УТВЕРЖДЕНО
распоряжением Администрации
Кыштымского городского округа
«09» 11 2015 г. № 64р

ПОЛОЖЕНИЕ
о порядке организации и проведения работ по защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в Администрации Кыштымского городского округа

СОГЛАСОВАНО
Начальник Управления
информационной безопасности
Министерства информационных
технологий и связи
Челябинской области

_____ Е.В.Огорельцев
«05» 11 2015 года

Положение
о порядке организации и проведения работ по защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в Администрации Кыштымского городского округа

1. Общие положения

1. Настоящее Положение о порядке организации и проведения работ по защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в Администрации Кыштымского городского округа (далее - Положение) разработано в соответствии с Федеральным законом от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Специальными требованиями и рекомендациями по технической защите конфиденциальной информации (СТР-К), утвержденными приказом Гостехкомиссии России от 30.08.2002 г. № 282, и другими нормативно-методическими документами по защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну.

2. Настоящее Положение определяет порядок организации и проведения работ по защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну (далее – информация ограниченного доступа), в Администрации Кыштымского городского округа (органах Администрации Кыштымского городского округа).

3. Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия её собственника.

4. При определении конфиденциальности документов, в том числе в электронной форме, необходимо руководствоваться Перечнем сведений конфиденциального характера в органах местного самоуправления Кыштымского городского округа (далее - Перечень), утвержденным постановлением Администрации Кыштымского городского округа.

5. Муниципальные служащие и работники Администрации Кыштымского городского округа (органа Администрации Кыштымского городского округа), которые в силу служебной необходимости должны иметь доступ к информации конфиденциального характера, обязаны ознакомиться с настоящим положением, Перечнем и подписать обязательство о неразглашении информации конфиденциального характера по форме, утвержденной распоряжением Администрации Кыштымского городского округа.

6. Ознакомление муниципальных служащих и работников Администрации Кыштымского городского округа (органа Администрации Кыштымского городского округа) (далее – Администрация (орган Администрации)) с Положением и Перечнем, а также инструктаж по работе с информацией конфиденциального характера производятся при приеме на службу (работу) в Администрацию (орган Администрации) общим отделом Администрации (кадровой службой органа Администрации).

Подписанное муниципальным служащим или работником Администрации (органа Администрации) обязательство о неразглашении информации конфиденциального характера хранится в его личном деле.

7. Порядок обращения со служебной информацией ограниченного доступа должен осуществляться в соответствии с требованиями Положения о порядке

обращения со служебной информацией ограниченного распространения в Администрации Кыштымского городского округа, утвержденного распоряжением Администрации Кыштымского городского округа от 18.06.2015 г. № 10дсп.

8. Ответственность за общее состояние и организацию работ по технической защите информации ограниченного доступа в Администрации Кыштымского городского округа возложена на Главу Кыштымского городского округа (руководителя органа Администрации).

Ответственность за выполнение мероприятий по защите информации ограниченного доступа в Администрации Кыштымского городского округа возложена на ведущего специалиста по технической защите информации отдела мобилизационной работы Администрации (ответственное лицо органа Администрации).

2. Информация, подлежащая защите, и потенциальные угрозы информационной безопасности объектов защиты

9. Защите подлежит информация ограниченного доступа (речевая информация и информация, обрабатываемая техническими средствами, а также представленная в виде носителей на бумажной, магнитной, магнитно-оптической и иной основе).

Объектами защиты при этом являются:

автоматизированные системы (далее - АС);

средства изготовления и размножения документов (далее - СИРД);

защищаемые помещения (далее - ЗП).

10. В качестве угроз информационной безопасности объектов защиты необходимо рассматривать:

использование разведками иностранных государств технических средств для получения информации ограниченного доступа, перехват информации, обсуждаемой в ЗП и циркулирующей в основных технических средствах и системах, а также воздействие на информационные ресурсы АС с целью разрушения, искажения и блокирования информации;

использованием криминальными структурами технических средств для получения информации, представляющей ценность в интересах планирования криминальных акций;

преднамеренные действия нарушителей и злоумышленников, незаконным путем проникших на объекты посредством контактного несанкционированного доступа к элементам АС, к носителям информации, к вводимой и выводимой информации, к программному обеспечению, а также подключения к линиям связи;

непреднамеренные действия персонала, приводящие к утечке, искажению, разрушению информации, подлежащей защите, в том числе ошибки эксплуатации технических и программных средств АС.

3. Цели и задачи технической защиты информации ограниченного доступа

11. Целями технической защиты информации ограниченного доступа являются:

исключение утечки информации ограниченного доступа с помощью технических средств разведки;

предотвращение несанкционированного доступа (далее - НСД) к информации ограниченного доступа, ее разрушения, искажения, уничтожения, блокировки и несанкционированного копирования в системах и средствах информатизации;

обеспечение условий быстрого, полного и всестороннего расследования случаев утечки информации;

устранение негативных последствий и условий в случае несанкционированной утечки и утраты информации.

12. Задачами технической защиты информации ограниченного доступа являются:

проведение в Администрации государственной политики по технической защите информации;

подготовка предложений по совершенствованию правового, нормативно-методического и организационного обеспечения технической защиты информации в Администрации;

анализ состояния и прогнозирование источников угроз безопасности информации;

учет информационных ресурсов, систем и средств формирования, передачи, хранения, обработки и распространения информации, подлежащих технической защите;

контроль и анализ состояния технической защиты информации в Администрации;

развитие и совершенствование системы подготовки кадров в области технической защиты информации в Администрации.

4. Порядок аттестации, ввода в эксплуатацию объектов информатизации и взаимодействия Администрации, специализированных сторонних организаций при эксплуатации объектов информатизации и системы защиты информации

13. В Администрации (органе Администрации) отделом мобилизационной работы Администрации (ответственным лицом органа Администрации) документально оформляется перечень объектов информатизации (АС, СИР и ЗП), а также лиц, ответственных за их эксплуатацию в соответствии с установленными требованиями по защите информации.

14. Все объекты информатизации (далее именуется - ОИ), предназначенные для обработки (хранения, циркуляции) информации ограниченного доступа, должны быть аттестованы на соответствие установленным нормам и требованиям по защите информации.

Аттестация предусматривает комплексную проверку (аттестационные испытания) защищаемого объекта информатизации в реальных условиях эксплуатации с целью оценки соответствия использованного комплекса мер и средств защиты требуемому уровню безопасности информации.

15. Аттестационные испытания проводятся аттестационной комиссией предприятий (организаций), имеющих лицензию Федеральной службы по техническому и экспортному контролю на деятельность по технической защите конфиденциальной информации (организации-лицензиаты ФСТЭК России).

Для проведения испытаний аттестационной комиссией подготавливаются и представляются:

технический паспорт на объект информатизации;

акт классификации объекта информатизации по требованиям защиты информации;

состав технических и программных средств, входящих в автоматизированную систему (или технических средств, расположенных в защищаемом помещении);

план контролируемой зоны;

перечень защищаемых в АС ресурсов (или конфиденциальность обсуждаемых в защищаемых помещении вопросов);

организационно-распорядительную документацию разрешительной системы доступа персонала к защищаемым ресурсам АС (обсуждаемым вопросам);

инструкции пользователям и администратору безопасности информации;

инструкции по эксплуатации средств защиты информации;

сертификаты соответствия требованиям по безопасности информации на используемые средства защиты информации.

В результате аттестационных испытаний оформляется «Аттестат соответствия», которым подтверждается, что объект информатизации соответствует требованиям стандартов или иных нормативных документов по защите конфиденциальной информации, утвержденных Федеральной службой по техническому и экспортному контролю Российской Федерации и другими органами государственного управления в пределах их компетенции.

На основании выданного специализированной организацией аттестата соответствия издается распоряжение о разрешении обработки информации ограниченного доступа на объекте информатизации и назначении лиц, ответственных за обеспечение защиты информации при его эксплуатации.

Методическое руководство, разработку требований к мерам защиты и контроль эффективности использования предусмотренных мер защиты информации ограниченного доступа обеспечивает отдел мобилизационной работы Администрации в соответствии с законодательством Российской Федерации в области защиты информации ограниченного доступа.

Отдел мобилизационной работы осуществляет следующие основные функции в области защиты информации ограниченного доступа:

осуществляет методическое руководство и участвует в разработке (согласовании) конкретных требований по защите информации ограниченного доступа и разработке технического задания на аттестацию объекта информатизации;

согласовывает степень участия персонала в обработке (обсуждении, передаче, хранении) защищаемой информации;

определяет класс защищенности объектов информатизации;

определяет перечень предполагаемых к использованию сертифицированных средств защиты информации.

Привлечение для организации работ по созданию системы защиты информации или ее отдельных компонентов сторонних специализированных организаций осуществляется в соответствии с порядком, устанавливаемым нормативными и организационно-распорядительными документами ФСТЭК России.

В случае привлечения для обеспечения безопасности информации сторонних специализированных организаций в соответствии с требованиями Федерального закона от 05.04.2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» рекомендуется выполнение следующих условий:

наличие у организации лицензии на право проведения работ по технической защите конфиденциальной информации;

проведение инструктажа исполнителей работ по вопросам информационной безопасности;

другие условия, устанавливаемые соответствующими нормативными и организационно-распорядительными документами.

Структурная схема взаимодействия Администрации и специализированных сторонних организаций при аттестации, вводе в эксплуатацию и эксплуатации ОИ и системы защиты информации приведена в приложении 1 к данному Положению.

5. Контроль состояния защиты информации ограниченного доступа Администрации

16. Контроль состояния защиты информации ограниченного доступа в Администрации осуществляется в целях:

предупреждения и пресечения возможности получения техническими средствами разведки охраняемых сведений об объектах информатизации Администрации;

выявления и предотвращения утечки информации по техническим каналам;

исключения или существенно затруднения несанкционированного доступа к информации, хищения технических средств и носителей информации;

предотвращения специальных программно-технических воздействий, вызывающих нарушение целостности информации или работоспособности систем информатизации.

17. Основными задачами контроля являются:

проверка организации выполнения мероприятий по защите информации в Администрации, учета требований по защите информации в разрабатываемых плановых и распорядительных документах;

проверка выполнения установленных норм и требований по защите информации;

оценка достаточности и эффективности мероприятий по защите информации;

проверка выполнения требований по антивирусной защите автоматизированных рабочих мест;

проверка знаний должностных лиц по вопросам защиты информации;

оперативное принятие мер по пресечению нарушений (требований) норм защиты информации на объектах информатизации Администрации Кыштымского городского округа.

18. Повседневный контроль за выполнением мероприятий по защите информации осуществляет работник Администрации (органа Администрации), ответственный за эксплуатацию объекта информатизации.

19. Периодический контроль за выполнением мероприятий по защите информации проводится руководителями структурных подразделений Администрации (руководителями органов Администрации), где эксплуатируется объект информатизации, не реже одного раза три месяца.

В ходе контроля проверяется:

соблюдение организационно-режимных требований;

выполнение требований по защите автоматизированных систем от несанкционированного доступа;

выполнение требований по антивирусной защите автоматизированных систем.

Результаты контроля отражаются в Журнале учета мероприятий по контролю над соблюдением режима защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну (приложение 2).

20. Контроль эффективности принятых мер защиты информации на объектах информатизации Администрации с использованием технических средств осуществляется не реже одного раза в год комиссией, назначаемой распоряжением Администрации, с оформлением протокола ежегодной проверки на соответствие требованиям по защите информации и заключения по результатам ежегодной проверки на соответствие требованиям по защите информации объекта информатизации.

Результаты контроля отражаются в техническом паспорте объекта информатизации.

6. Ответственность должностных лиц

21. Ответственность за организацию работ по защите информации в Администрации Кыштымского городского округа возлагается на Главу Кыштымского городского округа (руководителя органа Администрации).

22. Ответственность за планирование работ по защите информации, организацию контроля за эффективностью их выполнения, организацию разработки нормативно-методических документов по технической защите информации, разработку (совместно со структурными подразделениями Администрации, эксплуатирующими ОИ) распорядительных документов по вопросам организации технической защиты информации, аттестацию объектов информатизации возлагается на ведущего специалиста по технической защите информации отдела мобилизационной работы Администрации Кыштымского городского округа (ответственное лицо органа Администрации).

23. Ответственность за выполнение установленных мероприятий по технической защите информации на введенных в эксплуатацию объектах информатизации возлагается на руководителя структурного подразделения Администрации (органа Администрации), эксплуатирующего объект информатизации и ответственного за эксплуатацию объекта информатизации.

24. Ответственность за формирование политики антивирусной защиты, организацию своевременной инсталляции средств антивирусной защиты информации и обновление баз данных вирусных описаний на АС возлагается на администратора безопасности.

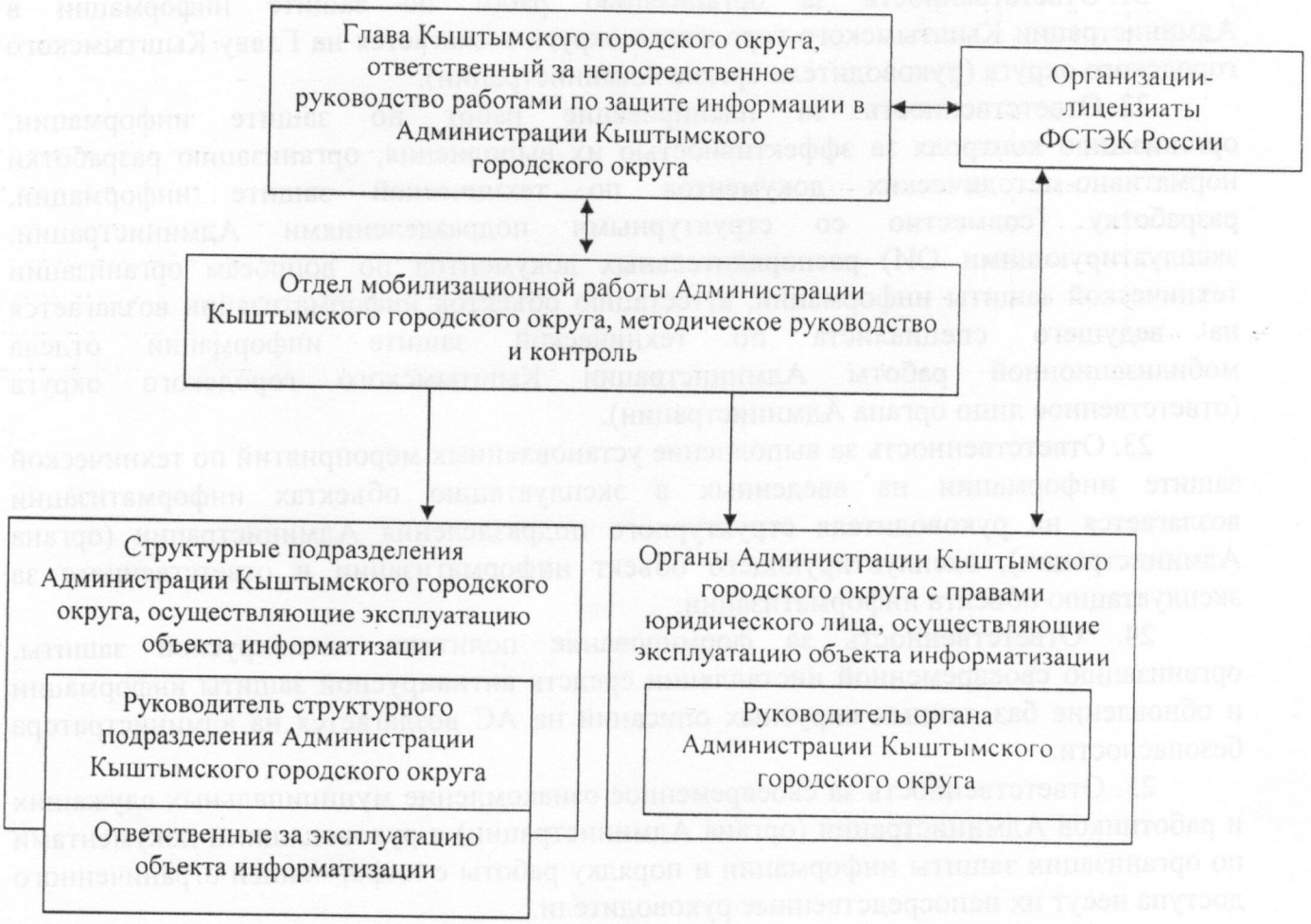
25. Ответственность за своевременное ознакомление муниципальных служащих и работников Администрации (органа Администрации) с руководящими документами по организации защиты информации и порядку работы с информацией ограниченного доступа несут их непосредственные руководители.

26. Должностные лица, допустившие разглашение информации ограниченного доступа, несут ответственность в соответствии с действующим законодательством Российской Федерации.

Исполняющий обязанности начальника
отдела мобилизационной работы
Администрации Кыштымского
городского округа Н.Л. Серышев

Приложение 1
к Положению о порядке организации
и проведения работ по защите информации
ограниченного доступа, не содержащей
сведений, составляющих государственную
тайну, в Администрации Кыштымского
городского округа

Структурная схема взаимодействия Администрации Кыштымского городского округа и специализированных организаций при аттестации, вводе в эксплуатацию и эксплуатации объектов информатизации (ОИ) и системы защиты информации



Приложение 2
к Положению о порядке организации
и проведения работ по защите информации
ограниченного доступа, не содержащей
сведений, составляющих государственную
тайну, в Администрации Кыштымского
городского округа

ЖУРНАЛ
учета мероприятий по контролю над соблюдением режима защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну

№ п/п	Дата	Наименование мероприятия	Исполнитель	Результат	Примечания
1	2	3	4	5	6