Приложение №3
УТВЕРЖДЕНЫ
постановлением
Администрации города
Тамбова
22.04.2013 N 3536

ПРАВИЛА
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации города Тамбова

1. Общие положения

Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации города Тамбова (далее - Правила) разработаны в соответствии с требованиями Постановления Правительства Российской Федерации от 21 марта 2012 г. N 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 ред. Постановления администрации города Тамбова от 28.11.2016 N 7227)

В Правилах определен порядок организации и осуществления внутреннего контроля обработки персональных данных (далее - ПДн) 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.

Порядок внутреннего контроля за соблюдением требований по обработке и обеспечению безопасности ПДн. В целях осуществления внутреннего контроля соответствия обработки ПДн установленным требованиям организуется проведение периодических проверок условий обработки ПДн. Проверки

осуществляются 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 действующему законодательству Российской Федерации;
- выполнения муниципальными служащими требований и правил обработки ПДн в информационных системах персональных данных (далее - ИСПДн);
- актуальности 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;
- актуальности перечня должностей должностных лиц, уполномоченных на обработку ПДн, имеющих доступ к ПДн;
- актуальности перечня должностных лиц, ответственных за проведение мероприятий по обезличиванию обрабатываемых ПДн;
- соблюдения прав субъектов персональных данных, чьи ПДн обрабатываются в ИСПДн;
- соблюдения обязанностей оператора ПДн, предусмотренных действующим законодательством в области ПДн;
- порядка взаимодействия с субъектами персональных данных, ПДн которых обрабатываются в ИСПДн, 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;
- актуальности сведений, содержащихся в уведомлении об обработке (о намерении осуществлять обработку) персональных данных;
- актуальности перечня ИСПДн;
- знания и соблюдения муниципальными служащими положений действующего законодательства Российской Федерации в области ПДн, локальных актов администрации города Тамбова;
- (в ред. Постановления администрации города Тамбова от 28.11.2016 N 7227) соблюдения муниципальными служащими конфиденциальности ПДн;
- соблюдения муниципальными служащими требований по обеспечению безопасности ПДн;

- наличия и актуальности локальных актов, технической и эксплуатационной документации технических и программных средств ИСПДн.

О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, лицо, ответственное за проведение проверки, докладывает главе администрации города Тамбова (заместителю главы администрации). (в ред. Постановления администрации города Тамбова от 28.11.2016 N 7227)

При проведении внутреннего контроля на ИСПДн 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.

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

Во время осуществления внутреннего контроля соответствия обработки ПДн установленным требованиям производится соответствие оценки 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 города Тамбова. (в ред. Постановления администрации города Тамбова от 28.11.2016 N 7227)

При оценке соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности ПДн, для каждой ИСПДн производится экспертное сравнение заявленной оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности ПДн и применяемых мер, направленных на обеспечение выполнения обязанностей, предусмотренных действующим законодательством в области ПДн и изложенных в настоящих Правилах осуществления внутреннего контроля соответствия обработки 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, оформляется в виде отдельного документа, подписывается председателем комиссии и утверждается главой администрации города Тамбова (заместителем главы администрации).
(в ред. Постановления администрации города Тамбова от 28.11.2016 N 7227)

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

администрации города Тамбова

Протокол N _____
контроля выполнения требований по обеспечению безопасности информации, содержащей сведения ограниченного доступа, при ее автоматизированной обработке на автоматизированном рабочем месте

_____

(наименование органа администрации города Тамбова)

Объект контроля:
- наименование автоматизированного рабочего места (далее - АРМ);
- заводской (инвентарный) номер системного блока персональной электронно-вычислительной машины АРМ;
- адрес размещения АРМ.

Назначение объекта:
- тип информации, обрабатываемой (хранимой) на АРМ;
- уровень защищенности персональных данных при их обработке в информационной системе.

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 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 (далее - СЗИ НСД) (при наличии);
- описания системы разграничения доступа и настроек СЗИ НСД; инструкции администратора безопасности;
- инструкции пользователя;

- 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 внешних носителей информации.

Метод проведения контроля: экспертно-документальный.

Средства контроля: программные возможности операционной системы, установленной на контролируемом АРМ.

Перечень документов, регламентирующих выполнение требований по обеспечению безопасности информации.

Контроль проводится в соответствии с требованиями:

- Указа Президента Российской Федерации от 17.03.2008 N 351 "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно- телекоммуникационных сетей международного информационного обмена";
- специальных требований и рекомендаций по технической защите конфиденциальной информации (Приказ Гостехкомиссии России от 30.08.2002 N 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 04.06.1999 N 114);
- нормативных и руководящих документов ФСТЭК России по защите информации.

Контроль выполнил:

_____ _____ _____

должность подпись фамилия, инициалы

При проведении контроля присутствовали:

_____ _____ _____

должность подпись фамилия, инициалы

_____ _____ _____

должность подпись фамилия, инициалы

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