или подпись об уничтожении ключевых документов
1	2	3	4	5	6	7	8	9	10

Приложение 2

к Инструкции по обеспечению информационной безопасности при работе с электронной подписью в администрации Артемовского городского округа

АДМИНИСТРАЦИЯ
АРТЕМОВСКОГО ГОРОДСКОГО ОКРУГА

№ _____ от _____

УТВЕРЖДАЮ
_____
(наименование должности руководителя)

_____ _____
(личная подпись) *(фамилия, инициалы)*

А К Т
об уничтожении ключевых документов

ОСНОВАНИЕ: _____
(наименование распорядительного документа, на основании которого
_____
документируется факт, событие или действие, его номер и дата)

Председатель комиссии:
_____
(наименование должности, фамилия, имя, отчество)

Члены комиссии:
1. _____
(наименование должности, фамилия, имя, отчество)
2. _____
(наименование должности, фамилия, имя, отчество)

Присутствовали: _____
_____
(наименование должности, фамилия, имя, отчество)

Комиссия _____ провела отбор машинных носителей информации (далее - МНИ):
(дата)

№ п/п	Учетный номер МНИ (*)	Фамилия, имя, отчество владельца ключевых документов	Примечание (**)

Всего подлежит уничтожению: ключевые документы с _____ МНИ
(число прописью)
и (или) _____ МНИ, содержащие ключевые носители.
(число прописью)

Правильность произведенных записей в настоящем акте с данными в журнале учета ключевых документов и с учетным номером МНИ сверены.

Уничтожение ключевых документов с МНИ и (или) МНИ, содержащие ключевые носители, произведено.

Соответствующие записи в журнале учета ключевых документов об уничтожении ключевых документов проставлены.

Председатель комиссии: _____ _____
(личная подпись) *(фамилия, инициалы)*

Члены комиссии: _____ _____
(личная подпись) *(фамилия, инициалы)*

_____ _____
(личная подпись) *(фамилия, инициалы)*

(*) указывается порядковый номер по журналу учета ключевых документов;
(**) указывается причина: истек срок действия ключевых документов; прекращены полномочия владельца ключевых документов; вышел из строя МНИ; произошла компрометация ключевых документов.

Приложение 10

УТВЕРЖДЕНА

распоряжением администрации
Артемовского городского округа
от 16.01.2019 № 13-ра

ИНСТРУКЦИЯ
по организации парольной защиты информации в администрации Артемовского городского округа

1. Общие положения

1.1. Инструкция по организации парольной защиты информации в администрации Артемовского городского округа (далее – Инструкция) устанавливает правила создания, смены и обеспечения конфиденциальности паролей муниципальными служащими и работниками, не замещающими должности муниципальной службы, администрации Артемовского городского округа (далее – работники) для обеспечения защиты информационных ресурсов администрации Артемовского городского округа (далее - Администрация) от несанкционированного доступа.

1.2. Организационное и техническое обеспечение процессов создания, использования и смены паролей для доступа работников Администрации к информационным ресурсам Администрации выполняют работники отдела автоматизированных систем и программного обеспечения управления информации администрации Артемовского городского округа (далее - специалисты АСиПО), осуществляющие проведение технического обслуживания информационных систем и средств защиты информации в Администрации.

1.3. Ответственность за соблюдение требований настоящей Инструкции возлагается на всех работников Администрации, являющихся пользователями информационных ресурсов Администрации.

2. Правила создания, смены и обеспечения конфиденциальности паролей

2.1. В соответствии с Инструкцией по управлению доступом к информационным ресурсам администрации Артемовского городского округа специалисты АСиПО:

создают для работников Администрации первичные пароли в соответствии с требованиями пункта 2.4 настоящей Инструкции;

устанавливают функцию автоматического напоминания работникам Администрации о необходимости смены пароля для доступа к информационно-телекоммуникационной сети Администрации с периодичностью один раз в 90 дней.

2.2. Выдачу работникам Администрации первичных паролей для доступа к информационно-телекоммуникационной сети Администрации и к информационным

системам Администрации, осуществляет отдел профилактики терроризма и информационной безопасности администрации Артемовского городского округа (далее – ОИБ).

2.3. Работники Администрации при первой регистрации в информационно-телекоммуникационной сети Администрации и автоматизированной системе электронного документооборота «Дело» должны сменить первичные пароли.

2.4. Пароли создаются (меняются) с учетом следующих требований:

пароли должны состоять не менее чем из 8 символов;

пароли обязательно должны содержать: буквы в верхнем и нижнем регистрах, цифры и специальные символы “ ~ ! @ # % ^ & * ( ) - + _ = \ | / ? , $

при смене паролей новые значения паролей должны отличаться от предыдущих не менее чем по 4 позициям;

пароли не должны включать в себя легко вычисляемые сочетания символов, которые можно угадать, в том числе основываясь на информации о работниках Администрации – владельцах паролей (имена, номера телефонов, даты рождения и т.д.), не содержать последовательность идентичных символов и не состоять из полностью числовых или полностью буквенных групп;

процедура генерации паролей осуществляется работниками Администрации самостоятельно.

2.5. Проведение инструктажа с работниками Администрации по правилам использования и сохранности паролей осуществляет ОИБ.

2.6. Работники Администрации обязаны:

производить периодическую смену личных паролей для доступа к информационно-телекоммуникационной сети Администрации не реже одного раза в 90 дней;

сохранять в тайне содержание паролей, не сообщать и не пересылать пароли другим лицам.

2.7. В случае компрометации паролей (либо подозрения на компрометацию) работники Администрации немедленно должны сообщить о факте компрометации непосредственному руководителю органа Администрации и администратору безопасности. Учетная запись пользователя информационной системы должна быть заблокирована и пароль должен быть заменен.

2.8. Восстановление утраченных паролей осуществляется в соответствии с пунктом 2.1 настоящей Инструкции.

3. Правила получения и обеспечения сохранности электронных идентификаторов

3.1. Электронные идентификаторы (iButton, e-Token, рутокен), содержащие

электронный ключ и используемые для доступа, регистрируются и выдаются работникам Администрации под подпись в журнале учета электронных идентификаторов в ОИБ.

3.2. В случае утери личного идентификатора пользователь информационной системы должен немедленно доложить об этом непосредственному руководителю органа Администрации и администратору безопасности. Учетная запись пользователя информационной системы должна быть заблокирована и личный идентификатор должен быть заменен.

3.3. Работники Администрации обязаны:

обеспечить сохранность электронных идентификаторов;

не оставлять без контроля в открытом доступе электронные идентификаторы;

сдать электронные идентификаторы в ОИБ или АСиПО при увольнении или переводе в другой орган Администрации.

Приложение 11

УТВЕРЖДЕНА

распоряжением администрации
Артемовского городского округа
от 16.01.2019 № 13-ра

ИНСТРУКЦИЯ
по организации антивирусной защиты информации в администрации Артемовского городского округа

1. Общие положения

1.1. Инструкция по организации антивирусной защиты информации в администрации Артемовского городского округа (далее – Инструкция) устанавливает правила применения муниципальными служащими и работниками, не замещающими должности муниципальной службы, администрации Артемовского городского округа (далее – работники) антивирусных средств защиты информации (далее – антивирусные средства) для обеспечения защиты информационных ресурсов администрации Артемовского городского округа (далее – Администрация) от разрушающего воздействия компьютерных вирусов.

1.2. Для организации в Администрации антивирусной защиты информации применяются только лицензионные и сертифицированные антивирусные средства, приобретаемые муниципальным казенным учреждением «Административно-хозяйственное управление».

1.3. Установку, настройку и обновление антивирусных средств на серверах и автоматизированных рабочих местах Администрации выполняют работники отдела автоматизированных систем и программного обеспечения управления информации администрации Артемовского городского округа (далее – специалисты АСиПО), осуществляющие проведение технического обслуживания информационных систем и средств защиты информации в Администрации.

Настройка параметров контроля антивирусных средств осуществляется в соответствии с руководством по применению конкретных антивирусных средств. Обновление баз антивирусных средств должно проводиться ежедневно в автоматическом режиме.

1.4. Ответственность за проведение мероприятий по антивирусному контролю возлагается:

на автоматизированных рабочих местах Администрации - на работников Администрации, являющихся пользователями информационных ресурсов Администрации (далее – пользователи);

на серверах Администрации - на специалистов АСиПО.

2. Правила применения антивирусных средств

2.1. Настройка антивирусных средств должна обеспечивать автоматический антивирусный контроль всех открываемых пользователем файлов, получаемых:

на внешних машинных накопителях информации;

с применением сервиса электронной почты;

при использовании информационно-телекоммуникационной сети Интернет.

2.2. При получении от антивирусных средств сообщения, содержащего предупреждение о наличии (подозрении на наличие) компьютерного вируса, пользователи обязаны:

немедленно прекратить на автоматизированных рабочих местах любую работу, не связанную с проведением антивирусного контроля;

поставить в известность о факте обнаружения зараженных компьютерным вирусом файлов лицо, передавшее зараженные файлы, для проведения анализа необходимости дальнейшего их использования;

провести удаление вируса или зараженных вирусом файлов;

обратиться за помощью к специалистам АСиПО при невозможности самостоятельного уничтожения компьютерного вируса;

провести повторную проверку зараженных файлов на предмет обнаружения компьютерных вирусов после успешного окончания антивирусного контроля зараженных файлов;

возобновить работу на автоматизированных рабочих местах только после повторного успешного окончания антивирусного контроля зараженных компьютерным вирусом файлов.

Приложение 12

УТВЕРЖДЕНА

распоряжением администрации
Артемовского городского округа
от 16.01.2019 № 13-ра

ИНСТРУКЦИЯ
по информационной безопасности при получении доступа к информационным ресурсам администрации Артемовского городского округа с использованием мобильных устройств

1. Общие положения

1.1. Инструкция по информационной безопасности при получении доступа к информационным ресурсам администрации Артемовского городского округа с использованием мобильных устройств (далее - Инструкция) регламентирует порядок обеспечения защиты информации при использовании муниципальными служащими администрации Артемовского городского округа (далее - муниципальные служащие) мобильных устройств в информационно-телекоммуникационной сети Интернет для получения доступа к информационным системам администрации Артемовского городского округа (далее - удаленный доступ).

1.2. Удаленный доступ может быть предоставлен муниципальным служащим, замещающим высшие должности муниципальной службы (далее – пользователи). Другим муниципальным служащим удаленный доступ предоставляется только после согласования с заместителем главы администрации Артемовского городского округа (далее – Администрация), курирующим сферу защиты информации.

1.3. Муниципальные служащие для получения удаленного доступа могут использовать в качестве мобильных устройств только служебные ноутбуки и планшетные компьютеры, приобретаемые муниципальным казенным учреждением «Административно-хозяйственное управление».

2. Порядок предоставления удаленного доступа

2.1. Для предоставления удаленного доступа муниципальным служащим в соответствии с Инструкцией по управлению доступом к информационным ресурсам Администрации оформляется заявка с обоснованием необходимости использования мобильного устройства и указанием информационных систем Администрации, к которым необходимо открыть удаленный доступ. Заявка подписывается первым заместителем главы Администрации.

2.2. Для обеспечения защиты информации при использовании пользователями

удаленного доступа отдел профилактики терроризма и информационной безопасности Администрации (далее – ОИБ) в соответствии с требованиями Положения о порядке организации и проведении работ по защите информации, не содержащей сведения, составляющие государственную тайну, в администрации Артемовского городского округа, определяет средства защиты информации, которые необходимо установить на мобильных устройствах.

2.3. Отдел автоматизированных систем и программного обеспечения управления информации Администрации (далее – АСиПО) после выполнения мероприятий, указанных в пунктах 2.1 и 2.2 настоящей Инструкции:

устанавливает на мобильных устройствах необходимые программное обеспечение и средства защиты информации;

заводит учетные записи пользователей (логины, пароли);

открывает удаленный доступ на мобильных устройствах только к тем информационным системам Администрации, которые указаны в заявке;

подает в ОИБ сведения об учетных данных мобильных устройств (тип, модель, заводской номер, инвентарный номер) и установленных на мобильных устройствах средств защиты информации (тип, заводской номер).

2.4. При увольнении пользователей из Администрации:

пользователи сдают мобильные устройства на хранение в учреждение, указанное в пункте 1.3 настоящей Инструкции;

специалисты АСиПО производят затирание всей служебной информации, которая содержится на сданных мобильных устройствах.

3. Обязанности пользователей

3.1. Пользователи при использовании мобильных устройств обязаны:

обрабатывать только служебную информацию;

не оставлять без личного контроля мобильные устройства;

обеспечивать сохранность мобильных устройств и целостность служебной информации;

не создавать условия, которые могут привести к компрометации их учетных записей;

квалифицированно использовать средства защиты информации, установленные на мобильных устройствах;

при возникновении проблем в работе средств защиты информации или ситуации, связанной с попыткой несанкционированного доступа посторонних лиц к служебной информации, немедленно обращаться в ОИБ.

3.2. Пользователям при работе на мобильных устройствах запрещается:

обрабатывать на мобильных устройствах информацию, отнесенную к сведениям, составляющим государственную тайну;

использовать на мобильных устройствах функцию автосохранения пароля;

изменять установленные настройки прав доступа к информационным системам Администрации, а также настройки программного обеспечения и средств защиты информации, которые установлены на мобильных устройствах.