ПРИЛОЖЕНИЕ № 1

к положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных администрации муниципального района «Мещовский район»

от «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г.

План мероприятий по защите персональных данных

в Администрации муниципального района «Мещовский район»

| № п\п | Наименование мероприятия | Срок выполнения | Примечание |
| --- | --- | --- | --- |
|  | Документальное регламентирование работы с ПДн | При необходимости | Разработка организационно-распорядительных документов по защите ПДн, либо внесение изменений в существующие |
|  | Получение согласий субъектов ПДн (физических лиц) на обработку ПДн в случаях, когда этого требует законодательство | Постоянно | В случаях, предусмотренных Федеральным законом «О персональных данных», обработка ПДн осуществляется только с согласия в письменной форме субъекта ПДн. Форма согласия приведена в Распоряжении «Об утверждении форм документов, необходимых в целях выполнения требований законодательства в области персональных данных». Равнозначным содержащему собственноручную подпись субъекта ПДн согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью |
|  | Пересмотр договора с третьими лицами на поручение обработки ПДн | При необходимости | В случае поручения обработки ПДн субъектов ПДн третьим лицам (например, кредитно-финансовым учреждениям) в договор включается пункт о соблюдении конфиденциальности при обработке ПДн, а также учитываются требования ч.3 ст.6 Федерального закона «О персональных данных» |
|  | Ограничение доступа сотрудников к ПДн | При необходимости (при создании ИСПДн) | В случае создания ИСПДн, а также приведения имеющихся ИСПДн в соответствие с требованиями закона необходимо разграничить доступ сотрудников Оператора к ПДн |
|  | Взаимодействие с субъектами ПДн | Постоянно | Работа с обращениями субъектов ПДн, ведение журналов учета передачи персональных данных, обращений субъектов ПДн, уведомление субъектов ПДн об уничтожении, изменении, прекращении обработки, устранении нарушений, допущенных при обработке ПДн, получении ПДн от третьих лиц |
|  | Ведение журналов учета отчуждаемых электронных носителей персональных данных, средств защиты информации | Постоянно |  |
|  | Повышение квалификации сотрудников в области защиты ПДн | Постоянно | Повышение квалификации сотрудников, ответственных за выполнение работ – не менее раза в три года, повышение осведомленности сотрудников – постоянно (данное обучение проводит ответственный за обеспечение безопасностиПДн в ИСПДн) |
|  | Инвентаризация информационных ресурсов | Раз в полгода | Проводится с целью выявления в информационных ресурсах присутствия ПДн |
|  | Установка сроков обработки ПДн и процедуры их уничтожения по окончании срока обработки | При необходимости | Для ПДнОператором устанавливаются сроки обработки ПДн, которые документально подтверждаются в нормативных документах Оператора. При пересмотре сроков необходимые изменения вносятся в соответствующие документы |
|  | Уничтожение электронных (бумажных) носителей информации при достижении целей обработки ПДн | При необходимости | Уничтожение электронных (бумажных) носителей информации при достижении целей обработки ПДн производится с оформлением Акта на списание и уничтожение электронных (бумажных) носителей информации. Форма соответствующего акта приведена в Распоряжении «Об утверждении форм документов, необходимых в целях выполнения требований законодательства в области персональных данных» |
|  | Определение уровня защищенности ПДн при их обработке в ИСПДн | При необходимости | Определение уровня защищенности ПДн при их обработке в ИСПДн осуществляется при создании ИСПДн, при изменении состава ПДн, объема обрабатываемых ПДн, субъектов ПДн |
|  | Выявление угроз безопасности и разработка моделей угроз и нарушителя | При необходимости | Разрабатывается при создании системы защиты ИСПДн |
|  | Аттестация ИСПДн на соответствие требованиям по обеспечению безопасности ПДн | При необходимости | Проводится совместно с лицензиатами ФСТЭК |
|  | Эксплуатация ИСПДн и контроль безопасности ПДн | Постоянно |  |
|  | Понижение требований по защите ПДн путем сегментирования ИСПДн, отключения от сетей общего пользования, обеспечения обмена между ИСПДн с помощью сменных носителей, создания автономных ИСПДн на выделенных АРМ и прочих доступных мер | При необходимости | В случае создания ИСПДн, а также приведения имеющихся ИСПДн в соответствии с требованиями закона |

ПРИЛОЖЕНИЕ № 2

к положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных администрации муниципального района «Мещовский район»

от «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г.

План внутренних проверок режима обработки и защиты персональных данных

вАдминистрации муниципального района «Мещовский район»

|  |  |  |  |
| --- | --- | --- | --- |
| № | Мероприятие | Периодичность | Дата, подпись исполнителя |
|  | Организация анализа и пересмотра имеющихся угроз безопасности ПДн, а также предсказание появления новых, еще неизвестных, угроз | Ежегодно |  |
|  | Проверка применения для обеспечения безопасности ПДн средств защиты информации, прошедших в установленном порядке процедуру соответствия | Раз в полгода |  |
|  | Контроль учета машинных носителей ПДн | Раз в полгода |  |
|  | Контроль за принимаемыми мерами по обеспечению безопасности ПДн и уровня защищенности ПДн в ИСПДн | Раз в полгода |  |
|  | Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в ИСПДн | Ежеквартально |  |
|  | Контроль внесения изменений в структурно-функциональные характеристики ИСПДн | Ежеквартально |  |
|  | Контроль корректности настроек средств защиты информации | Раз в полгода |  |
|  | Контроль за обеспечением резервного копирования | Ежеквартально |  |
|  | Поддержание в актуальном состоянии организационно-распорядительных документов по вопросам защиты ПДн | Раз в полгода |  |
|  | Осуществление внутреннего контроля и (или) аудита соответствия обработки ПДн ФЗ-152 «О персональных данных» и принятым в соответствии с ним нормативным правовым актам | Раз в полгода |  |
|  | Проверка ознакомления сотрудников, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн, в том числе требованиями к защите ПДн | Раз в полгода |  |
|  | Проверка получения согласий субъектов ПДн на обработку ПДн в случаях, когда этого требует законодательство | Раз в полгода |  |
|  | Проверка подписания сотрудниками, осуществляющими обработку ПДн, основных форм, необходимых в целях выполнения требований законодательства в сфере обработки и защиты ПДн:  - Уведомления о факте обработки ПДн без использования средств автоматизации;  - Обязательства о соблюдении конфиденциальности ПДн;  - Формы ознакомления с положениями законодательства Российской Федерации о ПДн, локальными актами Администрации муниципального района «Мещовский район» по вопросам обработки ПДн;  - Типового обязательства о прекращении обработки ПДн в случае расторжения служебного контракта (трудового договора);  - Разъяснения субъекту ПДн юридических последствий отказа предоставить свои ПДн | Раз в полгода |  |
|  | Проверка уничтожения материальных носителей ПДн с составлением соответствующего акта | Ежегодно |  |
|  | Проверка ведения журналов по учету обращений субъектов ПДн и учету передачи ПДн субъектов третьим лицам | Раз в полгода |  |
|  | Проведение внутренних проверок на предмет выявления изменений в правилах обработки и защиты ПДн | Ежегодно |  |
|  | Проверка соблюдения условий хранения материальных носителей ПДн | Раз в полгода |  |
|  | Проверка состояния актуальности Уведомления об обработке (намерении осуществлять обработку) ПДн | Раз в полгода |  |
|  | Поддержание в актуальном состоянии организационно-распорядительных документов по вопросам обработки ПДн, в том числе документов, определяющих политику Администрации муниципального района «Мещовский район» в отношении обработки ПДн | Раз в полгода |  |
|  | Оценка вреда, который может быть причинен субъектам ПДн в случае нарушения ФЗ-152 «О персональных данных» | Ежегодно |  |
|  | Оценка эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн | При необходимости |  |

ПРИЛОЖЕНИЕ № 3

к положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных администрации муниципального района «Мещовский район»

от «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г.

**Отчет о результатах проведения внутренней проверкирежима обработки и защиты персональных данных в Администрации муниципального района «Мещовский район»**

1. Внутренняя проверка произведена на основании Положения по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Администрации муниципального района «Мещовский район» от «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г.
2. Проверка проводилась «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_ г. по адресу:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. В ходе проверки были проведены следующие мероприятия:
2. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
3. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
4. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
5. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
6. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
7. Результаты проведения проверки:
8. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
9. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
10. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
11. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
12. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
13. Необходимые мероприятия.

На основании проведения внутренней проверки режима обработки и защиты ПДн рекомендуется осуществить следующие мероприятия:

1. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
2. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
3. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
4. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
5. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Подписи ответственных лиц, проводивших внутреннюю проверку режима обработки и защиты ПДн:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
| (дата) |  | (подпись) |  | (расшифровка подписи) |
|  |  |  |  |  |
| (дата) |  | (подпись) |  | (расшифровка подписи) |
|  |  |  |  |  |
| (дата) |  | (подпись) |  | (расшифровка подписи) |