АДМИНИСТРАЦИЯ ИНЖАВИНСКОГО РАЙОНА
ТАМБОВСКОЙ РАЙОНА

Р А С П О Р Я Ж Е Н И Е

10.04.2013 р.п. Инжавино № 67 -р

Об утверждении Правил осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации района.

В соответствии с постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами":

1. Утвердить Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации района согласно приложению.

2. Разместить настоящее Распоряжение на официальном сайте Администрации района в сети Интернет http://r53.tambov.gov.ru/.

3. Контроль за исполнением настоящего распоряжения возложить на управляющего делами администрации района Жукова Р.М.

Первый заместитель
главы администрации района И.Г. Ильин

Л.М. Жукова
2-75-53

ПРИЛОЖЕНИЕ
УТВЕРЖДЕНЫ
распоряжением администрации района
от 10.04. 2013 № 67 -р

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

1. Общие положения

Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации района (далее - Правила) относятся к основным организационно-распорядительным документам системы документов информационной безопасности администрации района и разработаны в соответствии с требованиями постановления Правительств Российской Федерации от 21 марта 2012 г. № 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами".

В Правилах определен порядок организации и осуществления внутреннего контроля обработки персональных данных (ПДн) в администрации района с целью своевременного выявления и предотвращения:

хищения технических средств и носителей информации;

утраты информации;

преднамеренных программно-технических воздействий на информацию и (или) средства вычислительной техники, вызывающих нарушение целостности информации и нарушение работоспособности автоматизированной системы;

несанкционированного доступа к ПДн с целью уничтожения, искажения, модификации (подделки), копирования и блокирования;

утечки информации по техническим каналам.

Внутренний контроль состояния защиты информации включает в себя:
контроль организации защиты информации;
контроль эффективности защиты информации.

2. Порядок внутреннего контроля за соблюдением требований по обработке и обеспечению безопасности персональных данных

В целях осуществления внутреннего контроля соответствия обработки ПДн установленным требованиям организуется проведение периодических проверок условий обработки ПДн. Проверки осуществляются муниципальным служащим

администрации района, ответственным за организацию обработки ПДн в администрации района либо комиссией, образуемой главой района, не реже одного раза в год в соответствии с утвержденным графиком.

При осуществлении внутреннего контроля соответствия обработки ПДн установленным требованиям производится проверка:

соблюдения принципов обработки ПДн;

соответствия локальных актов в области ПДн администрации района действующему законодательству Российской Федерации;

выполнения служащими администрации района требований и правил обработки ПДн в информационных системах персональных данных (ИСПДн) администрации района;

перечней ПДн, используемых для решения задач и функций структурными подразделениями администрации района и необходимости обработки ПДн в ИСПДн администрации района;

актуальности содержащихся в Правилах обработки ПДн в администрации района в каждой ИСПДн администрации района информации о законности целей обработки ПДн и оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности ПДн;

правильности осуществления сбора, систематизации, записи, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (распространения, предоставления, доступа), обезличивания, блокирования, удаления, уничтожения ПДн в каждой ИСПДн администрации района;

актуальности перечня должностей муниципальных служащих района, замещающих должности муниципальной службы в администрации района, уполномоченных на обработку ПДн, имеющих доступ к ПДн;

актуальности перечня должностей муниципальных служащих района, замещающих должности муниципальной службы в администрации района, ответственных за проведение мероприятий по обезличиванию обрабатываемых ПДн;

соблюдения прав субъектов персональных данных, чьи ПДн обрабатываются в ИСПДн администрации района;

соблюдения обязанностей администрации района как оператора ПДн, предусмотренных действующим законодательством в области ПДн;

порядка взаимодействия с субъектами персональных данных, ПДн которых обрабатываются в ИСПДн района, в том числе соблюдения сроков, предусмотренных действующим законодательством в области ПДн, соблюдения требований по уведомлениям, порядка разъяснения субъектам персональных данных необходимой информации, порядка реагирования на обращения (запросы) субъектов персональных данных, порядка действий при достижении целей обработки ПДн и отзыве согласий субъектами персональных данных;

наличия необходимых согласий субъектов персональных данных, чьи ПДн обрабатываются в ИСПДн администрации района;

актуальности сведений, содержащихся в уведомлении об обработке (о намерении осуществлять обработку) персональных данных;

актуальности перечня ИСПДн в администрации района;

наличия и актуальности сведений, содержащихся в Правилах обработки ПДн администрации района для каждой ИСПДн администрации района;

знания и соблюдения государственными гражданскими служащими района, замещающими должности муниципальной службы в администрации района (далее - служащие администрации района) положений действующего законодательства Российской Федерации в области ПДн;

знания и соблюдения служащими администрации района положений локальных актов администрации района в области обработки и обеспечения безопасности ПДн;

знания и соблюдения служащими администрации района инструкций, руководств и иных эксплуатационных документов на применяемые средства автоматизации, в том числе программное обеспечение, и средства защиты информации;

соблюдения служащими администрации района конфиденциальности ПДн;

актуальности локальных актов администрации района в области обеспечения безопасности ПДн, в том числе в Технических паспортах ИСПДн;

соблюдения служащими администрации района требований по обеспечению безопасности ПДн;

наличия локальных актов администрации района, технической и эксплуатационной документации технических и программных средств ИСПДн администрации района;

по иным вопросам.

О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, лицо, ответственное за проведение проверки, докладывает главе района.

При проведении внутреннего контроля на ИСПДн (отдельное автоматизированное рабочее место) администрации района составляется протокол контроля выполнения требований по обеспечению безопасности информации, содержащей сведения ограниченного доступа, при ее автоматизированной обработке на автоматизированном рабочем месте по форме, приведенной в приложении к настоящим Правилам.

3. Оценка соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных

Во время осуществления внутреннего контроля соответствия обработки ПДн установленным требованиям в администрации района производится оценка соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности ПДн и принимаемых мер по обработке и обеспечению безопасности ПДн в администрации района.

При оценке соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности ПДн, для каждой ИСПДн администрации района производится экспертное сравнение заявленной администрацией района в своих локальных актах

оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности ПДн и применяемых администрацией района мер, направленных на обеспечение выполнения обязанностей, предусмотренных действующим законодательством в области ПДн и изложенных в настоящих Правилах осуществления внутреннего контроля соответствия обработки ПДн в администрации района.

По итогам сравнений принимается решение о достаточности применяемых администрацией района мер, направленных на обеспечение выполнения обязанностей, предусмотренных действующим законодательством в области ПДн и возможности или необходимости принятия дополнительных мер или изменения установленного в администрации района порядка обработки и обеспечения безопасности ПДн.

Оценка соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности ПДн и принимаемых мер по обработке и обеспечению безопасности ПДн, в администрации района оформляется в виде отдельного документа, подписывается председателем комиссии и утверждается главой района.

По результатам принятых решений муниципальным служащим администрации района, ответственным за организацию обработки ПДн в администрации района, организуется работа по их реализации.

ПРИЛОЖЕНИЕ
к Правилам осуществления внутреннего контроля соответствия
обработки персональных данных требованиям к защите
персональных данных в администрации района

Форма

Протокол №
контроля выполнения требований по обеспечению безопасности информации, содержащей сведения ограниченного доступа, при ее автоматизированной обработке на автоматизированном рабочем месте

_____
(наименование структурного подразделения администрации района)

1. Объект контроля
Указать:
наименование автоматизированного рабочего места (АРМ);
заводской (инвентарный) номер системного блока ПЭВМ АРМ;
принадлежность к подразделению;
адрес размещения АРМ.
2. Назначение объекта
Указать:
тип информации, обрабатываемой (хранимой) на АРМ;
уровень защищенности персональных данных при их обработке в информационной системе.
3. Контролируемые вопросы
Состояние организации технической защиты информации при обработке (хранении) информации ограниченного доступа.
Контроль наличия руководящих документов, инструкций, документации, регламентирующей обработку (хранение) информации ограниченного доступа:
перечня защищаемых ресурсов и уровня их конфиденциальности;
перечня лиц, обслуживающих АРМ;
перечня лиц, имеющих право самостоятельного доступа в помещение с АРМ;
перечня лиц, имеющих право самостоятельного доступа к штатным средствам АРМ и уровень их полномочий;
распоряжения о назначения комиссии для определения уровня защищенности персональных данных;
распоряжения о назначении администратора информационной безопасности;
данных по уровню подготовки персонала;
инструкции по обеспечению защиты информации, обрабатываемой на АРМ;
перечня программного обеспечения;
описания технологического процесса обработки информации;
схемы информационных потоков;
технического паспорта;

матрицы доступа субъектов к защищаемым информационным ресурсам; акта установки системы активного зашумления (при наличии);
акта установки системы защиты информации от несанкционированного доступа (СЗИ НСД) (при наличии);
описания системы разграничения доступа и настроек СЗИ НСД;
инструкции администратору безопасности;
инструкции пользователю;
инструкции по антивирусному контролю;
распоряжения о допуске служащих;
распоряжения о вводе в эксплуатацию.
Контроль соответствия настройки подсистемы управления доступом, подсистемы регистрации и учета, подсистемы обеспечения целостности требованиям присвоенного класса защищенности от НСД.
В соответствии с требованиями руководящего документа "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации", утвержденного решением Председателя Гостехкомиссии от 30.03.1992, в настройках подсистемы управления доступом проверяется:
наличие требований к длине и сложности пароля;
ограничение максимального срока действия пароля;
настройки блокировки учетных записей при попытках несанкционированного доступа;
наличие административных прав у пользователей;
выполнение требований мандатного разграничения прав доступа к каталогам, программам, файлам.
В настройках подсистемы регистрации и учета контролируется:
отсутствие критических ошибок и несанкционированных запусков процессов, зарегистрированных в журнале приложений;
отсутствие зарегистрированных критических системных ошибок в системном журнале;
отсутствие зарегистрированных изменений действующих политик безопасности, прав доступа, настроек системы защиты информации в журнале системы защиты информации;
возможности несанкционированного доступа к информации, аудиты отказа, зарегистрированные в журнале безопасности.
В настройках подсистемы обеспечения целостности контролируется:
соответствие программного обеспечения, установленного на АРМ, аттестационным материалам;
отсутствие программных средств разработки и отладки приложений;
наличие средств антивирусного контроля, включая срок действия лицензии и периодичность обновления антивирусных баз.
Контроль наличия лицензионного программного обеспечения, установленного в процессе проведенной аттестации по требованиям безопасности информации.
Контроль срока действия лицензии, порядка и периодичности обновления баз антивирусной программы.

Контроль наличия сетевых плат (в том числе интегрированных) и физической возможности их использования.
Контроль возможности и фактов подключения незарегистрированных магнитных и иных носителей информации.

4. Метод проведения контроля:

Экспертно-документальный

5. Средства контроля:

Программные возможности операционной системы, установленной на контролируемом АРМ.

6. Перечень документов, регламентирующих выполнение требований по обеспечению безопасности информации

Контроль проводится в соответствии с требованиями:

- Указа Президента Российской Федерации "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена" от 17.03.2008 № 351;
- специальных требований и рекомендаций по технической защите конфиденциальной информации (приказ Гостехкомиссии России от 30.08.2002 № 282);
- руководящего документа "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации" (решение Председателя Гостехкомиссии от 30.03.1992);
- руководящего документа "Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей" (приказ Председателя Гостехкомиссии России от 4.06.1999 № 114);
- нормативных и руководящих документов ФСТЭК России по защите информации.

Контроль выполнили:

_____	_____	_____
должность	подпись	фамилия, инициалы
_____	_____	_____
должность	подпись	фамилия, инициалы

При проведении контроля присутствовали:

_____	_____	_____
должность	подпись	фамилия, инициалы
_____	_____	_____
должность	подпись	фамилия, инициалы

Дата проведения контроля: _____ .
(число, месяц, год)