ГЛАВА Г. ВОЛОГДЫ

ПОСТАНОВЛЕНИЕ
от 28 мая 2019 г. N 279

ОБ УТВЕРЖДЕНИИ КОНЦЕПЦИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВОЛОГОДСКОЙ ГОРОДСКОЙ ДУМЫ И ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВОЛОГОДСКОЙ ГОРОДСКОЙ ДУМЫ

В целях обеспечения безопасности персональных данных субъектов персональных данных, обрабатываемых в информационной системе персональных данных Вологодской городской Думы, на основании Федерального закона от 27 июля 2006 года N 152-ФЗ "О персональных данных", постановления Правительства Российской Федерации от 1 ноября 2012 года N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", на основании части 6 статьи 27, пункта 9 части 2 статьи 38 Устава городского округа города Вологды постановляю:

1. Утвердить прилагаемую Концепцию информационной безопасности Вологодской городской Думы.

2. Утвердить прилагаемую Политику информационной безопасности Вологодской городской Думы.

3. Признать утратившими силу следующие постановления Председателя Вологодской городской Думы:

от 31 декабря 2010 года N 159 "Об утверждении Политики информационной безопасности Вологодской городской Думы";

от 31 декабря 2010 года N 160 "Об утверждении Концепции информационной безопасности информационных систем персональных данных Вологодской городской Думы";

от 18 декабря 2015 года N 327 "О внесении изменений в постановление Председателя Вологодской городской Думы от 31 декабря 2010 года N 159 "Об утверждении Политики информационной безопасности Вологодской городской Думы";

от 18 декабря 2015 года N 329 "О внесении изменений в постановление Председателя Вологодской городской Думы от 31 декабря 2010 года N 160 "Об утверждении Концепции информационной безопасности информационных систем персональных данных Вологодской городской Думы";

от 31 марта 2016 года N 64 "О внесении изменений в постановление Председателя Вологодской городской Думы от 31 декабря 2010 года N 159 "Об утверждении политики информационной безопасности Вологодской городской Думы".

4. Утратил силу с 01.01.2022. - Постановление Главы г. Вологды от 13.12.2021 N 767.

4. Настоящее постановление подлежит опубликованию в газете "Вологодские новости" и размещению на официальном сайте Вологодской городской Думы в информационно-телекоммуникационной сети "Интернет".

Глава г. Вологды
Ю.В.САПОЖНИКОВ

Утверждена
Постановлением
Главы г. Вологды
от 28 мая 2019 г. N 279

КОНЦЕПЦИЯ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВОЛОГОДСКОЙ ГОРОДСКОЙ ДУМЫ

1. Общие положения

1.1. Настоящая Концепция информационной безопасности Вологодской городской Думы (далее - Концепция) определяет общие подходы к обеспечению информационной безопасности в Вологодской городской Думе (далее также - городская Дума, Дума).

1.2. Необходимость утверждения Концепции обусловлена расширением сферы применения информационных технологий и процессов при обработке персональных данных.

1.3. Концепция определяет основные цели, задачи и принципы обеспечения безопасности персональных данных в Вологодской городской Думе, а также общую стратегию построения системы защиты персональных данных Вологодской городской Думы.

1.4. Концепция разработана в соответствии с Федеральным законом от 27 июля 2006 года N 152-ФЗ "О персональных данных" (с последующими изменениями) на основании следующих правовых актов:

- постановление Правительства Российской Федерации от 6 июля 2008 года N 512 "Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных" (с последующими изменениями);

- постановление Правительства Российской Федерации от 15 сентября 2008 года N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации";

- постановление Правительства Российской Федерации от 1 ноября 2012 года N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";

- приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 года N 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных" (с последующими изменениями);

- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная заместителем директора Федеральной службы по техническому и экспортному контролю 14 февраля 2008 года;

- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная заместителем директора Федеральной службы по техническому и экспортному контролю 15 февраля 2008 года.

Концепция разработана в соответствии с системным подходом к обеспечению информационной безопасности в Вологодской городской Думе. Системный подход предполагает анализ актуальных угроз безопасности персональных данных и функционирование системы защиты персональных данных с позиции комплексного применения технических, организационных мер и средств защиты персональных данных.

1.5. В Концепции под информационной безопасностью понимается защищенность персональных данных и обрабатывающей их инфраструктуры от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных. Задачи информационной безопасности сводятся к минимизации ущерба от возможной реализации угроз безопасности персональных данных, а также к прогнозированию и предотвращению таких воздействий.

1.6. В Концепции используются термины и определения в значениях, определенных в Федеральном законе от 27 июля 2006 года N 152-ФЗ "О персональных данных" (с последующими изменениями) и Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора Федеральной службы по техническому и экспортному контролю 15 февраля 2008 года.

1.7. В Концепции используются следующие обозначения и сокращения:

АРМ - автоматизированное рабочее место;

ИСПДн - информационная система персональных данных Вологодской городской Думы;

ЛВС - локальная вычислительная сеть.

1.8. Концепция является основой для:

- Политики информационной безопасности Вологодской городской Думы;

- проведения организационных и технических мер по обеспечению информационной безопасности Вологодской городской Думы;

- принятия управленческих решений, связанных с обеспечением информационной безопасности;

- координации деятельности структурных подразделений аппарата Вологодской городской Думы при проведении работ по развитию и эксплуатации ИСПДн с соблюдением требований обеспечения безопасности персональных данных;

- разработки предложений по совершенствованию правового, методического, технического и организационного обеспечения безопасности персональных данных в ИСПДн.

2. Понятие системы защиты персональных данных, ее задачи, принципы и создание

2.1. Система защиты персональных данных представляет собой совокупность организационных и технических мероприятий для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также иных неправомерных действий с ними.

2.2. Система защиты персональных данных должна обеспечивать эффективное решение следующих задач:

- защита от вмешательства посторонних лиц в процесс функционирования ИСПДн;

- разграничение доступа пользователей;

- регистрация действий пользователей при использовании защищаемых ресурсов ИСПДн в системных журналах и периодический контроль корректности действий пользователей ИСПДн путем анализа содержимого этих журналов;

- контроль целостности (обеспечение неизменности) среды исполнения программ и ее восстановление в случае нарушения;

- защита от несанкционированной модификации и контроль целостности используемых в ИСПДн программных средств, а также защита системы от внедрения несанкционированных программ;

- защита персональных данных от утечки информации по техническим каналам при ее обработке, хранении и передаче по каналам связи;

- обеспечение функционирования криптографических средств защиты информации при компрометации обеспечения безопасности информации;

- своевременное выявление источников угроз безопасности персональных данных, причин и условий, способствующих нанесению ущерба субъектам персональных данных, создание механизма оперативного реагирования на угрозы безопасности персональных данных и негативные тенденции;

- создание условий для минимизации и локализации наносимого ущерба неправомерными действиями, ослабление негативного влияния и ликвидация последствий нарушения безопасности персональных данных.

2.3. Система защиты персональных данных строится на принципах комплексности, непрерывности, своевременности, преемственности и непрерывности совершенствования, персональной ответственности, гибкости системы защиты, открытости алгоритмов и механизмов защиты, простоты применения средств защиты, научной обоснованности и технической реализуемости, обязательности контроля.

2.4. Содержание принципов построения системы защиты персональных данных раскрывается в Политике информационной безопасности Вологодской городской Думы.

2.5. Создание системы защиты персональных данных включает следующие стадии:

- предпроектная стадия, включающая предпроектное обследование ИСПДн, при необходимости разработку технического (частного технического) задания на ее создание;

- стадия проектирования (разработки проектов) и реализации ИСПДн, включающая разработку системы защиты персональных данных в составе ИСПДн;

- стадия ввода в действие системы защиты персональных данных, включающая опытную эксплуатацию и приемосдаточные испытания средств защиты, а также оценку соответствия ИСПДн требованиям безопасности информации.

2.6. Документы, на основании которых строится система защиты персональных данных, требования к ее содержанию, определяются Политикой информационной безопасности Вологодской городской Думы.

3. Объект защиты персональных данных

3.1. В информационной системе объектами защиты являются информация, содержащаяся в информационной системе, технические средства (в том числе средства вычислительной техники, машинные носители информации, средства и системы связи и передачи данных, технические средства обработки буквенно-цифровой, графической, видео- и речевой информации), общесистемное, прикладное, специальное программное обеспечение, информационные технологии, а также средства защиты информации.

3.2. Виды персональных данных, подлежащих защите, и требования по обеспечению их защиты определяются Политикой информационной безопасности Вологодской городской Думы.

4. Меры, методы и средства обеспечения требуемого уровня защищенности персональных данных

4.1. Требования по обеспечению защиты персональных данных определяются Политикой информационной безопасности Вологодской городской Думы.

4.2. Обеспечение требуемого уровня защищенности достигается с использованием мер, методов и средств безопасности.

4.3. Меры по обеспечению безопасности персональных данных, подлежащих реализации в ИСПДн (далее также - меры), подразделяются на:

- законодательные (правовые);

- организационные (административные);

- физические;

- технические (аппаратные и программные).

Состав и содержание мер по обеспечению безопасности персональных данных, подлежащих реализации в ИСПДн, определяются Политикой информационной безопасности Вологодской городской Думы.

4.4. К законодательным (правовым) мерам относится действующее законодательство в сфере персональных данных, закрепляющее права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающее ответственность за нарушения этих прав и обязанностей, препятствуя тем самым неправомерному использованию персональных данных, и являющееся сдерживающим фактором для вероятных нарушителей.

4.5. К организационным (административным) мерам относятся меры организационного характера, регламентирующие процессы функционирования ИСПДн, использование ресурсов ИСПДн, а также порядок взаимодействия пользователей с ИСПДн таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

4.5.1. Организационные (административные) меры реализуются в соответствии с Политикой информационной безопасности Вологодской городской Думы и состоят из мер административного уровня и организационных мер.

4.5.2. К административному уровню относится формирование нормативной правовой базы обеспечения защиты персональных данных в ИСПДн.

4.5.3. Организационные меры должны:

- исключать возможность несанкционированных действий в отношении объектов защиты;

- определять коалиционные и иерархические принципы и методы разграничения доступа к персональным данным;

- определять порядок работы с программно-математическими и техническими (аппаратными) средствами защиты;

- обеспечивать противодействие несанкционированному доступу на этапах аутентификации,

авторизации, идентификации.

4.5.4. Организационные меры включают вопросы доступа в помещения, где размещается ИСПДн, допуска сотрудников к использованию ресурсов ИСПДн, ведения баз данных и осуществления модификации информационных ресурсов, обслуживания и осуществления модификации аппаратных и программных ресурсов ИСПДн, принятия инструкций в отношении участников обработки и обеспечения безопасности персональных данных в ИСПДн.

4.6. К физическим мерам относятся механические, электро- или электронно-механические устройства и сооружения, специально предназначенные для создания физических препятствий на возможных путях проникновения и доступа вероятных нарушителей к компонентам системы и защищаемой информации, а также технические средства визуального наблюдения, связи и охранной сигнализации.

4.7. Технические (аппаратно-программные) меры основаны на использовании различных электронных устройств и специальных программ, входящих в состав ИСПДн и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий и т.д.).

Применение технических (аппаратно-программных) мер должно приводить к следующим результатам:

- обеспечение физической целостности всех компонентов ИСПДн;

- каждый пользователь ИСПДн или группа пользователей ИСПДн имеют уникальное системное имя и минимально необходимые для выполнения им своих функциональных обязанностей полномочия по доступу к ресурсам системы;

- все изменения конфигурации технических и программных средств ИСПДн производятся в установленном порядке (регистрируются и контролируются);

- сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.) располагается в местах, недоступных для посторонних (специальных помещениях, шкафах и т.п.);

- ответственными сотрудниками аппарата Вологодской городской Думы осуществляются непрерывное управление и административная поддержка функционирования средств защиты.

5. Угрозы безопасности персональных данных при их обработке в ИСПДн и нарушители безопасности персональных данных

5.1. Для ИСПДн выделяются следующие основные категории возможных угроз безопасности персональных данных:

- угрозы от утечки информации по техническим каналам;

- угрозы несанкционированного доступа к персональным данным (в том числе по каналам связи);

- угрозы уничтожения, хищения аппаратных средств ИСПДн, носителей информации путем физического доступа к элементам ИСПДн;

- угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий);

- угрозы от непреднамеренных действий пользователей ИСПДн и нарушений безопасности

функционирования ИСПДн (системы защиты персональных данных в ее составе) из-за сбоев в программном обеспечении, а также от сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания и воздействий стихийных обстоятельств;

- угрозы от преднамеренных действий пользователей ИСПДн.

5.2. Конкретные угрозы безопасности персональных данных, актуальных при обработке персональных данных в ИСПДн, и их наименования отражаются в муниципальном правовом акте Главы города Вологды об обеспечении защиты персональных данных в ИСПДн.

5.3. Под вероятным нарушителем безопасности персональных данных в Вологодской городской Думе понимается лицо, которое в результате умышленных или неумышленных действий может нанести ущерб объектам защиты персональных данных.

5.4. Вероятные нарушители безопасности персональных данных делятся на две группы:

- внешние нарушители - лица, не имеющие права обработки, пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн;

- внутренние нарушители - лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн.

5.5. Вероятные нарушители безопасности персональных данных отражаются в муниципальном правовом акте Главы города Вологды об обеспечении защиты персональных данных в ИСПДн.

6. Ожидаемый эффект от реализации Концепции

6.1. Реализация Концепции позволит:

- оценить состояние безопасности информации ИСПДн, выявить источники внутренних и внешних угроз информационной безопасности, определить приоритетные направления предотвращения, отражения и нейтрализации этих угроз;

- разработать и (или) уточнить муниципальные правовые акты Главы города Вологды об обеспечении защиты персональных данных в ИСПДн;

- провести классификацию ИСПДн;

- провести организационно-режимные и технические мероприятия по обеспечению безопасности персональных данных в ИСПДн;

- обеспечить необходимый уровень безопасности объектов защиты.

6.2. Осуществление этих мероприятий обеспечит создание единой, целостной и скоординированной системы информационной безопасности персональных данных и создаст условия для ее дальнейшего совершенствования.

Утверждена
Постановлением
Главы г. Вологды
от 28 мая 2019 г. N 279

ПОЛИТИКА
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВОЛОГОДСКОЙ ГОРОДСКОЙ ДУМЫ

1. Общие положения

1.1. Настоящая Политика информационной безопасности (далее - Политика) Вологодской городской Думы (далее также - городская Дума, Дума) разработана в соответствии с основными целями, задачами и принципами обеспечения безопасности персональных данных в Вологодской городской Думе, а также общей стратегией построения системы защиты персональных данных Вологодской городской Думы, определенных Концепцией информационной безопасности Вологодской городской Думы.

1.2. Политика разработана в соответствии с Федеральным законом от 27 июля 2006 года N 152-ФЗ "О персональных данных" (с последующими изменениями) на основании следующих правовых актов:

- постановление Правительства Российской Федерации от 6 июля 2008 года N 512 "Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных" (с последующими изменениями);

- постановление Правительства Российской Федерации от 15 сентября 2008 года N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации";

- постановление Правительства Российской Федерации от 1 ноября 2012 года N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";

- приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 года N 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных" (с последующими изменениями);

- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная заместителем директора Федеральной службы по техническому и экспортному контролю 14 февраля 2008 года;

- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная заместителем директора Федеральной службы по техническому и экспортному контролю 15 февраля 2008 года.

1.3. В Политике используются термины и определения в значениях, определенных в Федеральном законе от 27 июля 2006 года N 152-ФЗ "О персональных данных" (с последующими изменениями) и Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора Федеральной службы по техническому и экспортному контролю 15 февраля 2008 года.

1.4. В Политике используются следующие обозначения и сокращения:

АРМ - автоматизированное рабочее место;

ИСПДн - информационная система персональных данных Вологодской городской Думы;

ЛВС - локальная вычислительная сеть.

1.5. Целью Политики является обеспечение безопасности объектов защиты персональных данных Вологодской городской Думы от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности персональных данных.

1.6. Безопасность персональных данных достигается путем исключения несанкционированного, в том числе непреднамеренного, доступа к персональным данным, результатами которого могут стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

1.7. Защите подлежат персональные данные, указанные в Перечне персональных данных, обрабатываемых в Вологодской городской Думе в связи с реализацией служебных (трудовых) отношений, а также в связи с осуществлением муниципальных функций.

1.8. Требования настоящей Политики распространяются на всех сотрудников Вологодской городской Думы и работников, выполняющих работы или оказывающих услуги Вологодской городской Думе по договору.

2. Требования к системе защиты персональных данных

2.1. Система защиты персональных данных строится на основании следующих документов:

- Перечня персональных данных, обрабатываемых в Вологодской городской Думе в связи с реализацией служебных (трудовых) отношений, а также в связи с осуществлением муниципальных функций;

- Акта определения уровня защищенности информационной системы персональных данных Вологодской городской Думы;

- Частной модели угроз безопасности персональных данных при их обработке в информационной системе персональных данных Вологодской городской Думы;

- Положения о разграничении прав доступа к обрабатываемым персональным данным в информационной системе персональных данных Вологодской городской Думы;

- документов Федеральной службы по техническому и экспортному контролю и Федеральной службы безопасности Российской Федерации.

2.2. В ИСПДн на основании анализа актуальных угроз безопасности персональных данных должны быть определены тип актуальных угроз и необходимый уровень защищенности, составлен список используемых технических средств защиты, а также программного обеспечения, участвующего в обработке персональных данных на всех элементах ИСПДн, в том числе:

- на АРМ лиц, осуществляющих работу в ИСПДн;

- на серверах приложений;

- в системах управления базами данных;

- в границах ЛВС;

- по каналам передачи в сети общего пользования и (или) международного обмена, если по ним передаются персональные данные.

2.3. В зависимости от уровня защищенности ИСПДн и типа актуальных угроз система защиты персональных данных может включать:

2.3.1. Технические средства:

- антивирусные средства для рабочих станций лиц, осуществляющих работу в ИСПДн, и серверов;

- средства межсетевого экранирования.

2.3.2. Функции защиты, обеспечиваемые штатными средствами обработки персональных данных операционными системами, прикладным программным обеспечением и специальными комплексами, реализующими следующие средства защиты:

- управление и разграничение доступа лиц, осуществляющих работу в ИСПДн (возможность доступа только к тем аппаратным, программным и информационным ресурсам ИСПДн и выполнения только тех операций с ними, которые необходимы конкретным пользователям ИСПДн для выполнения своих служебных обязанностей);

- регистрация и учет действий с информацией;

- обеспечение целостности данных;

- обнаружение вторжений.

2.4. Средства защиты, указанные в подпунктах 2.3.1, 2.3.2 пункта 2.3 настоящей Политики, отражаются в муниципальном правовом акте Главы города Вологды об обеспечении защиты персональных данных в ИСПДн.

2.5. В ИСПДн реализуются меры по обеспечению безопасности персональных данных, состав и содержание которых определены в приложении к настоящей Политике.

2.6. Меры по обеспечению безопасности персональных данных призваны обеспечить:

- конфиденциальность информации (обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя);

- целостность информации (состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право);

- доступность информации (возможность реализации беспрепятственного доступа к информации субъектов, имеющих на это надлежащие полномочия).

2.7. Раскрытие принципов построения системы безопасности персональных данных:

- комплексность - предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов;

- непрерывность - целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах цикла функционирования ИСПДн. ИСПДн должна находиться в защищенном состоянии на протяжении всего времени ее функционирования. В соответствии с этим принципом должны приниматься меры по недопущению перехода ИСПДн в незащищенное состояние;

- своевременность - предполагает упреждающий характер мер обеспечения безопасности персональных данных, то есть постановку задач по комплексной защите ИСПДн и реализацию мер обеспечения безопасности персональных данных на ранних стадиях разработки ИСПДн в целом и ее системы защиты информации в частности;

- преемственность и непрерывность совершенствования - предполагают постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования ИСПДн и ее системы защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области;

- персональная ответственность - предполагает возложение ответственности за обеспечение безопасности персональных данных и системы их обработки на каждого сотрудника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей сотрудников строится таким образом, чтобы в случае любого нарушения круг ответственных лиц был четко определяем;

- гибкость системы защиты - принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Для обеспечения возможности варьирования уровнем защищенности средства защиты должны обладать определенной гибкостью. Особенно важным это свойство является в тех случаях, когда установку средств защиты необходимо осуществлять на работающую систему, не нарушая процесса ее нормального функционирования;

- открытость алгоритмов и механизмов защиты - защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно давать возможности ее преодоления (даже разработчикам);

- простота применения средств защиты - механизмы защиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных установленным порядком пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций (ввод нескольких паролей и имен и т.д.);

- научная обоснованность и техническая реализуемость - информационные технологии, технические и программные средства, средства и меры защиты информации должны быть реализованы на современном уровне развития науки и техники, научно обоснованы с точки зрения достижения заданного уровня безопасности информации и должны соответствовать установленным нормам и требованиям по безопасности персональных данных;

- обязательность контроля - предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности персональных данных на основе используемых систем и средств защиты информации при совершенствовании критериев и методов оценки эффективности этих систем и средств. Контроль за деятельностью любого лица, осуществляющего работу в ИСПДн, каждого средства защиты и в отношении любого объекта защиты должен осуществляться на основе применения средств оперативного контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей.

2.8. Контроль эффективности системы защиты персональных данных должен осуществляется на периодической основе. Целью контроля эффективности является своевременное выявление ненадлежащих режимов работы системы защиты персональных данных (отключение средств защиты, нарушение режимов защиты, несанкционированное изменение режима защиты и т.п.), а также прогнозирование и превентивное реагирование на новые угрозы безопасности персональных данных.

Контроль может проводиться как администратором безопасности ИСПДн (оперативный

контроль в процессе информационного взаимодействия в ИСПДн), так и привлекаемыми для этой цели компетентными организациями, имеющими лицензию на этот вид деятельности, а также Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в пределах их компетенции.

Контроль может осуществляться администратором безопасности ИСПДн как с помощью штатных средств системы защиты персональных данных, так и с помощью специальных программных средств контроля.

3. Лица, осуществляющие работу в ИСПДн

3.1. В ИСПДн Вологодской городской Думы можно выделить следующие группы лиц, участвующих в обработке и хранении персональных данных:

- администратор ИСПДн;

- администратор безопасности ИСПДн;

- пользователь ИСПДн (оператор АРМ);

- администратор сети.

Данные о группах лиц, уровне их доступа и информированности должны быть отражены в Положении о разграничении прав доступа к обрабатываемым персональным данным в информационной системе персональных данных Вологодской городской Думы.

3.2. Администратором ИСПДн является сотрудник отдела Отдела автоматизации и материально-технического обеспечения Управления по обеспечению деятельности Главы города Вологды и Вологодской городской Думы, ответственный за настройку, внедрение и сопровождение ИСПДн, который обеспечивает функционирование системы управления доступом в ИСПДн и уполномочен осуществлять предоставление и разграничение доступа пользователя ИСПДн (оператора АРМ) к элементам, хранящим персональные данные.

Администратор ИСПДн:

- обладает полной информацией о системном и прикладном программном обеспечении ИСПДн;

- обладает полной информацией о технических средствах и конфигурации ИСПДн;

- имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн;

- обладает правами конфигурирования и административной настройки технических средств ИСПДн.

3.3. Администратором безопасности ИСПДн является сотрудник Отдела автоматизации и материально-технического обеспечения Управления по обеспечению деятельности Главы города Вологды и Вологодской городской Думы, ответственный за функционирование системы управления доступом в ИСПДн, включая обслуживание и настройку административной, серверной и клиентской составляющих.

Администратор безопасности ИСПДн:

- осуществляет настройку средств криптографической защиты информации, межсетевых экранов и систем обнаружения атак, в соответствии с которыми пользователь ИСПДн (оператор АРМ) получает возможность работать с элементами ИСПДн;

- осуществляет аудит средств защиты персональных данных;

- обеспечивает безопасность взаимодействия сети Вологодской городской Думы с сетями других организаций (в случае осуществления взаимодействия);

- обладает правами Администратора ИСПДн, указанными в подпункте 3.2 пункта 3 настоящей Политики;

- обладает полной информацией об ИСПДн;

- имеет доступ к средствам защиты информации, протоколирования и к ключевым элементам ИСПДн.

3.4. Пользователем ИСПДн (оператором АРМ) является сотрудник Вологодской городской Думы, осуществляющий обработку персональных данных, уполномоченный на обработку персональных данных, которая включает возможность просмотра персональных данных, ручной ввод персональных данных в систему ИСПДн, формирование справок и отчетов по информации, полученной в ИСПДн.

Пользователь ИСПДн (оператор АРМ):

- обладает всеми необходимыми сведениями (например, паролем), обеспечивающими доступ к обрабатываемым им персональным данным;

- располагает конфиденциальными данными, к которым имеет доступ;

- не имеет полномочий для управления системой защиты персональных данных.

3.5. Администратором сети Вологодской городской Думы является сотрудник Отдела автоматизации и материально-технического обеспечения Управления по обеспечению деятельности Главы города Вологды и Вологодской городской Думы, ответственный за функционирование сети Вологодской городской Думы.

Администратор сети:

- обладает информацией о системном и прикладном программном обеспечении ИСПДн;

- обладает информацией о технических средствах и конфигурации ИСПДн;

- имеет физический доступ к техническим средствам обработки информации и средствам защиты информации в ИСПДн.

3.6. Обязанности лиц, указанных в пунктах 3.2 - 3.5, описаны в следующих документах:

- Инструкция администратора информационной системы персональных данных Вологодской городской Думы;

- Инструкция администратора безопасности информационной системы персональных данных Вологодской городской Думы;

- Инструкция пользователя информационной системой персональных данных Вологодской городской Думы.

4. Требования по обеспечению защиты персональных данных

4.1. Сотрудники Вологодской городской Думы, осуществляющие работу в ИСПДн, должны выполнять требования положений законодательства Российской Федерации о персональных

данных, в том числе требования к защите персональных данных, муниципальных правовых актов по вопросам обработки и защиты персональных данных и документов, устанавливающих обязанности сотрудников по соблюдению требований конфиденциальности и безопасности персональных данных.

4.2. При приеме на работу сотрудник Вологодской городской Думы проходит ознакомление:

- с муниципальными правовыми актами по вопросам обработки и защиты персональных данных и документами, устанавливающими обязанности сотрудников по соблюдению требований конфиденциальности и безопасности персональных данных, - у лица, ответственного за организацию обработки персональных данных в Вологодской городской Думе;

- с информацией о санкционированном использовании ИСПДн - у лица, ответственного за обеспечение безопасности персональных данных в информационной системе Вологодской городской Думы.

4.3. Сотрудники Вологодской городской Думы, осуществляющие работу в ИСПДн и использующие технические средства аутентификации (например, токены, USB-ключи или смарт-карты), должны обеспечивать сохранность указанных средств и не допускать несанкционированный доступ к ним, а также не допускать возможность их утери или использования третьими лицами. Пользователи ИСПДн (операторы АРМ) несут персональную ответственность за сохранность технических средств аутентификации.

4.4. Сотрудникам Вологодской городской Думы, осуществляющим работу в ИСПДн, запрещается:

- устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а также записывать на них защищаемую информацию;

- разглашать защищаемую информацию, которая стала им известна при работе в ИСПДн, третьим лицам.

4.5. Сотрудники Вологодской городской Думы, осуществляющие работу в ИСПДн, обязаны:

- следовать установленным Инструкцией пользователя информационной системой персональных данных требованиям организации парольной защиты;

- обеспечить при работе с персональными данными в отсутствие возможности просмотра персональных данных третьими лицами с мониторов АРМ;

- немедленно сообщать лицу, ответственному за обеспечение безопасности персональных данных в информационной системе Вологодской городской Думы, обо всех наблюдаемых или подозрительных случаях работы ИСПДн, могущих повлечь за собой угрозы безопасности персональным данным, а также о выявленных событиях, затрагивающих безопасность персональных данных.

4.6. Сотрудники Вологодской городской Думы, осуществляющие работу в ИСПДн, при наличии угроз безопасности персональных данных должны быть проинформированы об этом лицом, ответственным за обеспечение безопасности персональных данных в информационной системе Вологодской городской Думы.

5. Ответственность, связанная с обработкой и защитой персональных данных в ИСПДн

5.1. В соответствии со статьей 24 Федерального закона от 27 июля 2006 года N 152-ФЗ "О персональных данных" лица, виновные в нарушении требований указанного федерального

закона, несут предусмотренную законодательством Российской Федерации ответственность.

5.2. Виды предусмотренной законодательством Российской Федерации ответственности за нарушение Федерального закона от 27 июля 2006 года N 152-ФЗ "О персональных данных" применительно к обработке и защите персональных данных в ИСПДн:

- административная ответственность (в том числе за нарушение законодательства Российской Федерации в области персональных данных, нарушение правил защиты информации, незаконную деятельность в области защиты информации);

- дисциплинарная ответственность (за разглашение работником персональных данных другого работника);

- гражданско-правовая (материальная) ответственность (в виде возмещения ущерба (убытков), возникшего в связи с неправомерными действиями по обработке и защите персональных данных);

- уголовная ответственность (неправомерный доступ к компьютерной информации).

5.3. Администратор ИСПДн и Администратор безопасности ИСПДн несут ответственность за все действия, совершенные от имени их учетных записей или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

5.4. При нарушениях пользователями ИСПДн (операторами АРМ) требований, связанных с обработкой и защитой персональных данных в ИСПДн, они несут ответственность, установленную действующим законодательством Российской Федерации и указанную в пункте 5.2 настоящей Политики.

5.5. В положениях о структурных подразделениях аппарата Вологодской городской Думы, осуществляющих обработку персональных данных в ИСПДн, и должностных инструкциях сотрудников Вологодской городской Думы должны быть отражены обязанности сотрудников по соблюдению требований, установленных действующим законодательством о персональных данных, правовых актов работодателя по обеспечению безопасности персональных данных при их обработке в ИСПДн.

Приложение
к Политике
информационной безопасности
Вологодской городской Думы

СОСТАВ И СОДЕРЖАНИЕ
МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ,
ПОДЛЕЖАЩИХ РЕАЛИЗАЦИИ В ИНФОРМАЦИОННОЙ СИСТЕМЕ
ВОЛОГОДСКОЙ ГОРОДСКОЙ ДУМЫ

N п/п	Содержание мер по обеспечению безопасности персональных данных, подлежащих реализации в информационной системе Вологодской городской Думы
1. Идентификация и аутентификация субъектов доступа и объектов доступа	
1.1.	Идентификация и аутентификация пользователей, являющихся работниками

	Вологодской городской Думы
1.2.	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов
1.3.	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации
1.4.	Защита обратной связи при вводе аутентификационной информации
1.5.	Идентификация и аутентификация пользователей, не являющихся работниками Вологодской городской Думы (внешних пользователей)
2. Управление доступом субъектов доступа к объектам доступа	
2.1.	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей
2.2.	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа
2.3.	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы
2.4.	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы
2.5.	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)
2.6.	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу
2.7.	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации
2.8.	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети
2.9.	Регламентация и контроль использования в информационной системе технологий беспроводного доступа
2.10.	Регламентация и контроль использования в информационной системе мобильных технических средств
2.11.	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)
3. Ограничение программной среды	
3.1.	Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения

3.2.	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов
4. Защита машинных носителей персональных данных	
4.1.	Учет машинных носителей персональных данных
4.2.	Управление доступом к машинным носителям персональных данных
5. Регистрация событий безопасности	
5.1.	Определение событий безопасности, подлежащих регистрации, и сроков их хранения
5.2.	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения
5.3.	Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти
5.4.	Защита информации о событиях безопасности
6. Антивирусная защита	
6.1.	Реализация антивирусной защиты
6.2.	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)
7. Обнаружение вторжений	
7.1.	Обнаружение вторжений
8. Контроль (анализ) защищенности персональных данных	
8.1.	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей
8.2.	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации
8.3.	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации
8.4.	Контроль состава технических средств, программного обеспечения и средств защиты информации
9. Обеспечение целостности информационной системы и персональных данных	
9.1.	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации
9.2.	Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций

10. Обеспечение доступности персональных данных	
10.1.	Использование отказоустойчивых технических средств
10.2.	Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование
11. Защита среды виртуализации	
11.1.	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления, средствами виртуализации
11.2.	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин
11.3.	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных
11.4.	Контроль целостности виртуальной инфраструктуры и ее конфигураций
11.5.	Реализация и управление антивирусной защитой в виртуальной инфраструктуре
12. Защита технических средств	
12.1.	Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам
12.2.	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения, в которых они установлены
12.3.	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр
12.4.	Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов)
13. Защита информационной системы, ее средств, систем связи и передачи данных	
13.1.	Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи
13.2.	Исключение возможности отрицания пользователем факта отправки персональных данных другому пользователю
13.3.	Исключение возможности отрицания пользователем факта получения персональных данных от другого пользователя
13.4.	Обеспечение загрузки и исполнения программного обеспечения с машинных носителей персональных данных, доступных только для чтения, и контроль

	целостности данного программного обеспечения
13.5.	Защита беспроводных соединений, применяемых в информационной системе
14. Выявление инцидентов и реагирование на них	
14.1.	Определение лиц, ответственных за выявление инцидентов и реагирование на них
14.2.	Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий
14.3.	Принятие мер по устранению последствий инцидентов
15. Управление конфигурацией информационной системы и системы защиты персональных данных	
15.1.	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных
15.2.	Управление изменениями конфигурации информационной системы и системы защиты персональных данных