

##### АДМИНИСТРАЦИЯ ГОРОДА ЮГОРСКА

Ханты-Мансийского автономного округа – Югры

###### П О С Т А Н О В Л Е Н И Е

от 28 февраля 2019 года № 458

О комиссии по защите

персональных данных

администрации города Югорска

В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», 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», постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»:

1. Создать комиссию по защите персональных данных администрации города Югорска.

2. Утвердить:

2.1. Положение о комиссии по защите персональных данных администрации города Югорска (приложение 1).

2.2. Состав комиссии по защите персональных данных администрации города Югорска (приложение 2).

2.3. Правила осуществления внутреннего контроля соответствия обработки персональных данных в администрации города Югорска требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами (приложение 3).

3. Признать утратившими силу:

- постановление администрации города Югорска от 30.06.2015 № 2419 «Об утверждении Положения о комиссии по технической защите информации»;

- распоряжение администрации города Югорска от 22.09.2011 № 695 «О создании комиссии».

4. Контроль за выполнением постановления возложить на первого заместителя главы города – директора департамента муниципальной собственности и градостроительства администрации города Югорска С.Д. Голина.

**Глава города Югорска А.В. Бородкин**

**Приложение 1**

**к постановлению**

**администрации города Югорска**

**от 28 февраля 2019 года\_№ 458**

**ПОЛОЖЕНИЕ**

**о комиссии по защите персональных данных**

**администрации города Югорска**

1. Комиссия по защите персональных данных администрации города Югорска (далее – Комиссия) является коллегиальным, постоянно действующим органом. В своей деятельности Комиссия руководствуется Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», 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», постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

2. Комиссия формируется не менее чем из четырёх человек, в том числе из председателя Комиссии, секретаря Комиссии и двух членов Комиссии. Состав Комиссии утверждается постановлением администрации города Югорска.

В период отсутствия председателя Комиссии, секретаря Комиссии или члена Комиссии их обязанности исполняет лицо, исполняющее их обязанности по основной должности.

3. Полномочия Комиссии:

1) осуществление внутреннего контроля соответствия обработки персональных данных установленным требованиям к защите персональных данных в соответствии с Правилами, утверждёнными постановлением администрации города Югорска;

2) подготовка и утверждение ежегодного плана осуществления внутреннего контроля обработки персональных данных в администрации города Югорска установленным требованиям;

3) анализ и учёт результатов внутреннего контроля соответствия обработки персональных данных установленным требованиям к защите персональных данных;

4) подготовка предложений по совершенствованию системы защиты персональных данных в администрации города Югорска;

5) проведение расследования нарушений по вопросам защиты персональных данных в администрации города Югорска, разработка предложений по устранению недостатков и предупреждению подобного рода нарушений.

4. Комиссия имеет право осуществлять подготовку предложений о привлечении экспертов, сторонних организаций на платной основе для разработки и выполнения мероприятий по защите персональных данных.

5. Свою деятельность Комиссия осуществляет в соответствии с утверждённым планом деятельности. Заседания Комиссии созываются её председателем не реже 2 раз в год.

6. Заседание Комиссии считается правомочным, если на нём присутствует не менее двух третей от утверждённого состава Комиссии.

7. Решения Комиссии оформляются протоколом, который подписывают председатель Комиссии и секретарь Комиссии.

**Приложение 2**

**к постановлению**

**администрации города Югорска**

**от 28 февраля 2019 года\_№ 458**

Состав

комиссии по защите персональных данных

администрации города Югорска

|  |  |
| --- | --- |
| Первый заместитель главы города – директор департамента муниципальной собственности и градостроительства администрации города Югорска | - председатель комиссии |
| Заместитель начальника отдела информационных технологий администрации города Югорска | - секретарь комиссии |
|  |  |
| Начальник отдела информационных технологий администрации города Югорска | - член комиссии |
| Старший инженер-программист отдела информационных технологий администрации города Югорска | - член комиссии |

**Приложение 3**

**к постановлению**

**администрации города Югорска**

**от 28 февраля 2019 года\_№ 458**

**ПРАВИЛА**

**осуществления внутреннего контроля соответствия обработки**

**персональных данных в администрации города Югорска**

**требованиям к защите персональных данных, установленным**

**Федеральным законом «О персональных данных» и принятыми**

**в соответствии с ним нормативными правовыми актами**

1. Настоящие Правила определяют процедуру, направленную на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных в администрации города Югорска, основания и порядок проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

2. Проведение внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в органах и структурных подразделениях администрации города Югорска (далее - внутренний контроль) осуществляется комиссией по защите персональных данных администрации города Югорска (далее – Комиссия) не реже двух раз в год.

3. В целях осуществления внутреннего контроля Комиссия организует проведение плановых и внеплановых проверок.

Плановые проверки проводятся в соответствии с ежегодным планом осуществления внутреннего контроля обработки персональных данных в администрации города Югорска установленным требованиям, который разрабатывается и утверждается Комиссией.

Внеплановые проверки проводятся на основании информации в письменном виде о нарушениях правил обработки персональных данных, поступившей в администрацию города Югорска. Проведение внеплановой проверки организуется в течение 3 (трёх) рабочих дней со дня поступления информации о нарушениях правил обработки персональных данных.

Плановые и внеплановые проверки проводятся по решению председателя Комиссии. Срок проведения проверки составляет не более 30 дней со дня принятия решения о её проведении.

4. При проведении внутреннего контроля обработки персональных данных с использованием средств автоматизации проверяются:

1) соблюдение норм допуска и учёта лиц, допущенных к работе с персональными данными;

2) обеспечение рабочих мест средствами защиты информации;

3) соблюдение пользователями информационных систем персональных данных парольной политики:

- правил формирования пароля;

- правил ввода пароля;

- правил хранение пароля;

4) соблюдение пользователями информационных систем персональных данных антивирусной политики:

- поддержки рабочего состояния антивирусного программного обеспечения;

- своевременного обновления антивирусного программного обеспечения;

5) соблюдение пользователями информационных систем персональных данных Правил работы со съёмными носителями персональных данных:

- ведения журнала учёта съёмных носителей персональных данных;

- хранения съёмных носителей в персональных шкафчиках пользователей, запирающихся на ключ, расположенных в кабинетах, доступ к которым ограничен;

- проверки съёмного носителя на наличие вредоносных программ, перед каждым началом работы с ним;

- исключения копирования с данного носителя файлов сомнительного содержания и установки нелицензионного программного обеспечения;

- исключения передачи съёмного носителя третьим лицам;

- запрета на оставление съёмного носителя включённым/выключенным без присмотра;

- запрета на обработку информации, содержащейся на съёмном носителе в присутствии третьих лиц;

- запрета на вынос съёмного носителя за пределы служебного помещения;

6) соблюдение ответственными за криптографические средства защиты информации Правил работы с ними:

- хранения криптографических средств в персональных шкафчиках пользователей, запирающихся на ключ, расположенных в кабинетах, доступ к которым ограничен;

- исключения передачи криптографического средства третьим лицам;

- запрета на оставление криптографического средства включённым/выключенным без присмотра;

- запрета на вынос криптографического средства за пределы служебного помещения;

- запрета на использование для электронной цифровой подписи открытых и закрытых ключей электронной цифровой подписи, если пользователю известно, что эти ключи используются или использовались ранее;

- запрета на разглашение конфиденциальной информации, к которой пользователи допущены, средства её защиты, в том числе сведения о криптографических средствах;

- обязанности сообщать в орган криптографической защиты о ставших пользователям известными попытках третьих лиц получить сведения об используемых криптографических средствах;

- обязанности немедленно уведомлять орган криптографической защиты о фактах утраты криптографического средства;

7) соблюдение порядка доступа в помещения, где расположены элементы информационных систем персональных данных:

- все элементы информационных систем хранятся в индивидуальных ящиках каждого пользователя, запирающихся на ключ, расположенных в кабинетах;

- соблюдение ограничения доступа в кабинеты, где используются элементы информационных систем;

8) соблюдение порядка резервирования баз данных и хранения резервных копий:

- наличия актуальных резервных копий;

- поддержки рабочего состояния систем хранения резервных копий;

9) знание пользователями информационных систем персональных данных алгоритма действий во внештатных ситуациях:

- проведения анкетирования/опроса пользователя о порядке действий во внештатных ситуациях.

5. При проведении внутреннего контроля обработки персональных данных без использования средств автоматизации проверяются:

1) хранение бумажных носителей с персональными данными:

- соблюдение хранения бумажных носителей, содержащих персональные данные, в закрываемых шкафах;

- запрет передачи бумажных носителей, содержащих персональные данные, третьим лицам;

- запрет выноса бумажных носителей, содержащих персональные данные, за пределы служебного помещения;

- исключение возможности доступа к бумажным носителям, содержащим персональные данные, третьих лиц;

2) доступ в помещения, где обрабатываются и хранятся бумажные носители с персональными данными:

- все бумажные носители хранятся в индивидуальных ящиках каждого пользователя, расположенных в кабинетах;

- соблюдение ограничения доступа в кабинеты, где хранятся бумажные носители персональных данных.

6. Члены Комиссии соблюдают конфиденциальность и обеспечивают безопасность при обработке персональных данных, ставших им известными в ходе проведения мероприятий внутреннего контроля.

7. Результаты внутреннего контроля оформляются в виде Акта проверки соответствия обработки персональных данных требованиям к защите персональных данных (Приложение), который подписывается всеми членами Комиссии. При выявлении в ходе внутреннего контроля нарушений в Акте проверки указываются мероприятия по устранению нарушений и сроки их исполнения.

Информация о нарушениях, выявленных в ходе внутреннего контроля, доводится до главы города Югорска.

**Приложение к Правилам**

**осуществления внутреннего контроля**

**соответствия обработки персональных данных**

**в администрации города Югорска требованиям**

**к защите персональных данных, установленным**

**Федеральным законом «О персональных данных»**

**и принятыми в соответствии с ним**

**нормативными правовыми актами**

**АКТ**

**проверки соответствия обработки персональных данных**

**требованиям к защите персональных данных**

г.Югорск «\_\_\_»\_\_\_\_\_\_\_20\_\_\_г.

Комиссия по защите персональных данных администрации города Югорска в составе:

председателя комиссии:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

секретаря комиссии:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

членов комиссии:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

провела проверку соответствия обработки персональных данных требованиям к защите персональных данных в органе/структурном подразделении администрации города Югорска:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

перечень занимаемых помещений:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

количество рабочих мест с использованием средств автоматизации:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

количество рабочих мест без использования средств автоматизации:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Перечень используемых информационных систем персональных данных (ИСПДн):\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

В результате проверки соответствия условий обработки персональных данных требованиям к защите персональных данных выявлено:

1. Организация системы допуска и учёта лиц, допущенных к работе с конфиденциальной информацией:

|  |  |
| --- | --- |
| Выявленные нарушения |  |
| Корректирующие меры |  |
| Срок исполнения |  |

2. Организация системы защиты межсетевого взаимодействия:

|  |  |
| --- | --- |
| Выявленные нарушения |  |
| Корректирующие меры |  |
| Срок исполнения |  |

3. Организация режима безопасности помещений информационных систем, в которых осуществляется обработка конфиденциальной информации:

|  |  |
| --- | --- |
| Выявленные нарушения |  |
| Корректирующие меры |  |
| Срок исполнения |  |

4. Организация безопасного хранения и уничтожения материальных носителей конфиденциальной информации:

|  |  |
| --- | --- |
| Выявленные нарушения |  |
| Корректирующие меры |  |
| Срок исполнения |  |

5. Организация защиты от вредоносного кода:

|  |  |
| --- | --- |
| Выявленные нарушения |  |
| Корректирующие меры |  |
| Срок исполнения |  |

6. Организация парольной защиты:

|  |  |
| --- | --- |
| Выявленные нарушения |  |
| Корректирующие меры |  |
| Срок исполнения |  |

7. Организация управления инцидентами информационной безопасности и реагирование на них:

|  |  |
| --- | --- |
| Выявленные нарушения |  |
| Корректирующие меры |  |
| Срок исполнения |  |

8. Организация управления конфигурацией информационных систем Организации и системы защиты конфиденциальной информации:

|  |  |
| --- | --- |
| Выявленные нарушения |  |
| Корректирующие меры |  |
| Срок исполнения |  |

9. Организация системы криптографической защиты информации:

|  |  |
| --- | --- |
| Выявленные нарушения |  |
| Корректирующие меры |  |
| Срок исполнения |  |

10. Организация системы резервного копирования и восстановления:

|  |  |
| --- | --- |
| Выявленные нарушения |  |
| Корректирующие меры |  |
| Срок исполнения |  |

11. Организация централизованного управления системой защиты конфиденциальной информации:

|  |  |
| --- | --- |
| Выявленные нарушения |  |
| Корректирующие меры |  |
| Срок исполнения |  |

12. Организация системы обучения по вопросам обеспечения безопасности конфиденциальной информации:

|  |  |
| --- | --- |
| Выявленные нарушения |  |
| Корректирующие меры |  |
| Срок исполнения |  |

Председатель комиссии \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Секретарь комиссии \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Члены комиссии: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_