РОССИЙСКАЯ ФЕДЕРАЦИЯ
МУРМАНСКАЯ ОБЛАСТЬ

ЗАКРЫТОЕ АДМИНИСТРАТИВНО-ТЕРРИТОРИАЛЬНОЕ ОБРАЗОВАНИЕ г. СЕВЕРОМОРСК

АДМИНИСТРАЦИЯ ЗАТО г. СЕВЕРОМОРСК

Р А С П О Р Я Ж Е Н И Е

от 27.02.2015 г. № 190/2-р

Об утверждении Технического регламента по организации контроля эффективности защиты информации в Информационной системе администрации ЗАТО г.Североморск

В целях исполнения требований Федеральных законов от 27.07.2006 № 152-ФЗ «О персональных данных», от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации», постановления 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. Утвердить:

1.1. Технический регламент по организации контроля эффективности защиты информации в Информационной системе администрации ЗАТО г.Североморск, согласно приложению к распоряжению.

1.2. Должностную инструкцию ответственного за организацию обработки персональных данных в администрации ЗАТО г.Североморск.

2. Назначить ответственным за организацию обработки персональных данных в администрации ЗАТО г.Североморск начальника информационно-технического отдела администрации ЗАТО г.Североморск **Мышачкова Д.А.**, а в его отсутствие - временно исполняющего обязанности начальника информационно-технического отдела администрации ЗАТО г.Североморск.

3. Руководителям структурных подразделений администрации ЗАТО г.Североморск с правом юридического лица:

3.1. Обеспечить выполнение требований распоряжения.

3.2. Назначить ответственных за организацию обработки персональных данных.

Глава администрации
ЗАТО г.Североморск **И.Л. Норина**

Приложение
к распоряжению администрации
ЗАТО г.Североморск
от 27.02.2015 № 190/2-р

Технический регламент по организации контроля эффективности защиты информации в Информационной системе администрации ЗАТО г.Североморск

1. Общие положения

1.1. Настоящий Регламент устанавливает организацию и порядок проведения контроля защищенности информационных систем (ИС) администрации ЗАТО г.Североморск (далее - Администрация).

1.2. Регламент разработан на основе действующих в Российской Федерации правовых и нормативных документов по защите информации.

1.3. Положение является документом, обязательным для выполнения всеми должностными лицами при проведении работ, требующих защиты информации.

2. Цели и задачи контроля состояния защиты информации

2.1. Контроль состояния защиты информации в ИС (контроль защищенности ИС) в администрации ЗАТО г.Североморск осуществляется с целью своевременного выявления и предотвращения несанкционированного доступа к информации, ее утечки по техническим каналам, преднамеренных специальных воздействий на информацию (носители информации) и других угроз информационной безопасности.

2.2. Основными задачами контроля являются:

- проверка соответствия принятых и принимаемых мер по защите информации нормативно-правовым требованиям;
- проверка своевременности и полноты выполнения требований нормативных документов, регламентирующих организацию и порядок осуществления мероприятий по защите информации в Администрации.

При проведении контроля необходимо обеспечить подтверждение того, что:

- созданная система безопасности обеспечивает выполнение требований по защите информации при эксплуатации ИС;
- меры, средства и мероприятия, проводимые в целях защиты информации, соответствуют предъявляемым к ИС требованиям безопасности информации;
- средства защиты информации настроены и используются правильно;
- рекомендации предшествующих проверок реализованы.

3. Организация контроля

3.1. Основными составляющими контроля являются:

- автоматизированный контроль на основе мониторинга событий информационной безопасности;
- проверка правильности и полноты проводимых мероприятий по обеспечению соответствия ИС требованиям безопасности информации;
- проверка работоспособности и эффективности средств защиты информации. Проверка работоспособности средств защиты в рамках контрольных мероприятий проводятся в соответствии с программой проведения контроля состояния защиты информации в ИС;
- проверка своевременности внесения изменений в проектную, техническую и нормативно-техническую документацию по обеспечению безопасности информации;
- принятие на основании результатов контроля мер по устранению последствий нарушений требований безопасности вплоть до полного или частичного приостановления эксплуатации ИС, приостановления или прекращения действия «Аттестата соответствия»,

если иными мерами невозможно устранить нарушения требований безопасности информации;

- проведение в ходе мероприятий по контролю разъяснительной работы по применению требований законодательства Российской Федерации и нормативных документов в области обеспечения безопасности информации в АС.

3.2 Контроль состояния защиты информации в ИС проводится экспертной комиссией, образованной по распоряжению Главы Администрации. Контроль может проводиться специалистами сторонних организаций, имеющих необходимые лицензии ФСТЭК и ФСБ России, на основании договоров.

Результаты контроля оформляются актами, заключениями и записями в специальных журналах и доводятся до сведения пользователей и должностных лиц в соответствии с уровнем контроля.

Члены экспертных комиссий, осуществляющих контроль, имеют право:

- знакомиться с организацией работ по защите информации в ИС;

- получать по запросу в печатном виде документацию, касающуюся функционирования ИС;

- получать доступ ко всем помещениям, шкафам, стеллажам, сейфам, где размещены технические средства ИС и хранятся носители информации;

- требовать демонстрации режимов функционирования системы, конфигурации аппаратных и программных средств, их настроек и других параметров, влияющих на безопасность ресурсов ИС;

- получать доступ к журналам регистрации событий, происходящих в ИС;

- получать информацию о нарушениях безопасности в ИС и результаты разбора этих нарушений при наличии таковых;

- знакомиться с работой пользователей ИС.

Пользовательский персонал ИС Администрации должен содействовать проверяющим в реализации вышеуказанных прав.

Представители органов, осуществляющих контроль (эксперты), обязаны выполнять правила и распорядок работы отделов Администрации, а так же не должны препятствовать работе пользователей ИС.

3.3. Проверка работоспособности средств защиты в рамках контрольных мероприятий проводятся в соответствии с программами проведения контроля состояния защиты информации в ИС, разрабатываемыми проверяющими организациями и согласованными с Администрацией.

3.4. Одной из форм контроля защищенности ИС является аудит информационной безопасности (контроль эффективности защиты), заключающийся в оценке соответствия текущего состояния информационной безопасности ИС требованиям правовых и нормативных документов в области защиты информации.

3.5. Аудит информационной безопасности может проводиться независимой от инициатора аудита организацией, имеющей лицензию ФСТЭК России на осуществление мероприятий и оказание услуг по технической защите конфиденциальной информации.

3.6. Организация, проводящая аудит, должна информировать Администрацию обо всех мероприятиях, проводимых в рамках аудиторской проверки.

До сведения представителей Администрации должна доводиться информация о ходе аудита информационной безопасности и любых возникающих проблемах. Данные о защищенности ИС, собранные при проведении аудита, которые являются критическими для информационной безопасности ИС Администрации, должны быть немедленно доведены до сведения ответственных лиц Администрации.

3.7. Администрация должна обеспечивать предоставление организации, проводящей аудит, всей необходимой информации для проведения аудита информационной безопасности.

4. Проведение контроля

4.1. Контроль состояния защиты информации заключается в оценке:

- соблюдения требований правовых и организационно-распорядительных и нормативных документов по защите информации;

- корректности использования и работоспособности применяемых мер и средств защиты информации в соответствии с их эксплуатационной документацией;

- знаний и выполнения пользователями своих функциональных обязанностей в части защиты информации.

В результатах контроля должны содержаться оценка состояния защиты информации в ИС и, при необходимости, рекомендации по устранению недостатков и/или по совершенствованию системы защиты информации в ИС.

4.2. Внутренний плановый контроль состояния защиты информации при эксплуатации ИС проводится специалистами отдела информационно-технического обеспечения и защиты информации в соответствии с планом (приложение № 1). Планы составляются на заявленный срок таким образом, чтобы в течение года была проведена проверка выполнения всех требований информационной безопасности, которым должна отвечать ИС.

4.3. В рамках подготовки к проведению внутреннего планового контроля рекомендуется выполнить:

- формирование комиссии для проведения контроля из числа сотрудников отдела информационно-технического обеспечения и защиты информации;

- определение руководителя комиссии;

- формирование плана проведения контроля;

- подготовку отчетных материалов (актов, заключений) с результатами контроля (приложение № 2).

4.4. При проведении внутреннего планового контроля комиссия:

- проверяет на соответствие с законодательством РФ необходимых организационно-распорядительных и эксплуатационных документов на СЗИ и знание их сотрудниками Администрации;

- проверяет выполнение требований организационно-распорядительных и эксплуатационных документов сотрудниками Администрации;

- документирует результаты контроля;

- вырабатывает рекомендации по устранению недостатков в обеспечении информационной безопасности и по совершенствованию СЗИ ИС.

4.5. По результатам внутреннего планового контроля разрабатывается план по устранению недостатков в обеспечении информационной безопасности и по совершенствованию системы защиты информации ИС (приложение № 3), в соответствии с которым в Администрации разрабатываются и проводятся необходимые мероприятия.

4.6. При повседневном контроле осуществляется анализ событий, произошедших в ИС по различным системным журналам. Для расследования инцидентов, связанных с нештатными ситуациями или нарушением информационной безопасности, в Администрации могут создаваться комиссии.

4.7. В ходе проведения аудита информационной безопасности осуществляется оценка соответствия текущего состояния информационной безопасности требованиям правовых и нормативных документов в области защиты информации.

При проведении аудита информационной безопасности осуществляется анализ:

- организационно-распорядительных и эксплуатационных документов по обеспечению безопасности информации;

- организации работ по эксплуатации ИС, распределения обязанностей, ответственности и функций подразделений, участвующих в эксплуатации ИС;

- состава и характеристик используемых средств защиты и порядка их применения;

- порядка разработки, приобретения, испытания, внедрения и модификации программных средств ИС;

- порядка установки, эксплуатации, модификации, замены и ремонта технических средств защиты информации.

4.8. В ходе проведения аудита информационной безопасности эксперты указывают на возможные нарушения и несоответствия в обеспечении безопасности информации и дают рекомендации по их устранению.

4.9. По результатам аудита организацией, проводящей аудит, составляется заключение, содержащее рекомендации по устранению нарушений и несоответствий, которые не удалось устранить в процессе проведения аудита.

Приложение № 1
к Техническому регламенту
по организации контроля эффективности
защиты информации в Информационной
системе администрации ЗАТО г.Североморск,
утвержденному распоряжением
администрации ЗАТО г.Североморск от
27.02.2015 № 190/2-р

ПЛАН
внутренних проверок состояния защиты персональных данных
на период с « __ » _____ 201_ г по « __ » _____201_ г.

№	Мероприятие	Периодичность, срок исполнения	Исполнитель
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			

_____

Приложение № 2
к Техническому регламенту
по организации контроля эффективности
защиты информации в Информационной
системе администрации ЗАТО г.Североморск,
утвержденному распоряжением
администрации ЗАТО г.Североморск
от 27.02.2015 № 190/2-р

Администрация ЗАТО г.Североморск
АКТПРОВЕРКИ№_____

_____ _____
(населенный пункт) (дата)

Комиссией в составе:

Председателя комиссии:

_____ _____
(ФИО) (должность)

Членов комиссии:

_____ _____
(ФИО) (должность)

_____ _____
(ФИО) (должность)

_____ _____
(ФИО) (должность)

в соответствии с_____
(наименование, номер и дата документа, в соответствии с которым
_____в период с _____по_____
проводится проверка) (дата) (дата)
в присутствии_____
(должности, фамилии и инициалы ответственных представителей)
_____
проведена_____ проверка_____
(комплексная, целевая) (указать проверяемое
_____
ее подразделение, объект, систему)

1. В ходе работы проверено выполнение требований действующих норм и правил законодательства Российской Федерации, а также организационно-распорядительных и руководящих документов в области защиты информации:

_____
(указать наименования норм, правил и документов)
_____
_____

2. Необходимо устранить выявленные нарушения в установленные сроки:

№ п/п	Выявленные нарушения требований по защите информации, причины и условия, приведшие к этим нарушениям	Нарушенные законодательные акты, организационно-распорядительные и руководящие документы в области защиты информации	Содержание предписании по устранению нарушении	Срок устранения нарушений	Примечание
1	2	3	4	5	6

3. Выводы и принятые меры.

_____

(указать меры, которые были приняты комиссией в процессе проверки)

Председатель комиссии:

(ФИО)	(должность)

Члены комиссии:

(ФИО)	(должность)
(ФИО)	(должность)
(ФИО)	(должность)

Приложение № 3
к Техническому регламенту
по организации контроля эффективности
защиты информации в Информационной
системе администрации ЗАТО г.Североморск,
утвержденному распоряжением
администрации ЗАТО г.Североморск
от 27.02.2015 № 190/2-р

Руководитель _____
_____ И.О. Фамилия

«___» _____ 20__ г.

План устранения недостатков и замечаний, выявленных представителями в ходе проведения внутренней проверки в администрации ЗАТО г.Североморск

№ п/п	Недостатки и замечания, отмеченные в «Акте проверки...» (исх. от __ _____ 20__ № _)	Мероприятия по приведению организации и состояния работ в соот-ветствие с требованиями документов	Ответственные за выполнение должностные лица	Сроки завершения работ	Отметка о выполнении мероприятий, форма представления отчетных материалов и место их нахождения.	Примечание
1	2	3	4	5	6	7

Председатель комиссии:

(ФИО)	(должность)	(должность)

Члены комиссии:

(ФИО)	(должность)	(должность)
(ФИО)	(должность)	(должность)
(ФИО)	(должность)	(должность)

_____

Приложение № 2
к распоряжению администрации
ЗАТО г.Североморск
от 27.02.2015 № 190/2-р

Должностная инструкция
ответственного за организацию обработки персональных данных в администрации ЗАТО г.Североморск

1. Общие положения

1.1. Должностная инструкция разработана в соответствии с требованиями 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, утвержденного постановлением Правительства Российской Федерации от 21.03.2012 № 211.

1.2. Ответственным за организацию обработки персональных данных в администрации ЗАТО г.Североморска (далее - Администрации) назначается распоряжением Администрации ЗАТО г.Североморск.

1.3. Ответственный за организацию обработки персональных данных в Администрации в своей деятельности руководствуется Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Положением о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела, утвержденным Указом Президента Российской Федерации от 30.05.2005 № 609, Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 01.11.2012 № 1119, Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденным постановлением Правительства Российской Федерации от 15.09.2008 № 687, приказом Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», и другими правовыми актами по вопросам обработки и защиты персональных данных.

2. Обязанности ответственного за организацию обработки персональных данных в Управлении

2.1. Ответственный за организацию обработки персональных данных в Администрации обязан:

- осуществлять внутренний контроль за соблюдением работниками Администрации законодательства Российской Федерации, локальных актов по обработке персональных данных, требований к защите персональных данных и принимать меры по устранению выявленных нарушений;

- организовывать проведение занятий и (или) доведение до сведения работников Администрации положений законодательства Российской Федерации о персональных данных, локальных актов Администрации по вопросам обработки персональных данных, требований к защите персональных данных;

- руководить разработкой в Администрации распоряжений, положений, инструкций, правил, порядков, перечней и других документов, регламентирующих порядок обработки персональных данных по вопросам защиты персональных данных в соответствии с требованиями законодательства и нормативно-правовых актов Российской Федерации;

- организовывать и контролировать прием и обработку обращений и запросов субъектов персональных данных или их представителей;

- при организации обработки персональных данных принимать необходимые правовые, организационные и технические меры для защиты персональных данных от неправомерного намеренного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении персональных данных;

- докладывать главе администрации города Мурманска о выявленных нарушениях обработки персональных данных или требований по их защите, принимаемых мерах и способах устранения выявленных нарушений.

3. Ответственность лица, ответственного за организацию обработки персональных данных

3.1. В соответствии с законодательством Российской Федерации ответственный за организацию обработки персональных данных несет дисциплинарную, административную и гражданско-правовую ответственность за невыполнение или халатное выполнение обязанностей по организации, контролю и обеспечению выполнения требований законодательства, нормативно-правовых актов Российской Федерации по вопросам обработки и защиты персональных данных в Администрации.

4. Права ответственного за организацию обработки персональных данных

4.1. Ответственный за организацию обработки персональных данных имеет право:

- требовать от работников Администрации письменных объяснений по фактам нарушения ими требований законодательства Российской Федерации, локальных актов об обработке и защите персональных данных;

- вносить предложения главе администрации ЗАТО г.Североморск об отстранении работников от обработки персональных данных, применению к ним дисциплинарных взысканий, в том числе об увольнении работников, при обнаружении нарушения ими требований законодательства Российской Федерации, локальных актов по вопросам обработки персональных данных или требований к защите персональных данных.

_____