



ПОСТАНОВЛЕНИЕ

АДМИНИСТРАЦИИ ГОРОДСКОГО ОКРУГА «ГОРОД ГУБАХА» ПЕРМСКОГО КРАЯ

02.03.2017

№ 236

Об утверждении Правил осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

В целях обеспечения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных руководствуясь Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», 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 и муниципальными органами», Постановлением Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»,

ПОСТАНОВЛЯЮ:

1. Утвердить прилагаемые Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных администрации городского округа «Город Губаха».
2. Опубликовать настоящее постановление в информационно-коммуникационной сети «Интернет» на официальном сайте администрации городского округа «Город Губаха».
3. Контроль за выполнением настоящего постановления возложить на заместителя главы администрации по вопросам организации управления и внутренней политики А.Ю. Самара.

Глава города –
глава администрации

Н.В. Лазейкин

ПРАВИЛА
осуществления внутреннего контроля соответствия обработки
персональных данных требованиям к защите персональных данных

1. Общие положения

Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации городского округа «Город Губаха» (далее - Правила) относятся к основным организационно-распорядительным документам системы документов информационной безопасности администрации городского округа «Город Губаха» (далее – Администрация) и разработаны в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и Постановления Правительства РФ 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».

Целью контроля безопасности режима обработки ПДн в Администрации городского округа «Город Губаха» (далее – Администрация) является определение истинного состояния дел в области защиты ПДн, оценки эффективности принимаемых для исключения утечки ПДн мер, выявления возможных каналов утечки, выработки предложений и рекомендаций руководству Администрации по совершенствованию системы защиты ПДн (СЗПДн). Организация контроля возлагается на Администратора безопасности. В число основных объектов контроля безопасности режима обработки ПДн входят:

- структурные подразделения Администрации городского округа «Город Губаха», привлекаемые к обработке ПДн;
- сотрудники Администрации городского округа «Город Губаха», допущенные в установленном порядке к ПДн, и их носителям, и выполняющие работы с их использованием;
- служебные помещения, в которых проводятся работы с носителями ПДн;

- места непосредственного хранения носителей ПДн (хранилища, сейфы, шкафы);
- непосредственно носители ПДн (документы, материалы, изделия, магнитные носители);
- компоненты информационных систем ПДн (ИСПДн), в которых осуществляется обработка ПДн;
- Локальная сеть Администрации городского округа «Город Губаха».

Особенности контроля безопасности ПДн в отдельных ИСПДн могут регулироваться дополнительными инструкциями и регламентами.

2. Планирование мероприятий по обеспечению и контролю безопасности персональных данных

2.1 Основные цели планирования мероприятий по обеспечению безопасности ПДн:

организация проведения комплекса мероприятий по защите ПДн, направленных на исключение возможных каналов утечки ПДн;

установление персональной ответственности всех должностных лиц Администрации городского округа «Город Губаха» за решение вопросов защиты ПДн в ходе деятельности Администрации;

определение сроков (времени, периода) проведения конкретных мероприятий по защите ПДн;

систематизация (объединение) всех проводимых на плановой основе мероприятий по различным направлениям защиты ПДн;

установление системы контроля за обеспечением защиты ПДн в Администрации, а также системы отчетности о выполнении конкретных мероприятий;

уточнение (конкретизация) функций и задач по защите ПДн, решаемых отдельными должностными лицами и функциональными подразделениями Администрации.

Основой для планирования мероприятий по защите ПДн в Администрации городского округа «Город Губаха» служат:

требования законодательных и иных нормативных правовых актов по защите ПДн;

положения внутренних организационно-распорядительных документов Администрации городского округа «Город Губаха» (приказов, положений, инструкций), определяющих порядок ведения деятельности по защите конфиденциальной информации, а также конкретизирующих вопросы защиты ПДн в Администрации городского округа «Город Губаха»;

результаты комплексного анализа состояния дел в области защиты ПДн, проводимого ответственным сотрудником Администрации;

результаты контроля за состоянием защиты ПДн, проводимого контролирующими органами (Роскомнадзором, правоохранительными органами и т.п.);

результаты проверки вышестоящими учреждениями;

особенности повседневной деятельности Администрации и специфика выполнения в Администрации работ с использованием ПДн.

Планирование мероприятий по обеспечению и контролю безопасности ПДн осуществляется на календарный год, в отдельных случаях могут составляться планы на календарный месяц, неделю, а также на иной определенный срок.

Планы мероприятий по обеспечению безопасности ПДн относятся к конфиденциальным документам, учитываются и хранятся в порядке, установленном для документов соответствующей степени конфиденциальности. Разработка планирующих документов по защите ПДн в Администрации осуществляется сотрудником, ответственным за обеспечение безопасности ПДн в Администрации, в тесном взаимодействии с другими подразделениями (отдельными должностными лицами). Кроме того, при подготовке планов должны учитываться предложения функциональных подразделений Администрации осуществляющих обработку ПДн.

2.2 Структура и основное содержание планов по обеспечению и контролю безопасности ПДн Основным организационно-планирующим документом Администрации в сфере защиты ПДн является План мероприятий по обеспечению безопасности ПДн на календарный год, содержащий необходимый перечень мероприятий для обеспечения защиты ПДн.

План мероприятий по обеспечению безопасности ПДн составляется на основании списка мер, методов и средств защиты, определенных нормативными правовыми актами и методическими документами по защите ПДн, действующими приказами. План мероприятий по обеспечению безопасности ПДн в Администрации на календарный год утверждается главой Администрации до начала календарного года, на который он разработан.

Утвержденный план под роспись доводится до сведения ответственных за проведение и организацию указанных в плане мероприятий в части их касающейся. Типовой план мероприятий по обеспечению безопасности ПДн на календарный год может содержать следующие основные разделы:
1) Организационные (административные) мероприятия, связанные с:

- разработкой организационно-планирующих документов в ходе повседневной деятельности Администрации; подготовкой и изданием

распоряжений Администрации по различным вопросам в сфере защиты ПДн; переработкой и уточнением должностных обязанностей сотрудников и др.;

- подготовкой персонала по вопросам защиты ПДн — организацией и проведением занятий со всеми категориями сотрудников Администрации с учетом специфики выполняемой ими работы; изучением положений нормативно-методических документов в области защиты ПДн и, при необходимости, доведением их требований до сведения сотрудников под роспись; проведением инструктажей с вновь прибывшими или назначенными на должность сотрудниками;

- организацией и ведением конфиденциального делопроизводства в части защиты ПДн — вопросы учета, хранения, размножения и уничтожения носителей ПДн, порядок работы с ними персонала Администрации; мероприятия, непосредственно касающиеся деятельности по рассмотрению запросов субъектов ПДн, а также связанные с работой комиссий по отбору документов и материалов, содержащих ПДн, для уничтожения;

- организацией защиты ПДн при привлечении к обработке ПДн внешних организаций(контрагентов).

2) *Мероприятия по физической защите*, связанные с созданием и совершенствованием системы пропускного режима и физической охраны Администрации городского округа «Город Губаха».

3) *Технические мероприятия*, связанные с защитой ПДн при из обработке в информационных системах персональных даны (ИСПДн) — организационные мероприятия по подготовке и вводу в эксплуатацию объектов информатизации, обрабатывающих ПДн, по технической защите ПДн, защите ПДн от НСД; предотвращению утечки ПДн по каналам связи.

4) *Контролирующие мероприятия*, в том числе связанные с организацией и проведением всех видов проверок состояния защиты ПДн и наличия носителей ПДн. Данный раздел плана предполагает разработку отдельного Плана внутренних проверок режима защиты ПДн. К контролирующим мероприятиям также относится аналитическая работа, связанная с составлением отчетов о состоянии дел в области защиты ПДн.

В План включается следующая информация:

- 1) Наименование мероприятия.
- 2) Периодичность мероприятия (разовое/периодическое).
- 3) Исполнитель мероприятия/ответственный за исполнение.

Контроль за выполнением конкретных мероприятий, включенных в данный план, осуществляется руководителем Администрации. Ответственный сотрудник осуществляют текущий контроль за практической реализацией включенных в план мероприятий и информируют об их выполнении указанные должностных лиц.

3. Организация контроля режима обработки персональных данных в Администрации городского округа «Город Губаха»

Основными задачами контроля режима обработки ПДн являются следующие:

1. сбор, обобщение и анализ информации о состоянии СЗПДн Администрации;
2. анализ состояния дел в области защиты ПДн в функциональных подразделениях Администрации;
3. проверка организации выполнения мероприятий по защите ПДн в функциональных подразделениях Администрации, учета требований по защите ПДн в разрабатываемых плановых и распорядительных документах;
4. выявление угроз безопасности ПДн и выработка мер по их нейтрализации;
5. проверка наличия носителей ПДн;
6. проверка выполнения установленных норм и требований по защите ПДн от утечки по техническим каналам, оценка достаточности и эффективности мероприятий по защите ПДн;
7. оперативное принятие мер по пресечению нарушений требований (норм) защиты ПДн в ИСПДн;
8. разработка предложений по устранению (ослаблению) демаскирующих признаков и технических каналов утечки информации;
9. оказание практической помощи должностным лицам в устранении нарушений требований нормативно-методических документов;
10. применение мер административной и дисциплинарной ответственности к лицам, нарушающим требования по порядку обращения с носителями ПДн;

Основным видом контроля режима обработки ПДн в Администрации являются проверки, подразделяемые на плановые и внеплановые.

Плановые проверки организуются заблаговременно, включаются в соответствующий План внутренних проверок режима защиты ПДн, включающий периодичность проведения внутренних проверок и ответственных исполнителей.

Внеплановые проверки организуются и проводятся при необходимости по указанию Главы Администрации городского округа «Город Губаха» или его заместителей. Они могут проводиться как в масштабах всего, так и в его функциональных подразделениях. Особенность организации таких проверок состоит в том, что они отсутствуют в Планах внутренних проверок режима защиты ПДн.

Алгоритм подготовки и проведения внеплановой проверки следующий:

1) принятие решения о проведении проверки (например, после инцидента безопасности);

2) подготовка перечня проверяемых вопросов;

3) определение ответственных за проведение проверки лиц;

4) определение сроков проверки;

5) непосредственное проведение проверки;

6) оформление результатов работы;

7) выработка предложений и рекомендаций;

8) доклад результатов проверки на месте;

9) анализ недостатков с проверяемыми;

10) доклад результатов лицу, назначившему проверку.

В ходе выполнения проверки осуществляется сопоставление результатов выполнения конкретных мероприятий по обеспечению безопасности ПДн с положениями нормативно-методических документов по защите ПДн и соответствующими стандартами Администрации. При этом проверочные мероприятия подразделяются на проверки режима неавтоматизированной обработки ПДн и обработки ПДн с использованием средств автоматизации.

В проведении проверок участвуют сотрудники ответственных подразделений. Результаты проверки оформляются в виде акта и доводятся до сведения руководителя проверенного структурного подразделения. В данном акте перечисляются выявленные недостатки, а также формулируются предложения по их устранению, повышению эффективности работы должностных лиц (сотрудников) в области защиты ПДн.

Проверяющие лица устанавливают конкретные сроки устранения выявленных недостатков и реализации предложений (рекомендаций). При осуществлении контроля режима обработки ПДн особое внимание уделяется вопросам обращения с носителями ПДн и их хранения в функциональных подразделениях Администрации. Проверяются порядок учета, хранения, размножения (копирования) и уничтожения носителей ПДн; оборудование помещений, в которых хранятся указанные носители или осуществляется работа с ними; порядок передачи носителей одними исполнителями другим, в том числе и при убытии лиц в командировку (отпуск, на лечение) и т.д.

Постоянному контролю подлежат также вопросы допуска и доступа всех категорий должностных лиц к ПДн, в том числе и непосредственно к носителям ПДн, вопросы организации и осуществления пропускного и внутриобъектового режимов в Администрации, организация охраны.

Сотрудник, ответственный за обеспечение безопасности ПДн, организует и ведет учет результатов контроля, всех видов проводимых проверок.

В план внутренних проверок могут быть включены следующие пункты:

1) Контроль соблюдения организационно-режимных требований в помещениях, в которых осуществляется обработка ПДн.

Ежегодно в соответствии с Планом внутренних проверок должна быть проведен контроль соблюдения организационно-режимных требований в помещениях, в которых осуществляется обработка ПДн. Данный вид контроля включает:

- проверку актуальности перечня лиц, имеющих право самостоятельного доступа в помещение;
- проверку корректности расположения мониторов рабочих станций, на которых осуществляется обработка ПДн, исключающего несанкционированный ПДн не допущенными лицами;
- наличие жалюзи на окнах;
- контроль отсутствия конфиденциальных документов, содержащих ПДн, без присмотра на рабочих столах сотрудников;
- контроль сохранности пломб на технических средствах передачи и обработки ПДн, а также на устройствах их защиты;
- и т.п.

2) Контроль доступа к приложениям информационных систем, в которых осуществляется обработка ПДн.

Ежеквартально в целях снижения рисков несанкционированного доступа к информации должен проводиться контроль доступа к приложениям ИСПДн, включающий в себя:

- контроль фактов подачи заявок на блокирование доступа к ИСПДн, в которых осуществляется обработка конфиденциальной информации, увольняемых сотрудников и своевременности подачи таких заявок;
- контроль использования предоставленных прав доступа (в том числе и право удаленного доступа). Если предоставленные права доступа не используются в течение трех и более месяцев, администратор безопасности может инициироваться расследование правомерности подачи заявки на доступ;
- и т.п;

3) Контроль порядка обращения с носителями ПДн.

Ежеквартально ответственным сотрудником должен осуществляться контроль порядка обращения с носителями ПДн, включающий в себя:

- проверку корректности ведения журнала учета машинных носителей и соответствия записей в журнале записям в автоматизированной системе контроля съемных магнитных носителей информации;
- проверку корректности ведения журналов учета конфиденциальных документов в части ПДн;

- и т.п.

4) Проверка выполнения запросов субъектов персональных данных.

Ежеквартально должна проводиться проверка выполнения запросов субъектов ПДн по средствам контроля заполнения и выполнения Журнала учета обращений субъектов ПДн по вопросам обработки ПДн.

5) Контроль нейтрализации выявленных нарушений режима обработки ПДн

Ежеквартально должен осуществляться контроль нейтрализации выявленных нарушений режима обработки ПДн, включающий в себя проверку корректности ведения базы данных инцидентов информационной безопасности, заполнения отчетов об инцидентах, а также все ли обнаруженные инциденты нейтрализованы.

6) Организация анализа и пересмотра имеющихся угроз безопасности ПДн.

Ежегодно на основании анализа произошедших инцидентов информационной безопасности, изменений в условиях обработки ПДн в ИСПДн должна осуществляться корректировка Частных моделей угроз безопасности ПДн при их обработке в ИСПДн, а при необходимости и моделирование новых моделей угроз безопасности ПДн в соответствии с действующими нормативными правовыми актами и методическими документами ФСТЭК и ФСБ России.

7) Поддержание в актуальном состоянии нормативно – правовой базы

Ежегодно проводить актуализацию нормативно-организационных документов по вопросам обеспечения безопасности ПДн в соответствии с:

- изменениями требований законодательных и иных нормативных правовых актов по защите ПДн, отраслевых стандартов;

- результатами анализа состояния дел в области защиты ПДн, проводимого ответственным сотрудником на основании материалов плановых проверок и расследований выявленных инцидентов информационной безопасности;

- результатами контроля за состоянием защиты ПДн, проводимого (Роскомнадзором, правоохранительными органами и т.п.).