ПРАВИЛА ОСУЩЕСТВЛЕНИЯ ВНУТРЕННЕГО КОНТРОЛЯ СООТВЕТСТВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕБОВАНИЯМ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ, УСТАНОВЛЕННЫМ ФЕДЕРАЛЬНЫМ ЗАКОНОМ «О ПЕРСОНАЛЬНЫХ ДАННЫХ», ПРИНЯТЫМИ В СООТВЕТСТВИИ С НИМ НОРМАТИВНЫМИ ПРАВОВЫМИ АКТАМИ И МУНИЦИПАЛЬНЫМИ ПРАВОВЫМИ АКТАМИ В АДМИНИСТРАЦИИ ГОРОДСКОГО ОКРУГА ТОЛЬЯТТИ

Распоряжение от 12.07.2013 № 4292-р/1
Распоряжение от 03.06.2024 № 4673-р/1

I. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящие правила разработаны в соответствии с требованиями Федерального закона от 27.07.2006г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27.07.2006г. № 152–ФЗ «О персональных данных», 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 и муниципальными органами», Постановления Правительства Российской Федерации от 01.11.2012г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Правила определяют процедуры, направленные на выявление и предотвращение нарушений законодательства в сфере защиты персональных данных, разбирательства и составления актов разбирательства инцидента информационной безопасности (далее – ИБ) по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений, а так же выявления и предотвращения нарушений ИБ в администрации.

1.1. Основные термины и понятия, используемые в Правилах.

Инцидент ИБ – событие, в результате наступления которого в администрации произошло разглашение конфиденциальной информации, персональных данных, нарушение работоспособности информационных систем, внесение несанкционированных изменений в информационные ресурсы администрации.

Нарушитель ИБ – лицо, предпринявшее попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно и использовавшее для этого различные возможности, методы и средства.

Информационная система персональных данных (далее - ИСПДн) – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;

Информационные ресурсы (далее - ИР) – совокупность данных, организованных для эффективного получения достоверной информации, документы и отдельные массивы документов в информационных системах;

Автоматизированное рабочее место (далее – АРМ) – индивидуальный комплекс технических и программных средств, предназначенный для автоматизации работы сотрудников органов администрации;

Система защиты от несанкционированного доступа (далее СЗНД) – система защиты информации, предотвращающая или существенно затрудняющая несанкционированный доступ к информации.

II. ПОРЯДОК ПРОВЕДЕНИЯ ПРОВЕРОК УСЛОВИЙ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ.

2.1. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в администрации организуется проведение периодических проверок условий обработки персональных данных.

2.2. Проверки осуществляются департаментом информационных технологий и связи администрации (далее – ДИТиС). Ответственным за организацию проверок является сотрудник, ответственный за организацию обработки персональных данных.

2.3. Плановые проверки соответствия обработки персональных данных установленным требованиям в администрации проводятся на основании утвержденного приказом руководителя ДИТиС ежегодного плана.

Внеплановые проверки организуются в течение трех рабочих дней при наступлении следующих событий:

- поступившее в администрацию письменное заявление субъекта персональных данных о нарушениях правил обработки персональных данных;
- поступившее в ДИТиС сообщение от сотрудников органов администрации о предполагаемом нарушении правил обработки персональных данных;
- получение сигнала о нарушении режима конфиденциальности системы защиты информации;
- получение предписания органов надзора за соблюдением прав субъектов персональных данных.

2.4. При проведении любой проверки соответствия обработки персональных данных установленным требованиям устанавливается соответствие принимаемых мер по обеспечению безопасности персональных данных при их обработке, мерам, указанным в положении об обработке персональных данных, утвержденном распоряжением администрации от 30.12.2010 №13996-р/1.

2.5. Ответственный за организацию проверок имеет право:

- запрашивать у сотрудников органов администрации информацию, необходимую для реализации полномочий;
- принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;
- вносить руководителю ДИТиС предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке.

2.6. Проверка должна быть завершена в срок не позднее чем через тридцать календарных дней со дня принятия решения о её проведении.

2.7. Руководитель ДИТиС контролирует своевременность и правильность проведения проверки.

2.8. Ответственный за организацию проверок предоставляет руководителю ДИТиС акт о результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений по форме согласно приложению №1 к настоящим Правилам.

III. ПОРЯДОК РАЗБИРАТЕЛЬСТВА ИНЦИДЕНТА ИБ

3.1. Разбирательство по вопросам инцидентов ИБ проводится сотрудниками отдела информационной безопасности.

3.2. Цели разбирательства инцидентов ИБ:

- выработка организационных и технических решений, направленных на снижение рисков нарушения ИБ, предотвращение подобных нарушений в будущем;
- обеспечение безопасности обработки персональных данных;
- обеспечение прав субъектов персональных данных на обеспечение безопасности и конфиденциальности их персональных данных, обрабатываемых администрацией;
- предотвращение несанкционированного доступа к информационным системам.

3.3. Этапы разбирательства инцидента ИБ:

- подтверждение или опровержение факта возникновения инцидента ИБ;
- подтверждение или корректировка уровня значимости инцидента ИБ;
- уточнение дополнительных обстоятельств инцидента ИБ;
- получение доказательств возникновения инцидента ИБ, обеспечение их сохранности и целостности;
- минимизация последствий инцидента ИБ;
- информирование и консультирование сотрудников органов администрации по действиям обнаружения, устранения последствий и предотвращения инцидентов ИБ;
- разработка мероприятий по обнаружению и (или) предупреждению инцидентов ИБ.

3.4. Выявление инцидента ИБ.

Основными источниками информации об инцидентах ИБ являются:

- результаты плановых или внеплановых проверок соответствия обработки персональных данных установленным требованиям;
- факты, выявленные сотрудниками органов администрации.

Сотрудник органа администрации может выявить признаки наличия Инцидента ИБ путем анализа текущей ситуации на предмет ее соответствия требованиям Распоряжения мэра городского округа Тольятти от 30.12.2010 № 13996-р/1 «Положение об обработке персональных данных в администрации городского округа Тольятти» (Далее - Положение об обработке ПДн). Выявленные несоответствия дают основания предполагать факт возникновения инцидента ИБ. Любые сведения о предполагаемом инциденте ИБ незамедлительно передаются выявившим их сотрудником в ДИТиС в произвольной форме любым доступным способом:

- по контактам, указанным в телефонном справочнике официального сайта администрации;
- через непосредственного руководителя.

3.5. Ответственный за проведение проверок после получения информации о предполагаемом инциденте ИБ незамедлительно фиксирует дату, время и место возникновения предполагаемого инцидента ИБ и определяет сотрудника ДИТиС, осуществляющего разбирательство.

3.6. В срок не более одного рабочего дня с момента поступления информации об инциденте ИБ, сотрудник ДИТиС, осуществляющий разбирательство, определяет и инициирует первоочередные меры (отключение АРМ предполагаемого нарушителя ИБ от информационной системы, восстановление информации из резервной копии, исправление ошибки ввода, проведение дополнительного инструктажа по ИБ), направленные на локализацию инцидента ИБ и минимизацию его последствий.

3.7. В случае нарушения прав субъекта персональных данных разбирательство и реагирование происходит в порядке и в сроки, предусмотренные Правилами рассмотрения запросов субъектов персональных данных в администрации городского округа Тольятти, утвержденными постановлением мэрии от 24.05.2013г. №1670-п/1 «Об утверждении Правил рассмотрения запросов субъектов персональных данных или их представителей в администрации городского округа Тольятти».

3.8. Проведение разбирательства инцидента ИБ.

3.8.1. В процессе проведения разбирательства инцидента ИБ устанавливаются:

- дата и время совершения инцидента ИБ;
- орган администрации, затронутый инцидентом ИБ;
- информационные ресурсы, затронутые инцидентом ИБ;
- ФИО, должность предполагаемого нарушителя ИБ;
- уровень критичности инцидента ИБ;
- обстоятельства и мотивы совершения инцидента ИБ;
- характер и размер реального и потенциального ущерба;
- обстоятельства, способствовавшие совершению инцидента ИБ.

3.8.2. Осуществляющий разбирательство сотрудник ДИТиС в процессе проведения расследования инцидента ИБ при необходимости запрашивает информацию в органах администрации. Запрос направляется на имя руководителя органа администрации с указанием сроков предоставления информации (с учетом необходимости ее анализа, сбора и подготовки).

3.8.3. После получения необходимой информации по инциденту ИБ осуществляющий разбирательство сотрудник ДИТиС проводит анализ полученных данных.

3.8.4. С целью минимизации последствий инцидента ИБ возможно временное отключение прав доступа у предполагаемого нарушителя ИБ к информационным ресурсам (далее - ИР) на время проведения расследования. Информация об отключении прав доступа сотрудником ДИТиС, ответственным за проведение разбирательства, направляется руководителю предполагаемого нарушителя ИБ.

3.8.5. Восстановление временно отключенных у нарушителя ИБ прав доступа к ИР производится по заявке руководителя нарушителя ИБ или осуществляющего разбирательство сотрудника ДИТиС.

3.10. Собранная в процессе разбирательства инцидента ИБ информация фиксируется осуществляющим разбирательство сотрудником ДИТиС в карточке инцидента ИБ (приложение №2 к настоящим Правилам) и учитывается при подготовке акта разбирательства инцидента ИБ (приложение №3 к настоящим Правилам).

3.11. Осуществляющий разбирательство сотрудник ДИТиС направляет акт разбирательства инцидента ИБ руководителю ДИТиС для последующей передачи руководителям органов администрации, затронутых инцидентом ИБ.

3.12. На основании полученного акта разбирательства инцидента ИБ руководитель органа администрации, затронутого инцидентом ИБ, в срок не более трех рабочих дней организует проведение мероприятий, направленных на снижение рисков ИБ в будущем:

- повторное ознакомление нарушителя ИБ с должностной инструкцией, с действующими нормативно-правовыми актами в области ИБ;
- анализ и пересмотр имеющихся прав доступа к информационным ресурсам у нарушителя ИБ;
- доведение до всех сотрудников органа администрации требований правовых актов в области ИБ.

Приложение №1
к Правилам осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным Законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и муниципальными правовыми актами в администрации городского округа Тольятти

Акт проверки соответствия условий обработки персональных данных положению об обработке персональных данных в

_____
(наименование структурного подразделения органа администрации)

_____ _____
Адрес расположения дата

Раздел, пп. Положения	Проверяемое условие обработки ПДн	Отметка о соответствии
II, 2.1.2.	Наличие записи в должностных инструкциях сотрудников	да / нет
	Наличие подписанного обязательства о неразглашении информации, содержащей персональные данные	да / нет
II, 2.2.1.	Наличие согласия субъекта ПДн об обработке ПДн (за исключением случаев, предусмотренных частью 2 статьи 6 Федерального закона от 27.07.2006г. № 152–ФЗ «О персональных данных»)	да / нет / не требуется
II, 2.2.2.	Наличие утвержденного перечня работников подразделения мэрии, допущенных к обработке персональных данных в связи с исполнением своих служебных (трудовых) обязанностей	да / нет
II, 2.2.3.	Отсутствие обработки специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни	да / нет
II, 2.2.6.; II, 2.4.7.	Наличие журнала учета электронных носителей персональных данных	да / нет / не требуется
при автоматизированной обработке ПДн		
II, 2.2.7.	Отсутствие обработки необезличенных ПДн после достижения цели, в случае отсутствия необходимости в достижении цели обработки ПДн, в случае отзыва субъектом персональных данных согласия на обработку	да / нет
II, 2.3.2.	Функционирование на АРМ пользователей системы антивирусной защиты, СЗНСД (при наличии)	да / нет
при неавтоматизированной обработке ПДн		

II, 2.4.2.	Использование отдельных носителей для каждой категории персональных данных	да / нет / не требуется
II, 2.4.3.	Отсутствие фиксации на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы	да / нет
	Обособление ПДн от иной информации, на отдельных материальных носителях, в специальных разделах или на полях форм (бланков)	да / нет
II, 2.4.3.	Группировка документов, содержащих ПДн в отдельные дела (папки) в зависимости от цели их обработки	да / нет
	Наличие внутренних описей документов с указанием цели обработки и категории персональных данных в делах с документами, содержащими ПДн	да / нет / не требуется
II, 2.4.6.	Наличие организационных (охрана помещений) и технических мер (установка сертифицированных средств защиты информации), исключающих возможность несанкционированного доступа к персональным данным лиц, не допущенных к их обработке	да / нет
II, 2.4.10.	Хранение документов и внешних электронных носителей информации, содержащих ПДн в запираемых и опечатываемых металлических шкафах (сейфах).	да / нет / не требуется
II, 2.4.11.	Наличие оформленных актов при уничтожении ПДн	да / нет
III.	Наличие приказа о назначении ответственного за проведение мероприятий по защите персональных данных	да / нет

От ДИТиС:

_____

_____

От структурного подразделения органа администрации

_____

_____

Приложение №2

к Правилам осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным Законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и муниципальными правовыми актами в администрации городского округа Тольятти

Карточка инцидента информационной безопасности (ИБ)

Дата инцидента ИБ _____ Номер инцидента ИБ _____

Информация о сообщившем:

Ф.И.О.	должность	Подразделение органа администрации	Рабочий телефон

Тип инцидента:		*Действительный* □	*Попытка* □	*Подозрение* □	
Предполагаемый вид угрозы информационной безопасности	*Непреднамеренная* □	*Преднамеренная* □	*Удаленное вмешательство* □	*Ошибка проектирования информационной системы* □	*технический сбой* □
Нарушитель:	*Отсутствует* □	*не установлен* □	*Внешний* □ *Организация, Ф.И.О., должность нарушителя*	*Внутренний* □ *Орган администрации, Ф.И.О., должность нарушителя*	
Последствия инцидента:	*без последствий* □	*нарушение работоспособности компонентов ИС* □	*нарушение целостности ИР, фальсификация документов* □	*нарушение режима конфиденциальности информации* □	
Объект, которому нанесен ущерб:	*Информация* □	*Средства вычислительной техники* □	*Программное обеспечение* □	*Средства связи* □	
Действия, предпринятые для разрешения инцидента:	*Описание действий*	*никаких действий не требуется* □	*Без привлечения внешнего исполнителя* □	*С привлечением внешнего исполнителя* □	

_____*подпись сотрудника ДИТиС, проводившего разбирательство*_____

Приложение №3

к Правилам осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным Законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и муниципальными правовыми актами в администрации городского округа Тольятти

«УТВЕРЖДАЮ»

Руководитель департамента информационных технологий и связи

_____

«_____» _____ 20_ _г.

Акт № ____ от _____

Разбирательства инцидента информационной безопасности

Сотрудником отдела информационной безопасности _____*должность и Ф.И.О.*

*сотрудника, проводившего разбирательство инцидента ИБ*_____

Проведено разбирательство инцидента ИБ, выявленного _____*дата и орган администрации*

*затронутый инцидентом ИБ*_____

В результате разбирательства установлено:
Сотрудники органа администрации, причастные к инциденту ИБ ___*должность и Ф.И.О.*_____

_____*сотрудников огана администрации, причастных к возникновению инцидента ИБ*_____

Инцидент ИБ _____*описание произошедшего инцидента ИБ*_____

_____

Причины возникновения инцидента _____*причины, по которым стал возможен инцидент ИБ*_____

Ущерб (при наличии), причиненный инцидентом ИБ ___*перечень пострадавших ресурсов(объектов)*___

Действия, предпринятые для ликвидации последствий инцидента ИБ_____

_____описание действий, направленных на ликвидацию последствий инцидента ИБ_____

_____*подпись сотрудника ДИТиС, проводившего разбирательство*_____

_____*подпись ответственного за проведение проверок* ____