АДМИНИСТРАЦИЯ ГОРОДСКОГО ОКРУГА ГОРОД ВОРОНЕЖ
ВОРОНЕЖСКОЙ ОБЛАСТИ
УПРАВА ЦЕНТРАЛЬНОГО РАЙОНА
ГОРОДСКОГО ОКРУГА ГОРОД ВОРОНЕЖ

ПРИКАЗ

от 30.11.2016 № 63
г. Воронеж

Об обработке и защите персональных данных

В соответствии со ст. 29, 30 Федерального закона от 02.03.2007 № 25-ФЗ «О муниципальной службе в Российской Федерации», Указом Президента РФ от 30.05.2005 № 609 «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела», Федеральным законом РФ от 27.07.2006 № 152-ФЗ «О персональных данных», Трудовым Кодексом Российской Федерации, Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении «Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», Постановлением Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» и другими определяющими случаи и особенности обработки персональных данных нормативными правовыми актами, в целях обработки и защиты персональных данных в управе Центрального района городского округа город Воронеж (далее по тексту – управа района)

ПРИКАЗЫВАЮ:

1.1. Утвердить положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации в управе района, согласно приложению № 1.

1.2. Утвердить положение об обработке и защите персональных данных в управе района, согласно приложению № 2.

1.3. Утвердить правила обработки персональных данных, устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований, в управе района, согласно приложению № 3.

1.4. Утвердить правила рассмотрения запросов субъектов персональных данных или их представителей, согласно приложению № 4.

1.5. Утвердить правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в управе района, согласно приложению № 5.

1.6. Утвердить правила работы с обезличенными персональными данными в управе района, согласно приложению № 6.

1.7. Утвердить перечень информационных систем персональных данных, согласно приложению № 7.

1.8. Утвердить типовую форму согласия на обработку персональных данных муниципального служащего, согласно приложению № 8.

1.9. Утвердить типовую форму согласия на обработку персональных данных иных субъектов персональных данных, согласно приложению № 9.

1.10. Утвердить типовую форму разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные, согласно приложению № 10.

1.11. Утвердить типовое обязательство о неразглашении персональных данных субъекта персональных данных работников управы района непосредственно осуществляющих их обработку, согласно приложению № 11.

1.12. Утвердить порядок доступа работников управы района в помещения, в которых ведется обработка персональных данных, согласно приложению № 12.

1.13. Утвердить инструкцию администратору безопасности ИСПДн управы района, согласно приложению № 13.

1.14. Утвердить инструкцию по организации антивирусной защиты в ИСПДн управы района, согласно приложению № 14.

1.15. Утвердить инструкцию о порядке технического обслуживания и ремонта технических средств ИСПДн управы района, согласно приложению № 15.

1.16. Утвердить инструкцию по организации парольной защиты в ИСПДн управы района, согласно приложению № 16.

1.17. Утвердить инструкцию по порядку учета и хранению съемных носителей персональных данных в управе района, согласно приложению № 17.

1.18. Утвердить инструкцию пользователю автоматизированных систем ИСПДн управы района, согласно приложению № 18.

1.19. Утвердить инструкцию о порядке действий при возникновении чрезвычайных ситуаций в ИСПДн управы района, согласно приложению № 19.

2. Должностным лицам, ответственным за реализацию мер по обеспечению сохранности персональных данных подразделений обеспечить защиту персональных данных в соответствии с настоящим приказом.

3. Признать утратившим силу приказ управы района от 19.02.2016 № 19 «Об обработке и защите персональных данных».

4. Контроль за исполнением настоящего приказа возложить на руководителя аппарата управы района И.Н. Шеину.

Руководитель управы района А.А. Попов

Приложение №1
к приказу управы Центрального
района городского округа
город Воронеж

от «30» 11.2016 № 63

ПОЛОЖЕНИЕ
об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации в управе района

1. Общие положения

Обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы (далее - персональные данные), считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

Обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержатся в информационной системе персональных данных либо были извлечены из нее.

Правила обработки персональных данных, осуществляемой без использования средств автоматизации, установленные нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами организации, должны применяться с учетом требований настоящего Положения.

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

Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее - материальные носители), в специальных разделах или на полях форм (бланков).

При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе сотрудники организации-оператора или лица, осуществляющие такую обработку по договору с оператором), должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется оператором без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами организации (при их наличии).

При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма), должны соблюдаться следующие условия:

а) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о

цели обработки персональных данных, осуществляемой без использования средств автоматизации, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;

б) типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации - при необходимости получения письменного согласия на обработку персональных данных;

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

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

При ведении журналов (реестров, книг), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях, должны соблюдаться следующие условия:

а) необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена актом оператора, содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно

или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных, а также сведения о порядке пропуска субъекта персональных данных на территорию, на которой находится оператор, без подтверждения подлинности персональных данных, сообщенных субъектом персональных данных;

б) копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается;

в) персональные данные каждого субъекта персональных данных могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска субъекта персональных данных на территорию, на которой находится оператор.

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

а) при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

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

копирование персональных данных, подлежащих уничтожению или блокированию.

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

Правила, предусмотренные пунктами 9 и 10 настоящего Положения, применяются также в случае, если необходимо обеспечить раздельную обработку зафиксированных на одном материальном носителе персональных данных и информации, не являющейся персональными данными.

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

3. Меры по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации

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

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

При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются оператором.

Руководитель аппарата управы района  И.Н. Шеина

Приложение № 2
к приказу управы Центрального района
городского округа город Воронеж

от «30» 11. 2016 № 63

ПОЛОЖЕНИЕ
об обработке и защите персональных данных в управе района

I. Общие положения

1.1. Положение об обработке и защите персональных данных в управе района (далее - Положение) определяет цели, содержание и порядок обработки персональных данных, меры, направленные на защиту персональных данных, а также процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в области персональных данных в управе района (далее - управа).

1.2. Настоящее Положение определяет политику управы как оператора, осуществляющего обработку персональных данных, в отношении обработки и защиты персональных данных.

1.3. Настоящее Положение разработано в соответствии с Трудовым кодексом Российской Федерации (далее - Трудовой кодекс Российской Федерации), Кодексом Российской Федерации об административных правонарушениях, Федеральным законом от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации» (далее - Федеральный закон «О порядке рассмотрения обращений граждан Российской Федерации»), Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее - Федеральный закон «О персональных данных»), Федеральным законом от 02.03.2007 № 25-ФЗ «О муниципальной службе в Российской

Федерации», Федеральным законом от 25.12.2008 № 273-ФЗ «О противодействии коррупции» (далее - Федеральный закон «О противодействии коррупции»), Федеральным законом от 27.07.2010 № 210-ФЗ «Об организации предоставления муниципальных и муниципальных услуг» (далее - Федеральный закон «Об организации предоставления муниципальных и муниципальных услуг»), Указом Президента Российской Федерации от 30.05.2005 № 609 «Об утверждении Положения о персональных данных муниципального гражданского служащего Российской Федерации и ведении его личного дела», постановлением Правительства Российской Федерации от 06.07.2008 № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных», постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

1.4. Обработка персональных данных в управе осуществляется с соблюдением принципов и условий, предусмотренных настоящим Положением и законодательством Российской Федерации в области персональных данных.

II. Условия и порядок обработки персональных данных сотрудников управы.

2.1. Персональные данные сотрудников управы, обрабатываются в целях обеспечения кадровой работы, в том числе в целях содействия в прохождении службы, учета результатов исполнения должностных обязанностей, обеспечения личной безопасности сотрудников управы и членов их семьи, обеспечения сотрудниками управы установленных законодательством Российской Федерации условий труда, гарантий и компенсаций, сохранности принадлежащего им имущества, а также в целях противодействия коррупции.

2.2. В целях, указанных в пункте 2.1 настоящего Положения, обрабатываются следующие категории персональных данных сотрудников управы:

2.2.1. Фамилия, имя, отчество (в том числе предыдущие фамилии, имена и (или) отчества, в случае их изменения).

2.2.2. Число, месяц, год рождения.

2.2.3. Место рождения.

2.2.4. Информация о гражданстве (в том числе предыдущие гражданства, иные гражданства).

2.2.5. Вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи.

2.2.6. Адрес места жительства (адрес регистрации, фактического проживания).

2.2.7. Номер контактного телефона или сведения о других способах связи.

2.2.8. Реквизиты страхового свидетельства муниципального пенсионного страхования.

2.2.9. Идентификационный номер налогоплательщика.

2.2.10. Реквизиты страхового медицинского полиса обязательного медицинского страхования.

2.2.11. Реквизиты свидетельства муниципальной регистрации актов гражданского состояния.

2.2.12. Семейное положение, состав семьи и сведения о близких родственниках.

2.2.13. Сведения о трудовой деятельности.

2.2.14. Сведения о воинском учете и реквизиты документов воинского учета.

2.2.15. Сведения об образовании, в том числе о послевузовском профессиональном образовании (наименование и год окончания образовательного учреждения, наименование и реквизиты документа об образовании, квалификация, специальность по документу об образовании).

2.2.16. Сведения об ученой степени.

2.2.17. Информация о владении иностранными языками, степень владения.

2.2.18. Медицинское заключение по установленной форме об отсутствии у гражданина заболевания, препятствующего поступлению на государственную гражданскую службу или ее прохождению.

2.2.19. Фотография.

2.2.20. Сведения о прохождении службы, в том числе: дата, основания поступления на службу и назначения на должность, дата, основания назначения, перевода, перемещения на иную должность, наименование замещаемых должностей с указанием структурных подразделений, размера денежного содержания, результатов аттестации на соответствие замещаемой должности муниципальной службы, а также сведения о прежнем месте работы.

2.2.21. Информация, содержащаяся в трудовом договоре (контракте), дополнительных соглашениях к трудовому договору (контракту).

2.2.22. Сведения о пребывании за границей.

2.2.23. Информация о классном чине муниципальной службы (в том числе дипломатическом ранге, воинском или специальном звании, классном чине правоохранительной службы, классном чине гражданской службы субъекта Российской Федерации).

2.2.24. Информация о наличии или отсутствии судимости.

2.2.25. Информация об оформленных допусках к государственной тайне.

2.2.26. Государственные награды, иные награды и знаки отличия.

2.2.27. Сведения о профессиональной переподготовке и (или) повышении квалификации.

2.2.28. Информация о ежегодных оплачиваемых отпусках, учебных отпусках и отпусках без сохранения денежного содержания.

2.2.29. Сведения о доходах, об имуществе и обязательствах имущественного характера.

2.2.30. Номер расчетного счета.

2.2.31. Номер банковской карты.

2.2.32. Иные персональные данные, необходимые для достижения целей, предусмотренных пунктом 2.1 настоящего Положения.

2.3. Обработка персональных данных сотрудников управы, осуществляется с согласия указанных лиц, за исключением случаев, предусмотренных частью 2 статьи 11 Федерального закона «О персональных данных».

2.4. Обработка специальных категорий персональных данных сотрудников управы, осуществляется с письменного согласия указанных лиц, за исключением случаев, предусмотренных действующим законодательством.

2.5. Обработка персональных данных сотрудников управы, осуществляется при условии получения согласия указанных лиц в следующих случаях:

2.5.1. При передаче (распространении, предоставлении) персональных данных третьим лицам в случаях, не предусмотренных действующим законодательством Российской Федерации о муниципальной службе;

2.5.2. При трансграничной передаче персональных данных;

2.5.3. При принятии решений, порождающих юридические последствия в отношении указанных лиц или иным образом затрагивающих их права и законные интересы, на основании исключительно автоматизированной обработки их персональных данных.

2.6. В случаях, предусмотренных пунктом 2.5 настоящего Положения, согласие субъекта персональных данных оформляется в письменной форме, если иное не установлено Федеральным законом «О персональных данных».

2.7. Обработка персональных данных сотрудников управы, осуществляется отделом по работе с обращениями граждан и документооборота (далее - кадровое подразделение) и включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

2.8. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных сотрудников управы, осуществляется путем:

2.8.1. Получения оригиналов необходимых документов (заявление, трудовая книжка, автобиография, иные документы, предоставляемые в кадровое подразделение).

2.8.2. Копирования оригиналов документов.

2.8.3. Внесения сведений в учетные формы (на бумажных и электронных носителях).

2.8.4. Формирования персональных данных в ходе кадровой работы.

2.8.5. Внесения персональных данных в информационные системы управы, используемые кадровым подразделением.

2.9. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных осуществляется путем получения персональных данных непосредственно от сотрудников управы.

2.10. В случае возникновения необходимости получения персональных данных сотрудника управы у третьей стороны, то он должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Управа должна сообщить указанным лицам о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа дать письменное согласие на их получение.

2.11. Запрещается получать, обрабатывать и приобщать к личному делу сотрудника управы персональные данные, не предусмотренные пунктом 2.2 настоящего Положения, в том числе касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни.

2.12. При сборе персональных данных сотрудник кадрового подразделения, осуществляющий сбор (получение) персональных данных непосредственно от сотрудников управы обязан разъяснить указанным субъектам персональных данных юридические последствия отказа предоставить их персональные данные.

2.13. Передача (распространение, предоставление) и использование персональных данных сотрудников управы осуществляется лишь в случаях и в порядке, предусмотренных федеральными законами.

III. Условия и порядок обработки персональных данных субъектов в связи с предоставлением муниципальных и государственных услуг

3.1. В управе обработка персональных данных физических лиц осуществляется в целях предоставления муниципальных и государственных услуг (далее по тексту – услуги).

3.2. Персональные данные граждан, обратившихся в управу лично, а также направивших индивидуальные или коллективные письменные обращения или обращения в форме электронного документа, обрабатываются в целях рассмотрения указанных обращений с последующим уведомлением заявителей о результатах рассмотрения.

В соответствии с законодательством Российской Федерации в управе подлежат рассмотрению обращения граждан Российской Федерации, иностранных граждан и лиц без гражданства.

3.3. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных субъектов, обратившихся в управу для получения услуги, осуществляется путем:

3.3.1. Получения оригиналов необходимых документов (заявление).

3.3.2. Заверения копий документов.

3.3.3. Внесения сведений в учетные формы (на бумажных и электронных носителях).

3.3.4. Внесения персональных данных в прикладные программные подсистемы Единой информационной системы управы.

3.4. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных осуществляется путем получения персональных данных непосредственно от субъектов персональных данных (заявителей).

3.5. При предоставлении услуги управе запрещается запрашивать у субъектов персональных данных и третьих лиц, а также обрабатывать персональные данные в случаях, не предусмотренных законодательством Российской Федерации.

3.6. При сборе персональных данных уполномоченное должностное лицо структурного подразделения управы, осуществляющее получение персональных данных непосредственно от субъектов персональных данных, обратившихся за предоставлением услуги, обязано разъяснить указанным субъектам персональных данных юридические последствия отказа предоставить персональные данные.

3.7. Передача (распространение, предоставление) и использование персональных данных заявителей (субъектов персональных данных) в управе осуществляется лишь в случаях и в порядке, предусмотренных федеральными законами.

3.8. Перечень должностей служащих управы, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным в связи с предоставлением муниципальных услуг утверждается приказом управы района.

IV. Порядок обработки персональных данных субъектов персональных данных в информационных системах

4.1. Обработка персональных данных в управе осуществляется:

4.1.1. В информационной системе персональных данных управы.

4.1.2. На аттестованных под обработку персональных данных автоматизированных рабочих местах, входящих в состав Единой информационной системы управы.

4.1.3. На автоматизированных рабочих местах сотрудников кадрового подразделения управы.

4.1.4. Без использования средств автоматизации.

4.2. Информационная система персональных данных управы (далее - ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

К ИСПДн относятся:

- «Административная комиссия»;

- «Кадры»;

- «Бухгалтерия»;

- «Опека»;

- «Приемная граждан»;

- «Обращения граждан»;

- «Услуги по перепланировке»;

- «Летний отдых»;

- «ФК и спорт»;

- «Комиссия по делам несовершеннолетних»;

ИСПДн содержит персональные данные сотрудников управы, субъектов (заявителей), обратившихся в управу в целях получения услуг, и включает:

4.2.1. Персональный идентификатор.

4.2.2. Фамилию, имя, отчество субъекта персональных данных.

4.2.3. Вид документа, удостоверяющего личность субъекта персональных данных.

4.2.4. Серию и номер документа, удостоверяющего личность субъекта персональных данных, сведения о дате выдачи указанного документа и выдавшем его органе.

4.2.5. Адрес места жительства субъекта персональных данных.

4.2.6. Почтовый адрес субъекта персональных данных.

4.2.7. Контактный телефон, факс (при наличии) субъекта персональных данных.

4.2.8. Адрес электронной почты субъекта персональных данных.

4.2.9. ИНН субъекта персональных данных.

4.3. Автоматизированные рабочие места сотрудников кадрового подразделения предполагают обработку персональных данных сотрудников управы, предусмотренных пунктом 2.2 настоящего Положения.

4.4. Классификация информационных систем персональных данных, указанных в пункте 4.1 настоящего Положения, осуществляется в порядке, установленном законодательством Российской Федерации.

4.5. Сотрудникам управы, имеющим право осуществлять обработку персональных данных в информационных системах, предоставляется уникальный логин и пароль для доступа к соответствующей информационной системе. Доступ предоставляется к прикладным программным подсистемам в соответствии с функциями, предусмотренными должностными инструкциями сотрудников управы.

Информация может вноситься как в автоматическом режиме, при получении персональных данных с Единого портала муниципальных услуг или официального сайта администрации городского округа город Воронеж, так и в ручном режиме, при получении информации на бумажном носителе или в ином виде, не позволяющем осуществлять ее автоматическую регистрацию.

4.6. Обеспечение безопасности персональных данных, обрабатываемых в информационных системах персональных данных управы, достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, а также принятия следующих мер по обеспечению безопасности:

4.6.1. Определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

4.6.2. Применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение

которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных.

4.6.3. Применение прошедших в установленном порядке процедур оценки соответствия средств защиты информации.

4.6.4. Оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных, а так же не реже 1 раза в 3 года при последующей работе ИСПДн.

4.6.5. Учет машинных носителей персональных данных.

4.6.6. Обнаружение фактов несанкционированного доступа к персональным данным и принятие мер.

4.6.7. Восстановление персональных данных, модифицированных или удаленных, уничтоженных вследствие несанкционированного доступа к ним.

4.6.8. Установление правил доступа к персональным данным, обрабатываемым в информационных системах персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационных системах персональных данных.

4.6.9. Контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровней защищенности информационных систем персональных данных.

4.7. Лицо, ответственное за обеспечение информационной безопасности в управе, организует и контролирует ведение учета материальных носителей персональных данных.

4.8. Лицо, ответственное за обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных, должно обеспечить:

4.8.1. Своевременное обнаружение фактов несанкционированного доступа к персональным данным и немедленное доведение этой информации до ответственного за организацию обработки персональных данных в управе.

4.8.2. Недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование.

4.8.3. Возможность восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

4.8.4. Постоянный контроль за обеспечением уровня защищенности персональных данных.

4.8.5. Знание и соблюдение условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией.

4.8.6. Учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных.

4.8.7. При обнаружении нарушений порядка предоставления персональных данных незамедлительное приостановление предоставления персональных данных пользователям информационной системы персональных данных до выявления причин нарушений и устранения этих причин.

4.8.8. Разбирательство и составление заключений по фактам несоблюдения условий хранения материальных носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

4.9. Лицо, ответственное за обеспечение функционирования информационных систем персональных данных в управе, принимает все необходимые меры по восстановлению персональных данных, модифицированных или удаленных, уничтоженных вследствие несанкционированного доступа к ним.

4.10. Обмен персональными данными при их обработке в информационных системах персональных данных осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и путем применения программных и технических средств.

4.11. Доступ сотрудников управы к персональным данным, находящимся в информационных системах персональных данных, предусматривает обязательное прохождение процедуры идентификации и аутентификации.

4.12. В случае выявления нарушений порядка обработки персональных данных в информационных системах персональных данных уполномоченными должностными лицами незамедлительно принимаются меры по установлению причин нарушений и их устранению.

V. Сроки обработки и хранения персональных данных.

5.1. Сроки обработки и хранения персональных данных сотрудников управы, определяются в соответствии с законодательством Российской Федерации. С учетом положений законодательства Российской Федерации, устанавливаются следующие сроки обработки и хранения персональных данных муниципальных служащих:

5.1.1. Персональные данные, содержащиеся в приказах по личному составу сотрудников управы (о приеме, о переводе, об увольнении, об установлении надбавок), подлежат хранению в кадровом подразделении в течение двух лет, с последующим формированием и передачей указанных

документов в муниципальное бюджетное учреждение «Муниципальный архив городского округа город Воронеж» или государственный архив в порядке, предусмотренном законодательством Российской Федерации, где хранятся в течение 75 лет.

5.1.2. Персональные данные, содержащиеся в личных делах сотрудников управы, а также личных карточках муниципальных служащих, хранятся в кадровом подразделении в течение десяти лет, с последующим формированием и передачей указанных документов в муниципальное бюджетное учреждение «Муниципальный архив городского округа город Воронеж» или государственный архив в порядке, предусмотренном законодательством Российской Федерации, где хранятся в течение 75 лет.

5.1.3. Персональные данные, содержащиеся в приказах о поощрениях, материальной помощи сотрудникам управы, подлежат хранению в течение двух лет в кадровом подразделении с последующим формированием и передачей указанных документов в муниципальное бюджетное учреждение «Муниципальный архив городского округа город Воронеж» или государственный архив в порядке, предусмотренном законодательством Российской Федерации, где хранятся в течение 75 лет.

5.1.4. Персональные данные, содержащиеся в приказах о предоставлении отпусков, о краткосрочных внутрироссийских и зарубежных командировках, о дисциплинарных взысканиях сотрудников управы, подлежат хранению в кадровом подразделении в течение пяти лет с последующим уничтожением.

5.2. Сроки обработки и хранения персональных данных, предоставляемых субъектами персональных данных в управу в связи с получением услуг определяются нормативными правовыми актами, регламентирующими порядок их сбора и обработки.

5.3. Персональные данные граждан, обратившихся в управу лично, а также направивших индивидуальные или коллективные письменные

обращения или обращения в форме электронного документа, хранятся в течение пяти лет.

5.4. Персональные данные, предоставляемые субъектами на бумажном носителе в связи с предоставлением услуг, хранятся на бумажных носителях в структурных подразделениях управы, к полномочиям которых относится обработка персональных данных в связи с предоставлением услуги, в соответствии с утвержденными положениями о соответствующих структурных подразделениях управы.

5.5. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на разных материальных носителях персональных данных, в специальных разделах или на полях форм (бланков).

5.6. Необходимо обеспечивать раздельное хранение персональных данных на разных материальных носителях, обработка которых осуществляется в различных целях, определенных настоящим Положением.

5.7. Контроль за хранением и использованием материальных носителей персональных данных, не допускающий несанкционированное использование, уточнение, распространение и уничтожение персональных данных, находящихся на этих носителях, осуществляют руководители структурных подразделений управы.

5.8. Срок хранения персональных данных, внесенных в информационные системы персональных данных, указанные в пункте 5.1 настоящего Положения, должен соответствовать сроку хранения бумажных оригиналов.

VI. Порядок уничтожения персональных данных при достижении целей их обработки или при наступлении иных законных оснований

6.1. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных.

6.2. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

6.3. В случае выявления неправомерной обработки персональных данных, уполномоченное должностное лицо в срок, не превышающий 3 (трех) рабочих дней с даты этого выявления, обязано прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению управы. В случае, если обеспечить правомерность обработки персональных данных невозможно, уполномоченное должностное лицо в срок, не превышающий 10(десяти) рабочих дней с даты выявления неправомерной обработки персональных данных, обязано уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных уполномоченное должностное лицо обязано уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

6.4. В случае достижения цели обработки персональных данных структурные подразделения и должностные лица управы, осуществляющие

обработку персональных данных, обязаны прекратить их обработку или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению управы) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению управы) в срок, не превышающий 30 (тридцати) дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между управой и субъектом персональных данных либо если управа не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных федеральными законами.

6.5. В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных структурное подразделение, должностное лицо управы обязано прекратить их обработку и уничтожить персональные данные в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между управой и субъектом персональных данных. Об уничтожении персональных данных управа обязана уведомить субъекта персональных данных.

6.6. В случае отсутствия возможности уничтожения персональных данных в течение сроков, указанных выше, управа осуществляет блокирование таких персональных данных или обеспечивает их блокирование и обеспечивает уничтожение персональных данных в срок не более чем 6 (шести) месяцев, если иной срок не установлен федеральными законами.

VII. Рассмотрение запросов субъектов персональных данных

или их представителей

7.1. Сотрудники управы и лица, состоящих с ними в родстве (свойстве), а также граждане, персональные данные которых обрабатываются в управе в связи с предоставлением услуг, имеют право на получение информации, касающейся обработки их персональных данных, в том числе содержащей:

7.1.1. Подтверждение факта обработки персональных данных в управе.

7.1.2. Правовые основания и цели обработки персональных данных.

7.1.3. Цели и применяемые в управе способы обработки персональных данных.

7.1.4. Наименование и место нахождения управы, сведения о лицах (за исключением муниципальных служащих управы), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с управой или на основании федерального закона.

7.1.5. Обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом.

7.1.6. Сроки обработки персональных данных, в том числе сроки их хранения в управе.

7.1.7. Порядок осуществления субъектом персональных данных прав, предусмотренных законодательством Российской Федерации в области персональных данных.

7.1.8. Информацию об осуществленной или предполагаемой трансграничной передаче данных.

7.1.9. Наименование организации или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению

управы, если обработка поручена или будет поручена такой организации или лицу.

7.1.10. Иные сведения, предусмотренные законодательством Российской Федерации в области персональных данных.

7.2. Лица, указанные в пункте 7.1 настоящего Положения (далее - субъекты персональных данных), вправе требовать от управы уточнения их персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

7.3. Сведения, указанные в подпунктах 7.1.1 - 7.1.10 пункта 7.1 настоящего Положения, должны быть предоставлены субъекту персональных данных оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

7.4. Сведения, указанные в подпунктах 7.1.1 - 7.1.10 пункта 7.1 настоящего Положения, предоставляются субъекту персональных данных или его представителю уполномоченным должностным лицом структурного подразделения управы, осуществляющего обработку соответствующих персональных данных при обращении либо при получении запроса субъекта персональных данных или его представителя. Запрос должен содержать:

7.4.1. Номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе.

7.4.2. Сведения, подтверждающие участие субъекта персональных данных в правоотношениях с управой, либо сведения, иным образом подтверждающие факт обработки персональных данных в управе, подпись

субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с пунктом 4 части 2 статьи 9 Федерального закона «О персональных данных» и статьей 6 Федерального закона «Об электронной подписи».

7.5. Рассмотрение запросов осуществляется должностными лицами, в чьи обязанности входит обработка персональных данных.

7.6. Должностные лица управы обеспечивают:

- объективное, всестороннее и своевременное рассмотрение запроса;
- принятие мер, направленных на восстановление или защиту нарушенных прав, свобод и законных интересов субъектов персональных данных;
- направление письменных ответов по существу запроса.

7.7. В случае, если сведения, указанные в подпунктах 7.1.1 - 7.1.10 пункта 7.1 настоящего Положения, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно в управу или направить повторный запрос в целях получения указанных сведений и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

7.8. Субъект персональных данных вправе обратиться повторно в управу или направить повторный запрос в целях получения сведений, указанных в подпунктах 7.1.1 - 7.1.10 пункта 7.1 настоящего Положения, а также в целях ознакомления с обрабатываемыми персональными данными до

истечения срока, указанного в пункте 7.7 настоящего Положения, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в пункте 7.4 настоящего Положения, должен содержать обоснование направления повторного запроса.

7.9. Управа (уполномоченное должностное лицо управы) вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктами 7.7 и 7.8 настоящего Положения. Такой отказ должен быть мотивированным.

7.10. Должностные лица управы при рассмотрении и разрешении запроса обязаны:

- внимательно разобраться в его содержании, в случае необходимости истребовать дополнительные материалы или направить сотрудников на места для проверки фактов, изложенных в запросе, принять другие меры для объективного разрешения поставленных заявителем вопросов, выявления и устранения причин и условий, порождающих факты нарушения законодательства о персональных данных;
- принимать по запросу законные, обоснованные и мотивированные решения и обеспечивать своевременное и качественное их исполнение;
- сообщать в письменной форме заявителю о решениях, принятых по его запросу, со ссылками на законодательство Российской Федерации, а в случае отклонения запроса - разъяснять также порядок обжалования принятого решения.

7.11. Управа обязана сообщить субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение

тридцати дней с даты получения запроса субъекта персональных данных или его представителя.

7.12. В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя уполномоченные должностные лица управы обязаны дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий тридцати дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя.

7.13. Управа обязана предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных.

7.14. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, уполномоченные должностные лица управы обязаны внести в них необходимые изменения.

7.15. В срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, уполномоченные должностные лица управы обязаны уничтожить такие персональные данные.

7.16. Управа обязана уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

7.17. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных уполномоченные должностные лица управы обязаны осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных с момента такого обращения или получения указанного запроса на период проверки.

7.18. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных уполномоченные должностные лица управы обязаны осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

7.19. В случае подтверждения факта неточности персональных данных уполномоченные должностные лица управы на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязаны уточнить персональные данные в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

7.20. Для проверки фактов, изложенных в запросах, при необходимости организуются служебные проверки в соответствии с законодательством Российской Федерации.

7.21. По результатам служебной проверки составляется мотивированное заключение, которое должно содержать объективный анализ собранных материалов. Если при проверке выявлены факты совершения работником управы действия (бездействия), содержащего признаки административного правонарушения или состава преступления информация о данном факте передается незамедлительно в правоохранительные органы. Результаты служебной проверки докладываются руководителю управы района.

7.22. Запрос считается исполненным, если рассмотрены все поставленные в нем вопросы, приняты необходимые меры и даны исчерпывающие ответы заявителю.

7.23. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе если доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

VIII. Лицо, ответственное за организацию обработки персональных данных в управе

8.1. Ответственный за организацию обработки персональных данных в управе (далее - Ответственный за обработку персональных данных) назначается из числа муниципальных служащих, относящихся к высшей и (или) главной группе должностей в соответствии с распределением обязанностей.

8.2. Ответственный за обработку персональных данных в своей работе руководствуется законодательством Российской Федерации в области персональных данных и настоящим Положением.

8.3. Ответственный за обработку персональных данных обязан:

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

8.3.2. Осуществлять внутренний контроль за соблюдением муниципальными служащими требований законодательства Российской Федерации в области персонала.

8.3.3. Доводить до сведения сотрудников управы положения законодательства Российской Федерации в области персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных.

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

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

8.4. Ответственный за обработку персональных данных вправе:

8.4.1. Иметь доступ к информации, касающейся обработки персональных данных в управе и включающей.

8.4.1.1. Цели обработки персональных данных.

8.4.1.2. Категории обрабатываемых персональных данных.

8.4.1.3. Категории субъектов, персональные данные которых обрабатываются.

8.4.1.4. Правовые основания обработки персональных данных.

8.4.1.5. Перечень действий с персональными данными, общее описание используемых в управе способов обработки персональных данных.

8.4.1.6. Описание мер, предусмотренных статьями 18.1 и 19 Федерального закона «О персональных данных», в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств.

8.4.1.7. Дату начала обработки персональных данных.

8.4.1.8. Срок или условия прекращения обработки персональных данных.

8.4.1.9. Сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки.

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

8.4.2. Привлекать к реализации мер, направленных на обеспечение безопасности персональных данных, обрабатываемых в управе, иных муниципальных служащих с возложением на них соответствующих обязанностей и закреплением ответственности.

8.5. Ответственный за обработку персональных данных в управе несет ответственность за ненадлежащее выполнение возложенных функций по организации обработки персональных данных в управе в соответствии с положениями законодательства Российской Федерации в области персональных данных.

Руководитель аппарата управы района  И.Н. Шеина

Приложение № 3
к приказу управы Центрального
района городского округа
город Воронеж

от «30» 11.2016 № 63

ПРАВИЛА
обработки персональных данных, устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований в управе района

1. Обработка персональных данных должна осуществляться на законной и справедливой основе.

2. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

4. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

5. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

6. При обработке персональных данных должны быть обеспечены

точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

7. Меры, направленные на выявление и предотвращение нарушений, предусмотренных законодательством.

1) осуществление внутреннего контроля и (или) аудита, соответствия обработки персональных данных Федеральному закону РФ от 27.07.2006 № 152-ФЗ «О персональных данных» (далее - Федеральный закон) и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора;

2) оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом;

3) ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

8. Обеспечение безопасности персональных данных достигается, в частности:

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

2) применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

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

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

5) учетом машинных носителей персональных данных;

6) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

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

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

9. Целями обработки персональных данных работников являются:

1) обеспечение соблюдения законов и иных нормативных правовых актов;

2) соблюдение порядка и правил приема на службу;

3) использование в деятельности с применением средств автоматизации или без таких средств, включая хранение этих данных в архивах и размещение в информационно-телекоммуникационных сетях с целью предоставления доступа к ним;

4) заполнение базы данных автоматизированной информационной системы в целях повышения эффективности и быстрого поиска, проведения мониторинговых исследований, формирования статистических и аналитических отчётов в вышестоящие органы;

6) обеспечение личной безопасности работников.

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

11. В случае выявления неправомерной обработки персональных данных, осуществляемой оператором или лицом, действующим по поручению оператора, оператор в срок, не превышающий 3 (трех) рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению оператора, В случае, если обеспечить правомерность обработки персональных данных невозможно, оператор в срок, не превышающий 10 (десяти) рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос

уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

12. В случае достижения цели обработки персональных данных оператор обязан прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий 30 (тридцати) дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных настоящим Федеральным законом или другими федеральными законами.

13. В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных оператор обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между оператором и субъектом персональных данных. Об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных.

14. В случае отсутствия возможности уничтожения персональных данных в течение сроков, указанных выше, оператор осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим

лицом, действующим по поручению оператора) и обеспечивает уничтожение персональных данных в срок не более чем 6 (шесть) месяцев, если иной срок не установлен федеральными законами.

Руководитель аппарата управы района  И.Н. Шеина

Приложение № 4
к приказу управы Центрального
района городского округа
город Воронеж

от «30» 11.2016 № 63

ПРАВИЛА
рассмотрения запросов субъектов персональных данных или их представителей в управе района

1. Настоящими Правилами рассмотрения запросов субъектов персональных данных или их представителей в управе района (далее – Правила) определяются порядок учета (регистрации), рассмотрения запросов субъектов персональных данных или их представителей (далее – запросы).

2. Настоящие Правила разработаны в соответствии Федеральным законом от 27.07.2006 № 152 ФЗ «О персональных данных» (далее – Федеральный закон), Федеральным законом от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации», Трудовым Кодексом Российской Федерации, Постановлением Правительства Российской Федерации от 15.09. 2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации», Постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» и другими нормативными правовыми актами.

3. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных (часть 7 статьи 14 Федерального закона), в том числе содержащей:

– подтверждение факта обработки персональных данных в управе района (далее – Организация);

– правовые основания и цели обработки персональных данных;

– цели и применяемые в Организации;

– наименование и место нахождения в Организации, сведений о лицах (за исключением работников Организации), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Организацией или на основании федерального закона;

– обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

– сроки обработки персональных данных, в том числе сроки их хранения;

– порядок осуществления субъектом персональных данных прав, предусмотренных настоящим Федеральным законом;

– информацию об осуществленной или о предполагаемой трансграничной передаче данных;

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

– иные сведения, предусмотренные Федеральным законом или другими федеральными законами.

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

5. Субъект персональных данных вправе требовать от Организации уточнения его персональных данных, их блокирования или уничтожения в

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

6. Сведения, указанные в части 7 статьи 14 Федерального закона, должны быть предоставлены субъекту персональных данных в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

7. Сведения, указанные в части 7 статьи 14 Федерального закона, предоставляются субъекту персональных данных или его представителю Организацией при обращении либо при получении запроса субъекта персональных данных или его представителя.

8. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с Организацией (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Организацией, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

9. Рассмотрение запросов является служебной обязанностью руководителя аппарата управы района и уполномоченных должностных лиц, в чьи обязанности входит обработка персональных данных.

10. Должностные лица Организации обеспечивают:

- объективное, всестороннее и своевременное рассмотрения запроса;

– принятие мер, направленных на восстановление или защиту нарушенных прав, свобод и законных интересов субъектов персональных данных;

– направление письменных ответов по существу запроса.

11. Ведение делопроизводства по запросам старший инспектор по кадровой работе.

12. Все поступившие запросы регистрируются в день их поступления. На запросе проставляется штамп, в котором указывается входящий номер и дата регистрации.

13. Запрос прочитывается, проверяется на повторность, при необходимости сверяется с находящейся в архиве предыдущей перепиской. В случае, если сведения, указанные в части 7 статьи 14 Федерального закона, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно в Организацию или направить повторный запрос в целях получения сведений, указанных в части 7 статьи 14 Федерального закона, и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

Субъект персональных данных вправе обратиться повторно в Организацию или направить повторный запрос в целях получения сведений, указанных в части 7 статьи 14 Федерального закона, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в настоящем пункте, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для

ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду с необходимыми сведениями должен содержать обоснование направления повторного запроса.

14. Организация вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным частями 4 и 5 статьи 14 Федерального закона. Такой отказ должен быть мотивированным.

15. Прошедшие регистрацию запросы в тот же день докладываются руководителю Организации либо лицу, его заменяющему, который определяет порядок и сроки их рассмотрения, дает по каждому из них письменное указание исполнителям.

16. Руководитель аппарата управы района и другие должностные лица при рассмотрении и разрешении запроса обязаны:

- внимательно разобраться в их существе, в случае необходимости истребовать дополнительные материалы или направить сотрудников на места для проверки фактов, изложенных в запросах, принять другие меры для объективного разрешения поставленных заявителями вопросов, выявления и устранения причин и условий, порождающих факты нарушения законодательства о персональных данных;

- принимать по ним законные, обоснованные и мотивированные решения и обеспечивать своевременное и качественное их исполнение;

- сообщать в письменной форме заявителям о решениях, принятых по их запросам, со ссылками на законодательство Российской Федерации, а в случае отклонения запроса - разъяснять также порядок обжалования принятого решения.

17. Организация обязана сообщить субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными

при обращении субъекта персональных данных или его представителя либо в течение тридцати дней с даты получения запроса субъекта персональных данных или его представителя.

18. В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных, субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя уполномоченные должностные лица Организации обязаны дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий тридцати дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя.

19. Организация обязана предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных.

20. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, уполномоченные должностные лица Организации обязаны внести в них необходимые изменения.

21. В срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, уполномоченные должностные лица Организации обязаны уничтожить такие персональные данные.

22. Организация обязана уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

23. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных уполномоченные должностные лица Организации обязаны осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных с момента такого обращения или получения указанного запроса на период проверки.

24. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных уполномоченные должностные лица Организации обязаны осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

25. В случае подтверждения факта неточности персональных данных уполномоченные должностные лица Организации на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязаны уточнить персональные данные в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

26. В случае выявления неправомерной обработки персональных данных уполномоченные должностные лица Организации в срок, не превышающий трех рабочих дней с даты этого выявления, обязаны прекратить неправомерную обработку персональных данных. В случае, если обеспечить правомерность обработки персональных данных невозможно, уполномоченные должностные лица Организации в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязаны уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных Организация обязана уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

27. Для проверки фактов, изложенных в запросах при необходимости организуются служебные проверки в соответствии с законодательством Российской Федерации.

28. По результатам служебной проверки составляется мотивированное заключение, которое должно содержать объективный анализ собранных материалов. Если при проверке выявлены факты совершения работником Организации действия (бездействия), содержащего признаки административного правонарушения или состава преступления информация передается незамедлительно в правоохранительные органы. Результаты служебной проверки докладываются руководителя Организации.

29. Запрос считается исполненным, если рассмотрены все поставленные в нем вопросы, приняты необходимые меры и даны исчерпывающие ответы заявителю.

30. Ответы на запросы печатаются на бланке установленной формы и регистрируются за теми же номерами, что и запросы.

31. Руководитель аппарата управы района осуществляет непосредственный контроль за соблюдением установленного законодательством и настоящими Правилами порядка рассмотрения запросов.

32. При осуществлении контроля обращается внимание на сроки исполнения поручений по запросам и полноту рассмотрения поставленных вопросов, объективность проверки фактов, изложенных в запросах, законность и обоснованность принятых по ним решений, своевременность их исполнения и направления ответов заявителям.

Нарушение установленного порядка рассмотрения запросов влечет в отношении виновных должностных лиц ответственность в соответствии с законодательством Российской Федерации.

Руководитель аппарата управы района  И.Н. Шеина

Приложение №5
к приказу управы Центрального
района городского округа
город Воронеж

от «30» 11.2016 № 63

Правила
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в управе района

1. Настоящими Правилами осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее – Правила) в управе района (далее – Организация) определяются процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных; основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

2. Настоящие Правила разработаны в соответствии Федеральным законом от 27 июля 2006 г. № 152 ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации», Постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» и другими нормативными правовыми актами.

3. В настоящих Правилах используются основные понятия, определенные в статье 3 Федерального закона от 27 июля 2006 г. № 152 ФЗ «О персональных данных».

4. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в Организации организовывается проведение периодических проверок условий обработки персональных данных.

5. Проверки осуществляются ответственным за организацию обработки персональных данных в Организации либо комиссией, образуемой распоряжением руководителя Организации.

В проведении проверки не может участвовать гражданский служащий, прямо или косвенно заинтересованный в её результатах.

6. Проверки соответствия обработки персональных данных установленным требованиям в Организации проводятся на основании утвержденного руководителем Организации ежегодного плана осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям или на основании поступившего в Организацию письменного заявления о нарушениях правил обработки персональных данных (внеплановые проверки). Проведение внеплановой проверки организуется в течение трех рабочих дней с момента поступления соответствующего заявления.

7. При проведении проверки соответствия обработки персональных данных установленным требованиям должны быть полностью, объективно и всесторонне установлены:

- порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

- порядок и условия применения средств защиты информации;

- эффективность принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

- состояние учета машинных носителей персональных данных;

- соблюдение правил доступа к персональным данным;

- наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;

- мероприятия по восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- осуществление мероприятий по обеспечению целостности персональных данных.

8. Ответственный за организацию обработки персональных данных в Организации (комиссия) имеет право:

- запрашивать у сотрудников Организации информацию, необходимую для реализации полномочий;

- требовать от уполномоченных на обработку персональных данных должностных лиц уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;

- принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;

- вносить руководителю Организации предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;

- вносить руководителю Организации предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении

законодательства Российской Федерации в отношении обработки персональных данных.

9. В отношении персональных данных, ставших известными ответственному за организацию обработки персональных данных в Организации (комиссии) в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность персональных данных.

10. Проверка должна быть завершена не позднее чем через месяц со дня принятия решения о её проведении. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, руководителю Организации докладывает ответственный за организацию обработки персональных данных либо председатель комиссии, в форме письменного заключения.

11. Руководитель Организации, назначивший внеплановую проверку, обязан контролировать своевременность и правильность её проведения.

Руководитель аппарата управы района  И.Н. Шеина

Приложение № 6
к приказу управы Центрального
района городского округа
город Воронеж

от «30» 11.2016 № 63

ПРАВИЛА
работы с обезличенными персональными данными
в управе района

1. Общие положения

1.1. Настоящие Правила работы с обезличенными персональными данными управы района (далее – Организация) разработаны с учетом Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и постановления Правительства РФ от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

1.2. Настоящие Правила определяют порядок работы с обезличенными данными Организации.

2. Термины и определения

2.1. В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»:

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

2.1.2. Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение,

использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

2.1.3. Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

3. Условия обезличивания

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

3.2. Способы обезличивания при условии дальнейшей обработки персональных данных:

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

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

3.4. Для обезличивания персональных данных годятся любые способы явно не запрещенные законодательно.

3.4.1. Ответственное лицо Организации принимает решение о необходимости обезличивания персональных данных;

3.4.2. Начальники отделов, непосредственно осуществляющие обработку персональных данных, готовят предложения по обезличиванию персональных данных, обоснование такой необходимости и способ обезличивания;

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

4. Порядок работы с обезличенными персональными данными

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

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

4.3. При обработке обезличенных персональных данных с использованием средств автоматизации необходимо соблюдение:

- парольной политики;
- антивирусной политики;
- правил работы со съемными носителями (если они используется);
- правил резервного копирования;
- правил доступа в помещения, где расположены элементы информационных систем.

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

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

Руководитель аппарата управы района  И.Н. Шеина

Приложение № 7
к приказу управы Центрального
района городского округа
город Воронеж

от «30» 11.2016 № 63

ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ СИСТЕМ
ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Понятие информационной системы персональных данных.

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

2. Информационные системы персональных данных в управе Центрального района городского округа город Воронеж:

1) «Бухгалтерия»
2) «Кадры»
3) «Летний отдых»
4) «ФК и спорт»
5) «Комиссия по делам несовершеннолетних»
6) «Обращения граждан»
7) «Услуги по перепланировке»
8) «Приемная граждан»
9) «Административная комиссия»
10) «Опека»

Руководитель аппарата управы района И.Н. Шеина

Приложение № 8
к приказу управы Центрального
района **городского** округа
город Воронеж

от «30» 11.2016 № 63

СОГЛАСИЕ
субъекта персональных данных
на обработку персональных данных

Я, _____,

паспорт серия _____, номер _____,

выданный _____

"___" _____ _____ года, даю согласие управе Центрального района городского округа город Воронеж на автоматизированную, а также без использования средств автоматизации обработку моих персональных данных, а именно – совершение действий, предусмотренных п. 3 ч. 1 ст. 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных), и содержащихся в настоящем заявлении, в целях обеспечения соблюдения трудового законодательства и иных нормативных правовых актов, содействия в трудоустройстве, обучении и продвижения по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества, формирования муниципального резерва кадров, управленческого резерва для замещения вакантных должностей муниципальной службы, а именно:

фамилия, имя, отчество; сведения о смене фамилии, имени, отчества; число,

месяц, год рождения; место рождения; адрес регистрации; адрес местожительства (фактического проживания); контактный телефон; адрес электронной почты; табельный номер сотрудника; сведения из документа удостоверяющего личность; номер страхового свидетельства государственного пенсионного страхования; серия, номер полиса обязательного медицинского страхования; идентификационный номер налогоплательщика; характеристика сотрудника; сведения о воинском учете; данные, содержащиеся в военном билете; сведения об образовании, повышении квалификации и профессиональной переподготовке, наличии специальных знаний; сведения о профессиональной пригодности; сведения о наградах, поощрениях, почетных званиях; сведения о месте работы (должность, структурное подразделение, категория квалификации, период работы, стаж, сведения об аттестации); информация о трудовой деятельности (трудовой стаж, информация о приеме на работу, перемещении по должности, увольнении, основание прекращения трудового договора); форма допуска; сведения о доходах; данные о трудовом договоре (№ трудового договора, дата его заключения, дата начала и дата окончания договора, вид работы, срок действия договора, наличие испытательного срока, режим труда, длительность основного и дополнительного отпусков, длительность дополнительного отпуска за ненормированный рабочий день, дополнительные социальные льготы и гарантии, № и число изменения к трудовому договору, характер работы, форма оплаты, категория персонала, условия труда, продолжительность рабочей недели, система оплаты); данные об аттестации сотрудников; информация о государственном и негосударственном пенсионном обеспечении; семейное положение; сведения о близких родственниках (фамилия, имя, отчество, степень родства, год рождения, место работы, должность, сведения о доходах, номер контактного телефона); сведения о командировках; сведения о временной

нетрудоспособности; сведения об удержаниях из заработной платы; сведения о выданных подотчетных суммах; сведения о выданных банковских картах; сведения о выплачиваемых алиментах; сведения об исправительных работах; сведения, содержащиеся в выписке из ЕГРИП; сведения о банковских счетах; сведения о привлечении к административной ответственности; свидетельство о рождении ребенка; документы, подтверждающие отсутствие родителей (свидетельство о смерти, решение суда, справка об отбывании наказания, иные); справка о прекращении выплаты государственного пособия; сведения, подтверждающие отношение гражданина к льготной категории.

Для обработки в целях

_____

_____

_____

_____

(указать цели обработки)

Я утверждаю, что ознакомлен с документами управы Центрального района городского округа город Воронеж, устанавливающими порядок обработки персональных данных, а также с моими правами и обязанностями в этой области.

Согласие вступает в силу со дня его подписания и действует в течение неопределенного срока. Согласие может быть отозвано мною в любое время на основании моего письменного заявления.

"___" _____ 20___ г.

_____ _____

(подпись) (ФИО)

Руководитель аппарата управы района И.Н. Шеина

Приложение № 9
к приказу управы Центрального района
городского округа
город Воронеж

от «30» 11.2016 № 63

СОГЛАСИЕ
субъекта персональных данных
на обработку персональных данных

Я, _____,

паспорт серия _____, номер _____,

выданный _____

"___" _____ _____ года, даю согласие управе Центрального района городского округа город Воронеж на автоматизированную, а также без использования средств автоматизации обработку моих персональных данных, а именно – совершение действий, предусмотренных п. 3 ч. 1 ст. 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных), и содержащихся в настоящем заявлении, в целях реализации возложенных на управу Центрального района городского округа город Воронеж полномочий, а именно:

фамилия, имя, отчество; число, месяц, год рождения; место рождения; адрес регистрации; адрес местожительства (фактического проживания); контактный телефон; адрес электронной почты; сведения из документа удостоверяющего личность; идентификационный номер налогоплательщика.

Для обработки в целях

_____

_____

_____

(указать цели обработки)

Я утверждаю, что ознакомлен с документами управы Центрального района городского округа город Воронеж, устанавливающими порядок обработки персональных данных, а также с моими правами и обязанностями в этой области.

Согласие вступает в силу со дня его подписания и действует в течение неопределенного срока. Согласие может быть отозвано мною в любое время на основании моего письменного заявления.

"___" _____ 20___ г.

_____ _____

(подпись) (ФИО)

Руководитель аппарата управы района И.Н. Шеина

Приложение № 10
к приказу управы Центрального
района городского округа
город Воронеж

от «30» 11.2016 № 63

РАЗЪЯСНЕНИЕ
субъекту персональных данных юридических последствий отказа предоставить свои персональные данные

Уважаемый(-ая), _____
(фамилия, имя, отчество)

В соответствии с требованиями Федерального закона Российской Федерации N 152-ФЗ от 27.07.2006 "О персональных данных" уведомляем Вас, что обязанность предоставления Вами персональных данных установлена пунктом 2 части 1 статьи 6 Федерального закона «О персональных данных» (обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей).

В случае отказа Вами предоставить свои персональные данные управа Центрального района городского округа город Воронеж не сможет на законных основаниях осуществить такую обработку.

«____»_____20__ г. _____ _____
(дата) (подпись) (расшифровка подписи)

Ознакомлен:

«____»_____20__ г. _____ _____
(дата) (подпись) (расшифровка подписи)

Руководитель аппарата управы района И.Н. Шеина

Приложение № 11
к приказу управы Центрального
района городского округа
город Воронеж

от «30» 11.2016 № 63

ОБЯЗАТЕЛЬСТВО/СОГЛАШЕНИЕ
О НЕРАЗГЛАШЕНИИ ПЕРСОНАЛЬНЫХ ДАННЫХ СУБЪЕКТА
ПЕРСОНАЛЬНЫХ ДАННЫХ

Я, _____, паспорт серии _____, номер _____, выданный _____ _____ «___» _____ 20__ года в период трудовых отношений с управой Центрального района городского округа город Воронеж и в течение _____ лет после их прекращения в соответствии с распоряжением управы Центрального района городского округа город Воронеж от «__»_____20__ г. №_____ обязуюсь:

1) не разглашать и не передавать третьим лицам сведения, содержащие персональные данные, которые мне будут доверены или станут известны по работе, кроме случаев, предусмотренных законодательством Российской Федерации и с разрешения ответственного за обработку данных в управе Центрального района городского округа город Воронеж;

2) выполнять требования приказов, распоряжения и инструкций по обработке персональных данных в части меня касающейся;

3) в случае попытки посторонних лиц получить от меня сведения, содержащие персональные данные, а также в случае утери носителей информации, содержащих такие сведения, немедленно сообщить об этом лицу, ответственному за обработку персональных данных;

4) не производить преднамеренных действий, нарушающих достоверность, целостность или конфиденциальность персональных данных,

хранимых и обрабатываемых в управе Центрального района городского округа город Воронеж.

До моего сведения также доведены:

_____

_____

_____

_____

(указываются муниципальные правовые акты)

Мне известно, что нарушение этого обязательства может повлечь ответственность, предусмотренную трудовым, административным и уголовным законодательством Российской Федерации.

«___» _____ 20___ г. _____

(подпись)

Руководитель аппарата управы района И.Н. Шеина

Приложение № 12
к приказу управы Центрального
района городского округа
город Воронеж

от «30» 11.2016 № 63

ПОРЯДОК
доступа работников управы района в помещения,
в которых ведется обработка персональных данных

1. Общие положения

Настоящий Порядок доступа работников управы Центрального района городского округа город Воронеж в помещения, в которых ведется обработка персональных данных, (далее – Порядок) устанавливает единые требования к доступу работников управы района (далее – Организация) в служебные помещения, в целях предотвращения нарушения прав субъектов персональных данных, обрабатываемых в Организации и обеспечения соблюдения требований законодательства о персональных данных.

Настоящий Порядок обязателен для применения и исполнения всеми работниками Организации.

Служебными помещениями, в которых ведется обработка персональных данных, являются кабинеты, расположенные по адресу: г. Воронеж, ул. Никитинская, 8:

- кабинеты №№ 303, 304 – ИСПДн «Бухгалтерия»;
- кабинеты № 205, 207 – ИСПДн «Кадры»;
- кабинет № 502 – ИСПДн «Комиссия по делам несовершеннолетних»;
- кабинет № 414 – ИСПДн «Летний отдых»;
- кабинеты №№ 410, 414 – ИСПДн «ФК и спорт»;
- кабинет № 109 – ИСПДн «Обращения граждан»;
- кабинет № 114 – ИСПДн «Услуги по перепланировке»;
- кабинет № 111 – ИСПДн «Приемная граждан»;

- кабинет № 403 – ИСПДн «Административная комиссия»;

- кабинеты № 407, 409 и 416 – ИСПДн «Опека»;

2. Требования к служебным помещениям

В целях обеспечения соблюдения требований к ограничению доступа в служебные помещения Организации обеспечивается:

- использование служебных помещений строго по назначению;

- наличие на входах в служебные помещения дверей, оборудованных запорными устройствами, уплотняющими прокладками;

- содержание дверей служебных помещений в нерабочее время в закрытом на запорное устройство состоянии;

- остекление окон в здании Организации, содержание их в нерабочее время в закрытом состоянии;

- доступ в служебные помещения только работников Организации.

Доступ в служебные помещения работников допускается только для выполнения поручений и получения информации, необходимой для исполнения служебных обязанностей в соответствии с должностной инструкцией, иных лиц – в случаях, установленных законодательством.

В каждом служебном помещении назначается лицо, ответственное за соблюдение требований к ограничению доступа в служебное помещение.

Работникам запрещается передавать ключи от служебным помещений третьим лицам.

В нерабочее время доступ в помещения осуществляется по заранее согласованной заявке с ответственным за обработку персональных данных в Организации.

В случае возникновения нештатных ситуаций доступ в помещение осуществляется в присутствии сотрудника охраны, при этом в журнале приема-сдачи под охрану помещений делается соответствующая запись.

3. Контроль за соблюдением требований к доступу работников в служебные помещения

Текущий контроль за содержанием служебных помещений осуществляет ответственный за защиту персональных данных Организации.

Работники, обнаружившие попытку проникновения посторонних лиц в служебное помещение, немедленно сообщают об этом ответственному за защиту персональных данных Организации.

Руководитель аппарата управы района  И.Н. Шеина

Приложение № 13
к приказу управы Центрального
района городского округа
город Воронеж

от «30» 11.2016 № 63

ИНСТРУКЦИЯ
администратору безопасности ИСПДн
управы Центрального района городского округа город Воронеж

ОБЩИЕ ПОЛОЖЕНИЯ

Настоящая инструкция определяет основные функции и порядок работы администратора безопасности в технологическом процессе обработки конфиденциальной информации на объекте информатизации ИСПДн управы Центрального района городского округа город Воронеж с применением комплекса средств защиты информации (СЗИ) от несанкционированного доступа (НСД) Dallas Lock и VIP NET CUSTOM.

В процессе выполнения своих служебных обязанностей администратор безопасности должен выполнять требования нормативных документов по защите информации и требования эксплуатационной документации на комплекс Dallas Lock и VIP NET CUSTOM.

1. ФУНКЦИИ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ

1.1. Администратор безопасности обязан выполнять начальную установку и настройку комплекса СЗИ НСД на ПЭВМ объекта информатизации.

1.2. Администратор обязан вести учет электронных идентификаторов комплексов СЗИ НСД, выполнять действия по их регистрации на ПЭВМ,

организовывать их выдачу пользователям и периодически контролировать их наличие.

1.3. Администратор безопасности обязан проводить работы по генерации и регулярной смене паролей пользователей.

1.4. Администратор безопасности обязан выполнять действия по настройке комплексов СЗИ НСД на ПЭВМ объекта информатизации в соответствии с утвержденными правилами разграничения доступа (матрицей доступа).

1.5. Администратор безопасности обязан осуществлять оперативный контроль над функционированием комплекса СЗИ НСД на ПЭВМ объекта информатизации, проводить его периодическое тестирование и осуществлять контроль целостности резервных копий программного обеспечения комплекса на носителях.

1.6. Администратор безопасности обязан проводить проверки целостности программного обеспечения.

1.7. Администратор безопасности обязан осуществлять постоянный контроль над соблюдением операторами (пользователями) технологии обработки конфиденциальной информации, анализировать содержимое регистрационных журналов, формируемых комплексами СЗИ НСД и принимать конкретные меры по выявленным нарушениям.

1.8. Администратор безопасности обязан организовывать и контролировать проведение работ по ремонту, наладке и сервисному обслуживанию ПЭВМ и вспомогательных технических средств объекта информатизации.

1.9. Администратор безопасности обязан контролировать сохранность и целостность эталонных копий программного обеспечения.

1.10. Администратор безопасности обязан оказывать методическую и консультационную помощь операторам (пользователям) объекта информатизации в процессе эксплуатации комплексов СЗИ НСД.

2. УСТАНОВКА И НАСТРОЙКА КОМПЛЕКСА СЗИ НСД

2.1. Установка (повторная установка) комплексов СЗИ НСД выполняется в следующих ситуациях:

- на этапе ввода в действие объекта информатизации;
- в случае выхода из строя накопителей с конфиденциальной информацией;
- в случае возникновения сбойных и аварийных ситуаций, повлекших нарушения в работе программного обеспечения (ПО) ПЭВМ;
- в случае ввода новых ПЭВМ в состав объекта информатизации.

2.2. Установка комплекса СЗИ НСД на ПЭВМ объекта информатизации должна выполняться администратором безопасности в строгом соответствии с инструкциями, приведенными в эксплуатационной документации.

2.3. Установка ПО комплекса СЗИ НСД должна производиться с эталонных носителей (CD-дисков). Перед установкой комплекса ПО ПЭВМ должно быть проверено на отсутствие вирусного заражения.

2.4. Регистрация электронных идентификаторов пользователей и установка правил разграничения доступа производится в соответствии с утвержденными правилами разграничения доступа (матрицей доступа). Регистрация дополнительных (не указанных) в матрице доступа пользователей запрещена.

3. СОПРОВОЖДЕНИЕ СЗИ НСД В ПРОЦЕССЕ ЭКСПЛУАТАЦИИ

3.1 *Ведение служебной информации СЗИ НСД*

3.1.1 *Регистрация пользователей*

3.1.1.1. Действия по регистрации пользователей выполняются администратором безопасности на основании оформленных установленным

порядком приказов и распоряжений о допуске пользователей к обработке конфиденциальной информации.

3.1.1.2. В соответствии с установленными уровнями полномочий операторов (пользователей) и эксплуатационной документацией на комплекс СЗИ НСД администратор безопасности разрабатывает правила разграничения доступа (ПРД) и оформляет матрицу доступа.

3.1.1.3. На основании утвержденной матрицы доступа администратор безопасности, в соответствии с эксплуатационной документацией выполняет действия по настройке системы защиты ПЭВМ от НСД.

3.1.1.4. В процессе регистрации пользователей и настройки системы защиты администратор безопасности должен соблюдать следующие правила:

- все информационные ресурсы, к которым разрешен доступ пользователя (логические диски, каталоги и файлы) должны быть явно указаны;
- каталогам, в которых планируется размещать конфиденциальную информацию должны быть заранее присвоены соответствующие метки конфиденциальности;
- все запускаемые программы и подгружаемые модули должны быть явно указаны и включены в список контроля при запуске;
- должна быть обеспечена регистрация в системном журнале операций чтения, записи и удаления;
- журнал регистрации должен вестись для всех пользователей;
- должен быть активизирован режим ограничения времени действия пароля по количеству попыток неправильного ввода;
- должен быть активизирован режим полного удаления файлов;

- должен быть активизирован режим очистки освобождаемой памяти;
- доступ к портам ввода-вывода должен быть максимально ограничен.

3.1.1.5. Регистрация электронных идентификаторов пользователей, установка правил разграничения доступа выполняются средствами СЗИ НСД.

3.1.1.6. Контроль целостности файлов системы защиты обеспечивается средствами СЗИ НСД.

3.1.1.7. Контроль файловой системы, в том числе обнаружение изменения и создания новых файлов обеспечивается средствами программы контроля целостности файловой системы СЗИ НСД.

3.1.1.8. По окончании работ по регистрации пользователей администратор безопасности выполняет проверки функционирования общесистемной программной среды каждого зарегистрированного пользователя, тестирует работоспособность комплекса СЗИ НСД, и корректность реализации ПРД.

3.1.1.9. После выдачи идентификаторов каждому пользователю администратор (возможно совместно с пользователем) осуществляет генерацию пароля и контролирует установку пароля пользователем.

3.1.2 *Генерация и смена паролей*

3.1.2.1. Действия по генерации и смене паролей пользователей должны организовываться администратором безопасности.

3.1.2.2. Для организации работ по смене паролей администратор безопасности устанавливает ограничения на время действия пароля.

3.1.2.3. Процедура генерации паролей должна исключать задание в качестве паролей комбинаций критичных с точки зрения их подбора.

3.1.2.4. Смена паролей выполняется, в соответствии с эксплуатационной документацией на комплекс СЗИ НСД.

3.1.2.5. Установленные (новые) пароли администратор безопасности должен лично сообщать каждому конкретному пользователю. Администратор безопасности несет ответственность за разглашение личных паролей пользователей.

3.1.3 *Сопровождение ПРД*

3.1.3.1. Администратор безопасности обеспечивает реализацию разрешительной системы доступа в виде наборов правил разграничения доступа к техническим, программным средствам и информационным ресурсам формируемых для каждого регистрируемого пользователя.

3.1.3.2. Распределение и изменение прав доступа пользователей к конкретным программам и информационным ресурсам должно осуществляться на основании Заявок.

3.1.3.3. Правила разграничения доступа разрабатываются в соответствии с требованиями разрешительной системы доступа на основании заявок на доступ пользователей и документально оформляются в виде матрицы доступа или в виде дополнений и изменений матрицы доступа и физически реализуются настройками подсистемы разграничения доступа к объектам файловой системы.

3.1.3.4. Заявки на доступ пользователей к техническим средствам объекта должны содержать перечень (список) программ и информационных ресурсов, доступ к которым должен быть предоставлен каждому конкретному пользователю с указанием дисков и каталогов, на которых размещены данные ресурсы.

3.2 *Оперативный контроль над функционированием СЗИ НСД*

3.2.1. Администратор безопасности несет ответственность за нормальное функционирование комплекса СЗИ НСД на ПЭВМ объекта информатизации.

3.2.2. Администратор безопасности должен осуществлять периодическое тестирование работоспособности комплекса СЗИ НСД и корректности реализации ПРД.

3.2.3. В случае, когда средства комплекса СЗИ НСД отказывают в доступе легальным пользователям, администратор безопасности должен анализировать причины отказа в доступе и предпринимать оперативные действия по выявлению возможных нарушений.

3.2.4. Администратор безопасности должен предпринимать оперативные действия в случае возникновения внештатных ситуаций при работе ПЭВМ, анализировать причины их возникновения и предпринимать необходимые меры по восстановлению работоспособности комплекса СЗИ НСД и программного обеспечения.

3.2.5. Администратор безопасности должен постоянно контролировать уровень защищенности информации от НСД и, в случае выявления возможных каналов утечки информации за счет НСД, предпринимать оперативные меры по их устранению за счет изменения параметров настройки подсистемы разграничения доступа комплекса СЗИ НСД.

3.3 *Контроль соответствия программной среды эталону*

3.3.1. Контроль соответствия общесистемной программной среды эталону осуществляется администратором безопасности с использованием средств комплекса. Для этого администратор средствами администрирования формирует для каждого зарегистрированного пользователя списки файлов, входящих в состав общесистемного программного обеспечения, целостность которых контролируется и включает режим проверки целостности «до запуска» ОС.

3.3.2. Все исполняемые модули (файлы, содержащие исполняемый или интерпретируемый программный код), входящие в состав общесистемной программной среды доступ к которым разрешен конкретному пользователю, должны быть включены в список контроля целостности.

3.3.3. В случае выявления фактов нарушения целостности компонентов, входящих в состав общесистемного программного обеспечения, администратором безопасности должны предприниматься действия по анализу причин таких нарушений и действия по восстановлению данных компонент с эталонных копий.

3.3.4. Администратор безопасности должен обеспечивать контроль над сохранностью эталонных копий ПО и периодически проверять состояние учтенных носителей, на которых оно расположено.

3.4 *Приемка и ввод в эксплуатацию программных средств*

3.4.1. Администратор безопасности организует и контролирует выполнение работ по установке новых программных средств, включаемых в состав ИСПДн.

3.4.2. Перед установкой дистрибутивные носители с новыми программными средствами, вводимыми в состав объекта информатизации, должны быть соответствующим образом проверены.

3.4.3. Установка новых программных средств допускается только с проверенных носителей.

3.4.4. Перед установкой новых программных средств ПЭВМ должна быть физически отключена от ИСПДн. Если физическое отключение ПЭВМ не возможно (в силу специфики устанавливаемого ПО), выполнение работ по установке новых программных средств допускается только после полного прекращения обработки конфиденциальной информации в ИСПДн.

3.4.5. После выполнения работ по установке новых программных средств администратор безопасности проверяет их работоспособность и

средствами администрирования комплекса СЗИ НСД выполняет необходимые действия по их настройке. По результатам выполненных работ оформляется акт приемки нового программного обеспечения и утверждаются дополнения и изменения матрицы доступа.

3.4.6. Допуск пользователей к работе на ПЭВМ, на которых проводились работы по установке нового программного обеспечения, разрешается только после утверждения акта приемки и матрицы доступа.

3.5 *Контроль за ходом технологического процесса обработки информации*

3.5.1. Контроль хода технологического процесса обработки информации администратор безопасности осуществляет путем регистрации и анализа действий операторов (пользователей) по системному журналу.

3.5.2. Обработка и анализ системных журналов должны осуществляться регулярно, но не реже чем один раз в неделю.

3.5.3. В случае выявления нарушений администратор безопасности проводит мероприятия по выявлению виновников и причин нарушения. Результаты расследования доводятся до сведения руководства.

3.6 *Оказание методической и консультационной помощи пользователям*

3.6.1. Администратор безопасности организует и проводит инструктаж пользователей правилам применения и эксплуатации комплексов СЗИ НСД и периодически контролирует их знания.

3.6.2. Администратор безопасности должен оказывать методическую и консультационную помощь пользователям при применении и эксплуатации комплексов СЗИ НСД.

Руководитель аппарата управы района  И.Н. Шеина

Приложение № 14
к приказу управы Центрального
района городского округа
город Воронеж

от «30» 11.2016 № 63

ИНСТРУКЦИЯ
по организации антивирусной защиты в ИСПДн управы Центрального района городского округа город Воронеж

1. Общие положения

Компьютерный вирус является разрушающей программной закладкой и характеризуется значительным деструктивным потенциалом для программ, данных и любой информации, хранящейся на компьютерах и магнитных носителях. Особую опасность представляет то обстоятельство, что компьютерные вирусы могут скрытно и постепенно уничтожать, либо мгновенно разрушать хранящуюся в компьютере и на носителях информацию, при этом также могут пострадать аппаратные средства.

Основными путями вирусного вторжения являются неквалифицированное обращение пользователей с компьютерной техникой при использовании ими зараженных носителей и программ, либо целенаправленное спланированное воздействие извне с использованием компьютерных вирусов. При любых обстоятельствах это затрагивает вопросы защиты информации и интересы управы Центрального района городского округа город Воронеж.

2. Порядок, обеспечивающий безопасную работу на компьютере и с носителями информации

1. Вновь поступающее программное обеспечение должно быть подвергнуто входному контролю – проверке на отсутствие вирусов и проверке соответствия длины и контрольных сумм, если таковые указаны в

сопроводительных документах, полученным длинам и контрольным суммам.

2. Допуск сотрудников к самостоятельной работе на компьютерах и с внешними носителями осуществляется только после овладения ими навыками работы с компьютером, антивирусными пакетами программ.

3. На компьютерах может использоваться программное и аппаратное обеспечение, необходимое только для выполнения служебной деятельности. Запрещается использовать на компьютерах программные и аппаратные средства, не согласованные с целями обработки информации ограниченного доступа.

4. В обязательном порядке должен быть установлен и активирован пакет антивирусных программ. Ответственность за это несет администратор безопасности ИСПДн. Установка средств антивирусного контроля (в том числе настройка параметров средств антивирусного контроля) осуществляется в соответствии с руководствами по применению конкретных антивирусных средств. Антивирусные средства устанавливаются при вводе в эксплуатацию ИСПДн или при их плановой замене.

5. Периодически пользователь проверяет его дисковое пространство с использованием антивирусного пакета программ на возможное наличие компьютерного вируса.

6. Пользователь (в случае необходимости совместно с администратором безопасности) обязан проводить антивирусный контроль любой электронной информации (текстовые файлы любых форматов, файлы данных, исполняемые файлы, архивируемые/разархивируемые файлы и т.д.), получаемой на съемных носителях (магнитных дисках, оптических носителях, Flash - память и т.п.).

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

– приостановить работу;

– немедленно поставить в известность о факте обнаружения зараженных вирусом файлов администратора безопасности ИСПДн, владельца

зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;

– совместно с администратором безопасности провести анализ необходимости дальнейшего использования зараженных вирусом файлов;

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

Все факты обнаружения зараженных вирусом файлов администратор безопасности заносит в «Журнал регистрации работ по антивирусной защите и выявления вирусного заражения в ИСПДн», где отображается тип зараженного файла, характер содержащейся в файле информации, название вируса, тип вируса и выполненные антивирусные мероприятия.

3. Ответственность

Ответственность за поддержание установленного порядка проведения антивирусного контроля возлагается на администратора безопасности ИСПДн.

Пользователь и администратор безопасности несут ответственность за качество и своевременность выполнения задач и функций, возложенных на них в соответствии с настоящей Инструкцией.

Руководитель аппарата управы района  И.Н. Шеина

Приложение № 15
к приказу управы Центрального
района городского округа
город Воронеж

от «30» 11.2016 № 63

ИНСТРУКЦИЯ
о порядке технического обслуживания и ремонта технических средств ИСПДн управы Центрального района городского округа город Воронеж

1. Общие положения

1.1. Настоящая инструкция определяет правила работ по техническому обслуживанию, ремонту, модернизации технических средств, входящих в состав ИСПДн, защищенных от несанкционированного доступа (НСД) и предназначенных для обработки и хранения персональных данных.

1.2. Данные работы проводятся только с разрешения руководителя управы Центрального района городского округа город Воронеж после согласования со специалистом по защите информации ИСПДн.

2. Порядок проведения работ по техническому обслуживанию, ремонту, модернизации

2.1. В случае, когда необходимо провести работы по техническому обслуживанию (ремонту, модернизации) технических средств, входящих в состав ИСПДн, специалист по защите информации ИСПДн представляет служебную записку, в которой:

-указывает название (ПЭВМ, технического средства, системы), техническое обслуживание (ремонт, модернизацию) которой необходимо провести и с какой целью;

-обосновывает необходимость технического обслуживания

(модернизации);

-указывает планируемые место и сроки работ, режим их проведения;

-перечисляет меры безопасности, которые будут реализованы при техническом обслуживании (ремонте, модернизации) с целью недопущения доступа к персональным данным посторонних лиц.

2.2. В случае если для проведения работ необходимо привлекать лиц, не имеющих постоянного допуска к работе на ПЭВМ или в помещение, составляется список сотрудников, который согласовывается с руководителем.

Запрещается выносить технические средства и системы (ТСС), входящие в состав ИСПДн, с территории здания без согласования со специалистом по защите информации ИСПДн и разрешения руководителя.

2.3. При вскрытии печатей и пломб на технических средствах (системах), последующее опечатывание производится комиссионно в присутствии специалиста по защите информации, о чём составляется акт.

В акте указывается:

- номер (название) помещения, в котором проводились работы,

- дата и время начала и окончания работ,

- лица, присутствовавшие при вскрытии и обслуживании (ремонте, модернизации),

- наличие, целостность и места размещения печатей (пломб, специальных защитных знаков) до вскрытия ПЭВМ (технического средства, системы),

- установленные неисправности,

- виды и результаты проведенных работ,

- замененные или отремонтированные узлы (детали), наличие на этих узлах специальных защитных знаков,

- какими печатями (пломбами и т.д.) и в каких местах ПЭВМ (устройство) опечатано по окончании работ,

- необходимость проведения дополнительной специальной проверки и

специальных исследований (сертификации) ПЭВМ (технического средства, системы) или её отдельных узлов,

- иная необходимая для дальнейшей работы и обеспечения безопасности информация.

2.4. Если для ремонта (модернизации) ИСПДн (другого технического средства, системы, узла ПЭВМ в составе ИСПДн) необходимо направить в специализированную организацию, то комиссией составляется заключение.

2.5. Перед отправкой ПЭВМ (другого технического средства, системы, узла ПЭВМ) администратор безопасности информации обязан гарантированно удалить персональные данные с жесткого диска и иных устройств памяти ПЭВМ (другого технического средства, системы) сертифицированными средствами, о чем он составляет акт. По запросу из специализированной организации копия акта передаётся и ей.

2.6. В случае если не имеется возможности гарантировано удалить персональные данные с жесткого диска и иных устройств памяти ПЭВМ (другого технического средства, системы) сертифицированными средствами, эти устройства опечатываются и хранятся в ИСПДн с соблюдением требований, предъявляемым к хранению персональных данных.

2.7. Ремонт и замена жесткого диска производится в присутствии администратора безопасности информации. При диагностике и ремонте жесткого диска должны быть реализованы меры безопасности, исключающие несанкционированный доступ к хранящимся на нём данным.

Руководитель аппарата управы района И.Н. Шеина

Приложение № 16
к приказу управы Центрального
района городского округа
город Воронеж

от «30» 11.2016 № 63

ИНСТРУКЦИЯ
по организации парольной защиты в ИСПДн управы Центрального района городского округа город Воронеж

Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) при использовании сервера с ограниченным доступом в ИСПДн «Бухгалтерия», а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

1. Порядок парольной защиты

1. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей в ИСПДн и контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями возлагается на специалиста по защите информации.

2. Личные пароли должны генерироваться и распределяться централизованно с учетом следующих требований:

- длина пароля должна быть не менее 6 символов;

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

- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 3 позициях;

- личный пароль пользователь не имеет права сообщать никому.

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

3. Формирование личных паролей пользователей осуществляется централизованно. Ответственность за правильность их формирования и распределения возлагается на уполномоченного сотрудника - специалиста по защите информации. Для генерации «стойких» значений паролей могут применяться специальные программные средства. Система централизованной генерации и распределения паролей должна исключать возможность ознакомления (самих уполномоченных сотрудников, а также руководителей подразделений) с паролями других сотрудников подразделений.

4. Списки паролей в опечатанном виде хранятся в сейфе.

5. Полная плановая смена паролей пользователей должна проводиться регулярно.

6. Внеплановая смена личного пароля или удаление учетной записи пользователя ИСПДн в случае прекращения его полномочий (увольнение, переход на другую работу и т.п.) должна производиться по представлению специалиста по защите информации уполномоченными сотрудниками немедленно после окончания последнего сеанса работы данного пользователя с системой.

7. В случае компрометации личного пароля пользователя ИСПДн должны быть немедленно предприняты меры в соответствии с п.6 настоящей Инструкции.

8. Хранение сотрудником (исполнителем) значений своих паролей на материальном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у руководителя подразделения в опечатанном конверте или пенале (возможно вместе с персональным носителем информации и идентификатором).

9. Повседневный контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены и использования в подразделениях возлагается на специалиста по защите информации.

2. Ответственность

Пользователь и специалист по защите информации несут ответственность за качество и своевременность выполнения задач и функций, возложенных на них в соответствии с настоящей Инструкцией.

Руководитель аппарата управы района  И.Н. Шеина

Приложение № 17
к приказу управы Центрального
района городского округа
город Воронеж

от «30» 11.2016 № 63

ИНСТРУКЦИЯ
по порядку учета и хранению съемных носителей персональных данных в управе Центрального района городского округа город Воронеж

1. Общие положения

1.1. Настоящая Инструкция разработана в соответствии с Федеральным законом № 149-ФЗ от 27.07.2006 «Об информации, информационных технологиях и о защите информации», ГОСТ Р ИСО/МЭК 17799-2005 «Практические правила управления информационной безопасностью» и другими нормативными правовыми актами, и устанавливает порядок использования носителей информации.

1.2. Действие настоящей Инструкции распространяется на сотрудников управы Центрального района городского округа город Воронеж, подрядчиков и третью сторону.

2. Основные термины, сокращения и определения

2.1. Администратор ИС – технический специалист, обеспечивает ввод в эксплуатацию, поддержку и последующий вывод из эксплуатации ПО и оборудования вычислительной техники.

2.2.АРМ – автоматизированное рабочее место пользователя (ПК с прикладным ПО) для выполнения определенной производственной задачи.

2.3.ИБ – информационная безопасность – комплекс организационно-технических мероприятий, обеспечивающих конфиденциальность, целостность и доступность информации.

2.4. ИС – информационная система – система, обеспечивающая хранение, обработку, преобразование и передачу информации с использованием компьютерной и другой техники.

2.5. Носитель информации – любой материальный объект, используемый для хранения и передачи электронной информации.

2.6. Паспорт ПК – документ, содержащий полный перечень оборудования и программного обеспечения АРМ.

2.7. ПК – персональный компьютер.

2.8. ПО – программное обеспечение вычислительной техники.

2.9. ПО вредоносное – ПО или изменения в ПО, приводящие к нарушению конфиденциальности, целостности и доступности критичной информации.

2.10. ПО коммерческое – ПО сторонних производителей (правообладателей). Предоставляется в пользование на возмездной (платной) основе.

2.11. Пользователь – работник Организации, использующий мобильные устройства и носители информации для выполнения своих служебных обязанностей.

3. Порядок использования носителей информации

3.1. Под использованием носителей информации в ИС управы Центрального района городского округа город Воронеж понимается их подключение к инфраструктуре ИС с целью обработки, приема/передачи информации между ИС и носителями информации.

3.2. В ИС допускается использование только учтенных носителей информации, которые являются собственностью управы Центрального района городского округа город Воронеж и подвергаются регулярной ревизии и контролю.

3.3. К предоставленным органам исполнительной власти носителям персональных данных предъявляются те же требования ИБ, что и для стационарных АРМ (целесообразность дополнительных мер обеспечения ИБ определяется администраторами ИС).

3.4. Носители персональных данных предоставляются сотрудникам управы Центрального района городского округа город Воронеж по инициативе руководителей структурных подразделений в случаях:

- необходимости выполнения вновь принятым работником своих должностных обязанностей;
- возникновения у сотрудника управы Центрального района городского округа город Воронеж производственной необходимости.

3.5.Порядок учета, хранения и обращения со съемными носителями персональных данных, твердыми копиями и их утилизации.

- все находящиеся на хранении и в обращении съемные носители с персональными данными в органе исполнительной власти подлежат учёту;

- каждый съемный носитель с записанными на нем персональными данными должен иметь этикетку, на которой указывается его уникальный учетный номер;

- учет и выдачу съемных носителей персональных данных осуществляют сотрудники структурных подразделений, на которых возложены функции хранения носителей персональных данных. Факт выдачи съемного носителя фиксируется в журнале учета съемных носителей конфиденциальной информации;

- сотрудники управы Центрального района городского округа город Воронеж получают учтенный съемный носитель от уполномоченного сотрудника для выполнения работ на конкретный срок. При получении делаются соответствующие записи в журнале учета. По окончании работ пользователь сдает съемный носитель для хранения уполномоченному сотруднику, о чем делается соответствующая запись в журнале учета.

3.6.При использовании сотрудниками носителей конфиденциальной информации необходимо:

- соблюдать требования настоящей Инструкции;

- использовать носители информации исключительно для выполнения своих служебных обязанностей;

- ставить в известность ответственного за защиту персональных данных о любых фактах нарушения требований настоящей Инструкции;

- бережно относится к носителям персональных данных;

- обеспечивать физическую безопасность носителей информации всеми разумными способами;

- извещать ответственного за защиту персональных данных о фактах утраты (кражи) носителей персональных данных.

3.7.При использовании носителей персональных данных запрещено:

- использовать носители персональных данных в личных целях;

- передавать носители персональных данных лицам, не имеющим доступ к обработке персональных данных в данной ИС;

- хранить съемные носители с персональными данными вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;

- выносить съемные носители с персональными данными из служебных помещений для работы с ними на дому и т. д.

3.8.Любое взаимодействие (обработка, прием/передача информации), инициированное сотрудником управы Центрального района городского округа город Воронеж между ИС и неучтенными (личными) носителями информации, рассматривается как несанкционированное (за исключением случаев оговоренных с ответственным за защиту персональных данных заранее). Ответственный за защиту персональных данных оставляет за собой право блокировать или ограничивать использование носителей информации.

3.9.Информация об использовании сотрудником управы Центрального района городского округа город Воронеж носителей информации в ИС протоколируется и, при необходимости, может быть предоставлена руководителю управы Центрального района городского округа город Воронеж.

3.10. В случае выявления фактов несанкционированного и/или нецелевого использовании носителей персональных данных инициализируется служебная проверка, проводимая комиссией, состав которой определяется руководителем управы Центрального района городского округа город Воронеж.

3.11. По факту выясненных обстоятельств составляется акт расследования инцидента и передается руководителю управы Центрального района городского округа город Воронеж для принятия мер согласно локальным правовым актам управы Центрального района городского округа город Воронеж и действующему законодательству.

3.12. Информация, хранящаяся на носителях персональных данных, подлежит обязательной проверке на отсутствие вредоносного ПО.

3.13. При отправке или передаче персональных данных адресатам на съемные носители записываются только предназначенные адресатам данные. Отправка персональных данных адресатам на съемных носителях осуществляется в порядке, установленном для документов для служебного пользования.

3.14. Вынос съемных носителей персональных данных для непосредственной передачи адресату осуществляется только с письменного разрешения руководителя структурного подразделения.

3.15. В случае утраты или уничтожения съемных носителей персональных данных либо разглашении содержащихся в них сведений немедленно ставится в известность начальник соответствующего структурного подразделения. На утраченные носители составляется акт.

Соответствующие отметки вносятся в журналы учета съемных носителей персональных данных.

3.16. Съемные носители персональных данных, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей с конфиденциальной информацией осуществляется «уполномоченной комиссией». По результатам уничтожения носителей составляется акт по прилагаемой форме.

3.17. В случае увольнения или перевода работника в другое структурное подразделение, предоставленные носители персональных данных изымаются.

4. Ответственность

Работники, нарушившие требования настоящей Инструкции, несут ответственность в соответствии с действующим законодательством и локальными правовым актами управы Центрального района городского округа город Воронеж.

Руководитель аппарата управы района  И.Н. Шеина

Приложение

УТВЕРЖДАЮ
Руководитель управы Центрального района
городского округа город Воронеж

_____ А.А. Попов

«___» _____2016 г.

АКТ
уничтожения съемных носителей персональных данных

Комиссия, наделенная полномочиями приказом _____ от №_____ в составе:

_____

_____
(должности, ФИО)

провела отбор съемных носителей конфиденциальной информации (персональных данных), не подлежащих дальнейшему хранению:

№ п/п	Дата	Учетный номер съемного носителя	Примечание

Всего съемных носителей_____(цифрами и прописью)

На съемных носителях уничтожена конфиденциальная информация путем стирания ее на устройстве гарантированного уничтожения информации (механического уничтожения, сжигания и т.п.).

Перечисленные съемные носители уничтожены путем

_____
(разрезания, демонтажа и т.п.)

_____

Председатель комиссии

Члены комиссии

Руководитель аппарата управы района И.Н. Шеина

Приложение № 18
к приказу управы Центрального
района городского округа
город Воронеж

от «30» 11.2016 № 63

ИНСТРУКЦИЯ
пользователю автоматизированных систем ИСПДн управы Центрального района городского округа город Воронеж

Допуск пользователей для работы в ИСПДн, осуществляется в соответствии с приказом руководителя управы Центрального района городского округа город Воронеж и разрешительной системой доступа.

Пользователь имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам компьютера. При этом для хранения файлов, содержащих конфиденциальную информацию, разрешается использовать только специально выделенные каталоги на несъемных носителях информации, а также соответствующим образом учтенные съёмные носители информации.

Присвоение пользователю полномочий доступа к ресурсам компьютера, состав необходимого системного и прикладного программного обеспечения для решения поставленных задач и определение возможного времени работы пользователя в ИСПДн, осуществляется при первичной регистрации пользователя специалистом защиты информации.

Пользователь отвечает за правильность включения и выключения технических средств и систем, входа в систему и все действия при работе в ИСПДн.

Вход в систему может осуществляться по разным моделям:

Модель № 1 - вход пользователя в систему предусматривающую наличие пароля осуществляется на основе ввода имени, присвоенного при

первичной регистрации и ввода личного пароля. Требования к парольной защите определяется инструкцией по парольной защите. (Модель №1)

Модель № 2 - вход пользователя в систему осуществляется на основе персонального средства (в форме – фактора USB-ключа) аутентификации и защищённого хранения данных, аппаратно поддерживающего работу с цифровыми сертификатами и электронной цифровой подписью (ЭЦП) (далее - eToken).

В целях предотвращения несанкционированного доступа посторонних лиц к ресурсам пользователя осуществляется периодическая (раз в месяц) замена пароля постоянного пользователя. Замена личного пароля осуществляется пользователем самостоятельно. (Модель №1)

При работе со съемными носителями информации пользователь каждый раз перед началом работы обязан проверить их на наличие вирусов с использованием установленных антивирусных программ, в соответствии с Инструкцией по антивирусной защите.

Пользователь обязан:

- знать и строго выполнять установленные правила и обязанности по доступу к защищаемым ресурсам и соблюдению принятого режима информационной безопасности;
- обеспечить правильность вводимых данных;
- своевременно сообщать специалисту по защите информации об изменениях статуса пользователя;
- незамедлительно сообщить специалисту по защите информации факты выявления инцидентов с доступом к конфиденциальной информации.

В процессе работы пользователю запрещается:

• использовать для постоянного хранения и обработки конфиденциальной информации каталоги несъемных носителей информации, за исключением выделенных каталогов;

• осуществлять попытки несанкционированного доступа к ресурсам операционной системы;

• в рамках выделенных ресурсов и полномочий доступа к ним обрабатывать информацию с уровнем конфиденциальности, выше заявленного при регистрации;

• пытаться подменять функции администратора по перераспределению времени работы и полномочий доступа к ресурсам компьютера;

• покидать помещение с незаблокированной учетной записью$

•отключать установленные средства защиты информации;

• использовать машинные носители без их предварительной проверки антивирусными средствами;

• устанавливать программное обеспечение;

• менять параметры конфигурации ранее установленных программных средств;

• использовать пароль, предоставленный специалистом по защите информации для первоначального доступа в качестве постоянного рабочего пароля (Модель №1);

• использование различными пользователями одной и той же учетной записи, даже если пользователи имеют одинаковые полномочия по доступу (Модель №1);

• использование различными пользователями одного и того же eToken, даже если пользователи имеют одинаковые полномочия по доступу (Модель №2);

•

• запрещается передавать в любом виде или сообщать идентификаторы и пароли для доступа другим лицам, в том числе и своим руководителям (Модель №1);

•запрещается передавать eToken другим лицам, в том числе и своим руководителям(Модель №2);

• хранение пароля на любых твердых носителях, позволяющих другим лицам получить информацию о пароле (Модель №1);

• использовать информацию, полученную в результате доступа к БД, в целях, не предусмотренных его функциональными обязанностями.

Ответственность за сохранность и правильное использование информации, ставшей известной в процессе обработки конфиденциальной информации несет пользователь.

Возможность получения технического доступа к конфиденциальной информации не дает права пользователям обработки такой информации, если им не предоставлены права доступа к этой информации. Такие действия рассматриваются как попытки несанкционированного доступа.

При выявлении инцидентов с доступом к конфиденциальной информации доступ пользователей к ней может быть ограничен до окончания расследования инцидента, о чем пользователь уведомляется в кратчайшие сроки. По результатам служебного расследования нарушитель может быть лишен прав доступа к конфиденциальной информации, материалы расследования могут быть направлены в соответствующие службы для привлечения нарушителя к ответственности.

Пользователь несет ответственность за все действия, совершенные от имени его учетной записи, если не доказан факт несанкционированного использования этой учетной записи.

В моделе № 1 личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями

автоматизированной системы самостоятельно с учетом следующих требований:

- длина пароля должна быть не менее 6 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, номера телефонов и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 3 позициях;
- личный пароль пользователь не имеет права сообщать никому.

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

Для генерации «стойких» значений паролей могут применяться специальные программные средства.

При наличии технологической необходимости использования eToken, имен и паролей некоторых сотрудников (исполнителей) в их отсутствие (например, в случае возникновении нештатных ситуаций, форс-мажорных обстоятельств и т.п.):

- в Модели № 1 такие сотрудники обязаны сразу же после смены своих паролей их новые значения (вместе с именами своих учетных записей) в запечатанном конверте или опечатанном пенале передавать на хранение специалисту по защите информации;

- в Модели № 2 такие сотрудники обязаны в запечатанном конверте или опечатанном пенале передавать eToken на хранение специалисту по защите информации.

Опечатанные конверты должны храниться в сейфе.

Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в месяц.

Внеплановая смена личного пароля или удаление учетной записи, а так же инициализация eToken пользователя автоматизированной системы в случае прекращения его полномочий должна производиться специалистом по защите информации немедленно.

Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий администраторов и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой.

В случае компрометации личного пароля пользователя автоматизированной системы должны быть немедленно предприняты меры по внеплановой смене паролей.

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

При нарушениях пользователем правил, связанных с информационной безопасностью, он несет ответственность, установленную действующим законодательством Российской Федерации.

Руководитель аппарата управы района  И.Н. Шеина

Приложение № 19
к приказу управы Центрального
района городского округа
город Воронеж

от «30» 11.2016 № 63

Инструкция
о порядке действий при возникновении чрезвычайных ситуаций в ИСПДн
управы Центрального района городского округа город Воронеж

1. Общие положения

Настоящая Инструкция определяет возможные аварийные ситуации, связанные с функционированием ИСПДн, меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн после возникновений аварийных ситуаций.

Задачей данной Инструкции является:

- определение мер защиты от прерывания работоспособности;
- определение действий восстановления в случае прерывания.

Действие настоящей Инструкции распространяется на всех пользователей, имеющих доступ к ресурсам ИСПДн, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

- системы жизнеобеспечения;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

Пересмотр настоящего документа осуществляется по мере необходимости.

В настоящем документе под аварийной ситуацией понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн. Аварийная ситуация

становится возможной в результате реализации одной из угроз, приведенных ниже:

– технологические угрозы (пожар в здании, повреждение водой, взрыв, химический выброс в атмосферу);

– внешние угрозы (массовые беспорядки, сбои общественного транспорта, эпидемия, массовое отравление персонала);

– стихийные бедствия (удар молнии, сильный снегопад, сильные морозы, просадка грунта с частичным обрушением здания, затопление водой в период паводка, наводнение, вызванное проливным дождем, торнадо);

– телекоммуникационные и информационно-технические угрозы (сбой системы кондиционирования, сбой ИТ – систем);

– угроза, связанная с человеческим фактором (ошибка персонала, имеющего доступ к серверной, нарушение конфиденциальности, целостности и доступности конфиденциальной информации);

– угрозы, связанные с внешними поставщиками (отключение электроэнергии, сбой в работе интернет-провайдера, физический разрыв внешних каналов связи).

– Все действия в процессе реагирования на аварийные ситуации, возникающие в ИСПДн, должны документироваться администратором безопасности.

В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование сотрудники (Администратор и пользователи ИСПДн) предпринимают меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с вышестоящим руководством. По необходимости, иерархия может быть нарушена, с целью получения высококвалифицированной консультации в кратчайшие сроки.

2. Уровни реагирования на инцидент

При реагировании на инцидент, важно, чтобы пользователь правильно классифицировал критичность инцидента. Критичность оценивается на основе следующей классификации:

1) Незначительный инцидент. Незначительный инцидент определяется как локальное событие с ограниченным разрушением, которое не влияет на общую доступность элементов ИСПДн и средств защиты. Эти инциденты решаются пользователями и администратором безопасности ИСПДн.

Сбой программного обеспечения. Администратор безопасности выясняет причину сбоя программного обеспечения (далее – ПО). Если исправить ошибку своими силами (в том числе после консультации с разработчиками ПО) не удалось, копия акта и сопроводительных материалов (а также файлов, если это необходимо) направляются разработчику ПО.

Отключение электричества. Администратор безопасности проводит анализ на наличие потерь и (или) разрушения данных и ПО, а так же проверяет работоспособность оборудования. В случае необходимости, производится восстановление ПО и данных из последней резервной копии с составлением акта.

Потеря данных. При обнаружении потери данных администратор безопасности проводит мероприятия по поиску и устранению причин потери данных (антивирусная проверка, целостность и работоспособность ПО, целостность и работоспособность оборудования и др.). При необходимости, производится восстановление ПО и данных из резервных копий с составлением акта.

Обнаружена утечка информации (уязвимость в системе защиты). При обнаружении утечки информации ставится в известность администратор безопасности и начальник подразделения. Проводится служебное расследование. Если утечка информации произошла по техническим причинам, проводится анализ защищённости системы и, если необходимо,

принимаются меры по устранению уязвимостей и предотвращению их возникновения.

Физическое повреждение ПЭВМ. Ставится в известность администратор безопасности. Проводится анализ на утечку или повреждение информации. Определяется причина повреждения ПЭВМ и возможные угрозы безопасности информации. В случае возникновения подозрения на целенаправленный вывод оборудования из строя проводится служебное расследование. Проводится проверка ПО на наличие вредоносных программ-закладок, целостность ПО и данных. Проводится анализ электронных журналов. При необходимости проводятся меры по восстановлению ПО и данных из резервных копий с составлением акта.

2) Авария. Любой инцидент, который приводит или может привести к прерыванию работоспособности отдельных элементов ИСПДн и средств защиты. Эти инциденты решаются администратором безопасности совместно с руководством. К авариям относятся следующие инциденты:

– отказ элементов ИСПДн и средств защиты из-за повреждения водой, сбоя системы кондиционирования;

– отсутствие администратора безопасности более чем на сутки из-за химического выброса в атмосферу, сбоев общественного транспорта, эпидемии, массового отравления персонала, сильного снегопада, торнадо, сильных морозов.

3) Катастрофа. Любой инцидент, приводящий к полному прерыванию работоспособности всех элементов ИСПДн и средств защиты, а также к угрозе жизни пользователей ИСПДн, классифицируется как катастрофа. Обычно к катастрофам относят обстоятельства непреодолимой силы (пожар, взрыв), которые могут привести к неработоспособности ИСПДн и средств защиты на сутки и более.

К катастрофам относятся следующие инциденты:

– пожар в здании;

- взрыв;
- просадка грунта с частичным обрушением здания;
- массовые беспорядки.

3. Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций

К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения аварийных ситуаций, такие как:

- системы жизнеобеспечения;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

Системы жизнеобеспечения ИСПДн включают:

- пожарные сигнализации и системы пожаротушения;
- системы вентиляции и кондиционирования;
- системы резервного питания.

Помещения, в которых размещаются элементы ИСПДн и средства защиты должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

Администратор безопасности ознакомляет всех пользователей, находящихся в его зоне ответственности, с данной инструкцией в срок, не превышающий 3-х рабочих дней с момента выхода нового сотрудника на работу.

Должно быть проведено обучение сотрудников, имеющих доступ к ресурсам ИСПДн, порядку действий при возникновении аварийных

ситуаций. Должностные лица должны получить базовые знания в следующих областях:

- оказание первой медицинской помощи;
- пожаротушение;
- эвакуация людей;
- защита материальных и информационных ресурсов;
- методы оперативной связи со службами спасения и лицами, ответственными за реагирование сотрудниками на аварийную ситуацию;
- выключение оборудования, электричества, водоснабжения, газоснабжения.

Администратор безопасности ИСПДн должен быть дополнительно обучен методам частичного и полного восстановления работоспособности элементов ИСПДн.

Навыки и знания должностных лиц по реагированию на аварийные ситуации должны регулярно проверяться. При необходимости должно проводиться дополнительное обучение должностных лиц порядку действий при возникновении аварийной ситуации. Сроки и порядок их обучения согласуется с Администратором безопасности.

Руководитель аппарата управы района  И.Н. Шеина