Утвержден

постановлением Главы Бабаевского муниципального округа от 05.02.2024 № 5

(Приложение 1)

**ПЛАН МЕРОПРИЯТИЙ**

по обеспечению защиты персональных данных при их обработке  
в органах местного самоуправления Бабаевского муниципального округа  
на 2024 год

г. Бабаево

План мероприятий по обеспечению защиты персональных данных (далее - План), содержит необходимый перечень мероприятий для обеспечения защиты персональных данных в органах местного самоуправления Бабаевского муниципального округа (далее – ОМСУ округа).

План составлен на основании списка мер, методов и средств защиты, определённых в Политике обработки персональных данных в органах местного самоуправления Бабаевского муниципального округа.

Выбор конкретных мероприятий Плана осуществляется по результатам внутренней проверки.

В План включены следующие категории мероприятий:

* организационные (административные);
* физические;
* технические (программные);
* контролирующие.

В План включена следующая информация:

* название мероприятия.
* периодичность мероприятия (разовое/периодическое).
* исполнитель мероприятия/ответственный за исполнение.

ПЛАН МЕРОПРИЯТИЙ

по обеспечению защиты персональных данных при их обработке  
в органах местного самоуправления Бабаевского муниципального округа

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Мероприятие | Периодичность, срок исполнения | Исполнитель/ ответственный | Отметка об исполнении |
| Организационные мероприятия | | | | |
| 1 | Внутренняя проверка текущего состояния системы защиты ПДн в ОМСУ округа | разовое  срок до 01.10.2023 | комиссия по проведению внутренних проверок выполнения требований безопасности ПДн |  |
| 2 | Определение/уточнение обрабатываемых ПДн и  перечня ИСПДн | разовое, при необходимости | ответственные за обработку ПДн |  |
| 3 | Определение круга и ответственности лиц, участвующих в обработке ПДн | периодически  (при возникающих изменениях) | комиссия по проведению внутренних проверок выполнения требований безопасности ПДн |  |
| 4 | Определение прав разграничения доступа пользователей ИСПДн, необходимого для выполнения должностных обязанностей | периодически  (при возникающих изменениях) | комиссия по проведению внутренних проверок выполнения требований безопасности ПДн |  |
| 5 | Организация информирования и доведения до  сотрудников, имеющих доступ к ПДн, изменений в законодательстве РФ о ПДн, локальных актах по вопросам обработки ПДн, требований к защите ПДн | периодически  (по мере появления новых внутренних документов или существенного изменения действующих) | Администратор ИБ, ответственные за обработку ПДн |  |
| 6 | Документальное регламентирование работы с ПДн. Поддержание в актуальном состоянии локальных нормативных правовых актов и документов по ПДн (внесение изменений в положения, правила, перечни, приказы, инструкции и т.д.) | периодически  (при возникающих изменениях) | администратор ИБ, ответственные за обработку ПДн |  |
| 7 | Обеспечение неограниченного доступа к документам, определяющим политику Оператора в отношении обработки ПДн, через публикации на официальном сайте Учреждения локальных нормативных правовых актов | не позднее 10 дней после утверждения документа руководителем | технический специалист |  |
| 8 | Направление в уполномоченный орган (Роскомнадзор) уведомления о внесении изменений в ранее  представленные сведения | при необходимости | администратор ИБ |  |
| 9 | Получение письменных согласий субъектов ПДн на обработку и распространение персональных данных | постоянно | ответственные за обработку ПДн |  |
| 10 | Проведение обучающего инструктажа с сотрудниками, имеющими доступ к ПДн | при необходимости | администратор ИБ, ответственные за обработку ПДн |  |
| 11 | Подготовка отчёта по результатам проведённых в текущем году внутренних проверок и выполнению плана реализации мероприятий по защите персональных данных (ПДн) | декабрь 2024 | администратор ИБ |  |
| 12 | Разработка и утверждение Плана мероприятий по обеспечению защиты ПДн и плана-графика внутренних проверок в структурных подразделениях Учреждения на 2025 год | декабрь 2024 | администратор ИБ |  |
| Физические мероприятия | | | | |
| 1 | Организация пропускного режима в контролируемую зону | постоянно | Ответственные за обработку ПДн |  |
| 2 | Выборочный осмотр рабочих мест пользователей на предмет несанкционированного доступа, нарушения пломб, физического воздействия и внедрения  неучтённых технических средств | еженедельно | администратор ИБ, технический специалист |  |
| Технические (программные) мероприятия | | | | |
| 1 | Установка (обновление) антивирусной защиты | разовое  по окончанию срока лицензии | Технический специалист |  |
| 2 | Контроль над неизменностью настроек средств  антивирусной защиты и своевременным обновлением антивирусных баз | еженедельно | Технический специалист |  |
| 3 | Заведение, удаление учётных записей пользователей. Наделение, лишение, изменение полномочий  пользователей по доступу к ресурсам ИСПДн. | при необходимости | администратор ИБ, технический специалист |  |
| Контролирующие мероприятия | | | | |
| 1 | Контроль актуальности организационно-­распорядительных документов, регламентирующих вопросы защиты информации, в том числе списков лиц, допущенных к обработке ПДн | при существенном изменении законодательства в сфере защиты информации | ответственные за обработку ПДн, администратор ИБ, технический специалист |  |
| 2 | Контроль наличия согласий на обработку и распространение персональных данных субъектов персональных данных, чьи ПДн обрабатываются в ОМСУ округа | 1 раз в год | ответственные за обработку ПДн |  |
| 3 | Контроль наличия соглашений о неразглашении конфиденциальной информации, подписанных  сотрудниками, допущенными к обработке ПДн | 1 раз в год | ответственные за обработку ПДн |  |
| 4 | Проверка мест хранения носителей ПДн: сейфов и металлических шкафов, надёжность их замков;  проверка надёжности замков, установленных в  защищаемых помещениях | постоянно | администратор ИБ; ответственные  за обработку ПДн |  |
| 5 | Контроль соблюдения режима обработки ПДн | постоянно | администратор ИБ; ответственные  за обработку ПДн |  |
| 6 | Контроль соблюдения режима защиты информации | постоянно | администратор ИБ; ответственные  за обработку ПДн |  |
| 7 | Оценка состояния технических и программных средств ИСПДн | 1 раз в квартал | администратор ИБ; технический специалист |  |
| 8 | Контроль над выполнением антивирусной защиты | Еженедельно (оперативный контроль  в процессе информационного  взаимодействия в ИСПДн) | администратор ИБ; технический специалист |  |
| 9 | Контроль соблюдения режима защиты при  подключении к сетям общего пользования и (или) международного обмена | еженедельно  (оперативный контроль  в процессе информационного  взаимодействия в ИСПДн) | администратор ИБ; технический специалист |  |
| 10 | Контроль над обновлениями программного  обеспечения и единообразием применяемого ПО на всех элементах ИСПДн | еженедельно  (оперативный контроль  в процессе информационного  взаимодействия в ИСПДн) | Технический специалист |  |
| 11 | Инвентаризация съёмных электронных носителей  информации, печатей для опечатывания шкафов | Ноябрь 2024 | Технический специалист |  |
| 12 | Контроль за обеспечением резервного копирования | ежемесячно | администратор ИБ; технический специалист |  |
| 14 | Отслеживание объёмов обрабатываемых ПДн, состава обрабатываемых ПДн в ИСПДн, целей обработки ПДн | ежегодно | администратор ИБ; ответственные  за обработку ПДн |  |
| 15 | Внутренние проверки в структурных подразделениях по вопросу текущего состояния защиты ПДн, на предмет выявления изменений в режиме защиты и обработки, обеспечения защиты персональных данных в информационных системах персональных данных, используемых в ОМСУ округа | в течение года по плану-графику (прилагается) | комиссия по проведению внутренних проверок выполнения требований безопасности ПДн, руководители ОМСУ и структурных подразделений |  |

|  |
| --- |
| УТВЕРЖДЕН  постановлением главы Бабаевского муниципального округа  от 05.02.2024 № 5  (Приложение 2) |

ПЛАН-ГРАФИК

внутренних проверок состояния системы защиты персональных данных  
в органах местного самоуправления Бабаевского муниципального округа

на 2024 год

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Мероприятие | | | Исполнитель | |
| проверка текущего состояния системы защиты персональных данных (ПДн) | | | комиссия по проведению внутренних проверок выполнения требований безопасности ПДн | |
| № п/п | структурное подразделение | период проверки | отметка о  выполнении | примечание |
| 1 | Архивный отдел | март |  |  |
| 2 | Управление имущественных и земельных отношений (имущественный отдел) | май |  |  |
| 3 | Отдел опеки и попечительства | сентябрь |  |  |
| 4 | Комитет физической культуры и спорта | ноябрь |  |  |

|  |  |
| --- | --- |
|  | Утверждено  постановлением Главы  Бабаевского  муниципального округа  от 05.02.2024 № 5 (Приложение 3) |
|  | УТВЕРЖДАЮ  Глава Бабаевского муниципального округа \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Ю.В. Парфенов  «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_ 20\_\_ г. |

Заключение

о результатах проверки условий обработки персональных данных в органах местного самоуправления Бабаевского муниципального округа[[1]](#footnote-1)

|  |  |
| --- | --- |
| Наименование органа местного самоуправления |  |
| Номер реестровой записи в Реестре[[2]](#footnote-2) |  |
| Члены комиссии, проводившие проверку[[3]](#footnote-3) | *должность, фамилия, имя, отчество;*  *должность, фамилия, имя, отчество;*  *должность, фамилия, имя, отчество* |
| Даты проведения проверки | С \_\_ \_\_\_\_\_\_\_\_\_\_ 20\_\_ г.  по \_\_ \_\_\_\_\_\_\_\_\_\_ 20\_\_ г. |
| Ответственный за обработку персональных данных | *Фамилия, имя, отчество* |
| Должность ответственного за обработку персональных данных |  |
| Номер служебного телефона ответственного за обработку персональных данных | +7 81743\_\_\_\_\_\_\_ |
| Актуальность сведений в Реестре | *Да/нет* |
| Наличие в Реестре актуальных сведений об ответственном за обработку персональных данных | *Да/нет* |
| Наличие в Реестре актуальных сведений о месте нахождения баз данных информации, содержащих персональные данные граждан Российской Федерации[[4]](#footnote-4) | *Да/нет* |
| Наличие полного комплекта документов, утвержденных актом руководителя в соответствии с подпунктом б) пункта 1 Перечня мер[[5]](#footnote-5) | *Да/нет* |
| Выполнение требований подпункта в) пункта 1 Перечня мер | *Да/нет/не требуется*[[6]](#footnote-6)*.* Результаты оценки эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных винформационных системах персональных данных (ИСПДн)[[7]](#footnote-7) (всего *00* ИСПДн[[8]](#footnote-8))*:* *ИСПДн «наименование» аттестат соответствия от \_\_.\_\_.20\_\_ № \_\_\_\_ (действителен до \_\_.\_\_.20\_\_);* *ИСПДн «наименование» протокол утвержден \_\_.\_\_.20\_\_;* *ИСПДн «наименование» протокол утвержден \_\_.\_\_.20\_\_;*  *«наименование» утвержден \_\_.\_\_.20\_\_* |
| Выполнение требований подпункта г) пункта 1 Перечня мер | *Да/нет* |
| Выполнение требований подпункта д) пункта 1 Перечня мер | \_\_ \_\_\_\_\_\_\_\_\_\_ 20\_\_ г.;  \_\_ \_\_\_\_\_\_\_\_\_\_ 20\_\_ г.;  \_\_ \_\_\_\_\_\_\_\_\_\_ 20\_\_ г.[[9]](#footnote-9) |
| Выполнение требований подпункта е) пункта 1 Перечня мер | *Да/нет* |
| Выполнение требований подпункта з) пункта 1 Перечня мер | *Да/нет/обезличивание не осуществляется* |
| Адрес официального сайта в сети «Интернет» |  |
| Наличие на официальном сайте в сети «Интернет» документов, определяющих политику в отношении обработки персональных данных | *Да (активная ссылка на документы)/нет* |
| Нарушения и замечания, выявленные при проведении проверки с указанием их общего количества |  |
| Меры, необходимые для устранения выявленных нарушений и замечаний |  |

Заключение по результатам проверки условий обработки персональных данных: обработка персональных данных *соответствует*[[10]](#footnote-10)*/не соответствует* Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике *ОМСУ* в отношении обработки персональных данных, локальным актам *ОМСУ.*

|  |  |  |
| --- | --- | --- |
| *Должность*3 | \_\_\_\_\_\_\_\_\_\_\_ | *ФИО* |
|  | (подпись) |  |
| *Должность* | \_\_\_\_\_\_\_\_\_\_\_ | *ФИО* |
|  | (подпись) |  |
| *Должность* | \_\_\_\_\_\_\_\_\_\_\_ | *ФИО* |
|  | (подпись) |  |

|  |  |
| --- | --- |
|  | Утвержден  постановлением Главы  Бабаевского муниципального округа  от 05.02.2024 № 5 (Приложение 4) |
|  | УТВЕРЖДАЮ  Глава Бабаевского муниципального округа  Ю.В. Парфенов  «\_\_\_» \_\_\_\_\_\_\_\_\_\_ 20\_\_ г. |

Акт

оценки вреда субъектам персональных данных

|  |
| --- |
| *Место составления акта* |

Комиссия, созданная на основании распоряжения администрации Бабаевского муниципального округа от *00.00.2024* года № *00*, в составе председателя - \_\_\_\_\_\_\_\_\_\_\_\_\_, членов комиссии - \_\_\_\_\_\_\_\_\_\_\_\_\_\_, руководствуясь Федеральным [законом](consultantplus://offline/ref=99FD8F46D0712B7B45D581AABF0D5921AD1565F3AC54AAEE9EE203BD014A0EE1E2934D6B5AE00B52D45EE5BE4BR6z5M) от 27.07.2006 № 152-ФЗ «О персональных данных», Приказом Роскомнадзора от 28.10.2022 № 178 «Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных»,

составила настоящий акт оценки вреда о нижеследующем:

*Дата составления акта*, комиссия произвела оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» *ОМСУ-оператору*, находящейся по адресу: *000000, область, район, населенный пункт, улица, дом*.

В рамках деятельности по обработке персональных данных *ОМСУ-оператор* *осуществляет распространение персональных данных (указать нарушение).*

По результатам оценки установлено, что степень вреда, который может быть причинен субъектам персональных данных, обрабатываемых *ОМСУ-оператором* *высокая, средняя, низкая[[11]](#footnote-11)* (пп. 2.2 п. 2 Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных», утвержденных Приказом Роскомнадзора от 27.10.2022 N 178).

|  |  |  |
| --- | --- | --- |
| *Должность* | \_\_\_\_\_\_\_\_\_\_\_ | *ФИО* |
|  | (подпись) |  |
| *Должность* | \_\_\_\_\_\_\_\_\_\_\_ | *ФИО* |
|  | (подпись) |  |
| *Должность* | \_\_\_\_\_\_\_\_\_\_\_ | *ФИО* |
|  | (подпись) |  |

1. Проверка условий обработки персональных данных проводится в целях осуществления внутреннего контроля соответствия обработки персональных данных Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора проводится оператором в соответствии с пунктом 4 части 1 статьи 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», подпунктом д пункта 1 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.

   В соответствии с подпунктом б пункта 1 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, актом руководителя ОГВ, ОМСУ утверждаются правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным [законом](consultantplus://offline/ref=D388DDA761954F2600F7750B8771C6EA010E7F3DACF561B17D13638F3371CB84005FAC32CA46B0B1mBpBH) «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами оператора.

   При проведении проверки должны быть установлены, в частности:

   соответствие содержания и объема обрабатываемых персональных данных заявленным целям обработки персональных данных;

   соблюдение точности и при необходимости актуальности обрабатываемых персональных данных;

   соблюдение сроков обработки и хранения персональных данных;

   соблюдение порядка уничтожения персональных данных;

   соблюдение порядка доступа к персональным данным, включая наличие у сотрудников полномочий осуществлять обработку персональных данных либо осуществлять доступ к персональным данным;

   соблюдение порядка доступа сотрудников в помещения, в которых осуществляется обработка, в том числе хранение персональных данных (носителей персональных данных);

   соблюдение требований при обработке персональных данных, осуществляемой неавтоматизированным способом;

   выполнение принимаемых мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных;

   проведение оценки эффективности принимаемых мер по обеспечению безопасности персональных данных в информационных системах персональных данных.

   Проверку рекомендуется проводить не реже одного раза в год. [↑](#footnote-ref-1)
2. Реестр операторов, осуществляющих обработку персональных данных ([https://rkn.gov.ru/personal-data/register](https://rkn.gov.ru/personal-data/register/)). [↑](#footnote-ref-2)
3. Председателем комиссии, которая проводит проверку, должен быть ответственный за организацию обработки персональных данных. [↑](#footnote-ref-3)
4. В Реестре должны быть указаны полные адреса мест нахождения баз данных информации в формате: страна, субъект Российской Федерации, населенный пункт, улица, дом. [↑](#footnote-ref-4)
5. Перечень 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, утвержденный постановлением Правительства Российской Федерации от 21.03.2012 № 211. [↑](#footnote-ref-5)
6. Значение «не требуется» выбирается в случае отсутствия информационных систем персональных данных, оператором которых является соответствующий ОМСУ. [↑](#footnote-ref-6)
7. Оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных проводится оператором информационной системы персональных данных (ОМСУ) для каждой информационной системы персональных данных индивидуально не реже одного раза в 3 года в соответствии с пунктом 17 [требовани](#Par27)й к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 и пунктом 6 [Состава и содержани](#P34)я организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных приказом ФСТЭК России от 18.02.2018 № 21. Оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных для государственных (муниципальных) информационных систем проводится в форме аттестации информационной системы по требованиям защиты информации с привлечением организации, имеющей лицензию на деятельность по технической защите конфиденциальной информации. [↑](#footnote-ref-7)
8. В соответствии с подпунктом б пункта 1 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. [↑](#footnote-ref-8)
9. Указываются даты утверждения заключений о результатах проверок условий обработки персональных данных в ОМСУ за последние 3 года. [↑](#footnote-ref-9)
10. Значение «соответствует» не может быть принято если выбрано хотя бы одно значение, выделенное красным цветом по тексту настоящего документа, а также имеются нарушения и замечания, выявленные при проведении проверки. По итогам разработки документа выделения красным цветом убираются. [↑](#footnote-ref-10)
11. Оператор определяет степень потенциального вреда: высокую, среднюю или низкую.

    Высокая, если: обрабатываются сведения, характеризующие биометрические ПД (физиологические и биологические особенности), которые используются для установления личности; обрабатываются специальные категории ПД (национальная принадлежность, состояние здоровья, сведения о судимости и др.); производится обработка данных несовершеннолетних лиц для договоров, в которых они являются контрагентами, поручителями или выгодоприобретателями; персональных данные обезличиваются; обработка ПД россиян осуществляется иностранным лицом; осуществляется сбор данных с использованием баз за границей.

    Средняя в случаях: распространение ПД в интернете или их предоставление неограниченному кругу лиц; если данные обрабатываются в целях, которые отличаются от первоначальных; когда согласие на обработку персональных данных получено на сайте в интернете; продвижения товаров (услуг) с использованием базы потребителей, которой владеет другой оператор.

    Низкая при условии: ведения источников персональных данных, которые являются общедоступными (адресные книги или справочники). Сведения в такие источники включаются с письменного согласия субъекта (ст. 8 закона от 27.07.2006 № 152-ФЗ); назначения ответственным за обработку внештатного сотрудника. [↑](#footnote-ref-11)