|  |  |  |
| --- | --- | --- |
| ИСПОЛНИТЕЛЬНЫЙ КОМИТЕТАЛЕКСЕЕВСКОГО МУНИЦИПАЛЬНОГО РАЙОНАРЕСПУБЛИКИ ТАТАРСТАН | герб2серый | ТАТАРСТАН РЕСПУБЛИКАСЫ АЛЕКСЕЕВСКМУНИЦИПАЛЬ РАЙОНЫНЫҢ БАШКАРМА КОМИТЕТЫ  |
|  ПОСТАНОВЛЕНИЕ23.06.2020 | п.г.т.Алексеевское |  КАРАР№ 223 |

**Об утверждении регламента проведения**

**внутреннего контроля соответствия**

**обработки персональных данных**

**требованиям к защите**

**персональных данных**

Во исполнение требований Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных» и прочих нормативных документов по защите информации,

**постановляю**:

1. Утвердить и ввести в действие Регламент проведения внутреннего контроля соответствия обработки персональных данных в Исполнительном комитете Алексеевского муниципального района Республики Татарстан требованиям к защите персональных данных (далее – Регламент) (Приложение).
2. Требования Регламента довести до работников, непосредственно осуществляющих защиту персональных данных.
3. Контроль за исполнением настоящего постановления оставляю за собой.

**Руководитель**

**Исполнительного комитета Н.К.Кадыров**

Приложение

к постановлению

Исполнительного комитета

Алексеевского муниципального

района Республики Татарстан

от 23.06.2020 № 223

**РЕГЛАМЕНТ**

**проведения внутреннего контроля соответствия обработки персональных данных в Исполнительном комитете Алексеевского муниципального района Республики Татарстан требованиям к защите персональных данных**

1. **Основные термины и определения**

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

Инцидент информационной безопасности – любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность. Инцидентами информационной безопасности являются:

* утрата услуг, оборудования или устройств;
* системные сбои или перегрузки;
* ошибки пользователей;
* несоблюдение политики или рекомендаций по информационной безопасности;
* нарушение физических мер защиты;
* неконтролируемые изменения систем;
* сбои программного обеспечения и отказы технических средств;
* нарушение правил доступа.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

Средство защиты информации – программное обеспечение, программно-аппаратное обеспечение, аппаратное обеспечение, вещество или материал, предназначенное или используемое для защиты информации.

1. **Общие положения**
2. Настоящий Регламент проведения внутреннего контроля соответствия обработки персональных данных в Исполнительном комитете Алексеевского муниципального района Республики Татарстан требованиям к защите персональных данных (далее – Регламент), разработан в соответствии с законодательством Российской Федерации о персональных данных (далее – ПДн) и нормативными правовыми актами (методическими документами) федеральных органов исполнительной власти по вопросам безопасности ПДн при их обработке в информационных системах персональных данных (далее – ИСПДн).
3. Настоящий Регламент определяет порядок проведения внутреннего контроля соответствия обработки ПДн (далее – Внутренний контроль), требованиям к защите ПДн.
4. Регламент обязателен для исполнения всеми работниками Исполнительного комитета Алексеевского муниципального района Республики Татарстан (далее – Исполком), непосредственно осуществляющими защиту ПДн.
5. **Порядок проведения внутреннего контроля**
6. Для проведения внутреннего контроля в ИСПДн постановлением Исполнительного комитета создаётся комиссия, состоящая не менее чем из трех человек с обязательным включением в её состав:
* ответственного за обеспечение безопасности ПДн в ИСПДн;
* ответственного за организацию обработки ПДн в Комитете.
1. Председатель комиссии организует работу комиссии, решает вопросы взаимодействия комиссии с руководителями и работниками Исполкома, готовит и ведёт заседания комиссии, подписывает протоколы заседаний. По окончании работы комиссии готовится заключение по результатам внутреннего контроля, которое передается на рассмотрение Руководителю Комитета.
2. Внутренний контроль проводится в соответствии с «Планом проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных», утвержденным приказом Руководителя Комитета, форма которого установлена в Приложении 1 к настоящему Регламенту.
3. В «Плане проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных» указывается перечень проводимых мероприятий внутреннего контроля и периодичность их проведения.
4. Комиссия проводит внутренний контроль непосредственно на месте обработки ПДн, опрашивает работников Исполкома, осуществляющих обработку ПДн, осматривает рабочие места.
5. В ходе проведения внутреннего контроля осуществляется:
* контроль выполнения организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн, необходимых для выполнения требований к защите ПДн;
* анализ изменения угроз безопасности ПДн в ИСПДн, возникающих в ходе ее эксплуатации;
* проверка параметров настройки и правильности функционирования программного обеспечения и средств защиты информации (далее – СЗИ);
* контроль состава технических средств, программного обеспечения и СЗИ;
* состояние учета СЗИ;
* состояние учета средств шифровальной (криптографической) защиты информации;
* состояние учета съемных машинных носителей ПДн;
* соблюдение правил доступа к ПДн;
* контроль наличия (отсутствия) фактов несанкционированного доступа к ПДн;
* соблюдение пользователями ИСПДн парольной политики;
* соблюдение пользователями ИСПДн антивирусной политики;
* соблюдение пользователями ИСПДн правил работы со съемными машинными носителями ПДн.
1. В целях проведения внутреннего контроля все работники Комитета обязаны по первому требованию членов комиссии предъявить для проверки все числящиеся за ними материалы и документы, дать устные или письменные объяснения по существу заданных им вопросов.
2. По завершении внутреннего контроля комиссией составляется «Акт о проведении контроля соответствия обработки персональных данных», форма которого установлена в Приложении 2 к настоящему Регламенту.
3. В «Акте о проведении контроля соответствия обработки персональных данных» указываются:
* перечень проведенных мероприятий;
* выявленные нарушения;
* мероприятия по устранению нарушений;
* решения по результатам внутреннего контроля;
* сроки устранения нарушений.
1. Периодичность проведения внутреннего контроля составляет не реже 1 раза в год.
2. Предложения о создании комиссии и о плановом/внеплановом проведении внутреннего контроля представляются Руководителю Исполкома Ответственным за организацию обработки ПДн и Ответственным за обеспечение безопасности ПДн в ИСПДн.
3. **Ответственность**
	1. Ответственный за организацию обработки ПДн в Исполнительном комитете несет ответственность за организацию проведения внутреннего контроля соответствия обработки ПДн в Комитете требованиям к защите ПДн.
4. **срок действия и порядок внесения изменений**
	1. Настоящий Регламент вступает в силу с момента его утверждения и действует бессрочно, до замены новым Регламентом.
	2. Настоящий Регламент подлежит пересмотру не реже одного раза в три года.
	3. Изменения и дополнения в настоящий Регламент вносятся постановлением Исполнительного комитета.

**Управляющий делами**

**Исполнительного комитета Г.А.Юсупова**

Приложение 1

к Регламенту проведения внутреннего контроля соответствия обработки персональных данных в Исполнительном комитете Алексеевского муниципального района Республики Татарстан требованиям к защите персональных данных

**ФОРМА**

**План проведения внутреннего контроля**

**соответствия обработки персональных данных**

**в Исполнительном комитете Алексеевского муниципального района Республики Татарстан**

| № п/п | Мероприятие | Регулярность проведения |
| --- | --- | --- |
|  | Анализ актуальности локальных нормативных актов (внутренних документов) по вопросам обеспечения безопасности персональных данных: * Проверка соответствия локальных нормативных актов (внутренних документов) по вопросам обеспечения безопасности персональных данных действующему законодательству РФ по защите персональных данных;
* Учет в локальных нормативных актах (внутренних документах) по вопросам обеспечения безопасности персональных данных изменений в деятельности Исполнительного комитета Алексеевского муниципального района Республики Татарстан по обработке и защите персональных данных.
 | 1 раз в три года или по мере обновления законодательства РФ |
|  | Проверка ознакомления работников с положениями законодательства РФ по защите персональных данных, документами, определяющими политику Исполнительного комитета Алексеевского муниципального района Республики Татарстан в отношении обработки персональных данных и организационно-распорядительными документами по вопросам персональных данных. | 1 раз в год |
|  | Проверка выполнения работниками – пользователями информационных систем персональных данных инструкций по эксплуатации информационных систем персональных данных, положения о разрешительной системе доступа. | 1 раз в год |
|  | Проверка актуальности прав разграничения доступа пользователей информационных систем персональных данных, необходимых для выполнения должностных обязанностей. | 1 раз в год |
|  | Проверка актуальности определенных угроз безопасности персональных данных для информационных систем персональных данных. | 1 раз в год |
|  | Проверка полноты реализованных технических мер по обеспечению безопасности персональных данных в информационных системах персональных данных с учетом структурно-функциональных характеристик информационных системах персональных данных, информационных технологий, особенностей функционирования информационных системах персональных данных. | 1 раз в год |
|  | Проверка наличия сертифицированных средств защиты информации, в случаях, когда применение таких средств необходимо для нейтрализации актуальных угроз безопасности персональных данных. | 1 раз в год |
|  | Проверка правил обращения со съемными машинными носителями персональных данных. | 1 раз в год |
|  | Проверка актуальности информации, содержащейся в Уведомлении об обработке персональных данных, предоставленной в Роскомнадзор. | 1 раз в год |
|  | Проверка соответствия условий использования средств криптографической защиты условиям, предусмотренным эксплуатационной и технической документацией к ним. | 1 раз в год |
|  | Выявление уязвимостей в информационных системах персональных данных в т.ч. в системе защиты с использованием средства инструментального анализа защищенности. | 1 раз в год |

Приложение 2

к Регламенту проведения внутреннего контроля соответствия обработки персональных данных в Исполнительном комитете Алексеевского муниципального района Республики Татарстан требованиям к защите персональных данных

**ФОРМА**

**АКТ**

|  |  |  |  |
| --- | --- | --- | --- |
|  | «\_\_\_» \_\_\_\_\_\_\_\_\_\_ 20\_\_ г. |  | № \_\_\_\_\_\_\_\_\_\_\_\_ |
| Алексеевское |

О проведении контроля соответствия обработки

персональных данных

Комиссия в составе:

Председатель:

|  |  |  |
| --- | --- | --- |
|  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

Члены комиссии:

|  |  |  |
| --- | --- | --- |
|  | 1. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  | 2. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  | 3. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

составила настоящий акт о том, что комиссией были проведены мероприятия по контролю соответствия обработки персональных данных в Исполнительном комитете Алексеевского муниципального района Республики Татарстан требованиям к защите персональных данных. Результат проведенного внутреннего контроля отражен в Таблице 1.

Таблица 1

| № п/п | Мероприятие | Выявленные недостатки | Мероприятия по устранению недостатков | Срок проведения мероприятий | Ответственное лицо |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Внутренний контроль проводился в соответствии с «Регламентом проведения внутреннего контроля соответствия обработки персональных данных в Исполнительном комитете Алексеевского муниципального района Республики Татарстан требованиям к защите персональных данных».

|  |  |  |
| --- | --- | --- |
| Председатель: |  |  |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Члены комиссии: |  |  |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  |  |  |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  |  |  |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

ЛИСТ ОЗНАКОМЛЕНИЯ

с приказом Исполнительного комитета Алексеевского муниципального района Республики Татарстан от «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 2020 г. № \_\_\_\_\_\_

«Об утверждении регламента проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных»

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № п/п | Фамилия имя отчество | Должность | Дата ознакомления | Подпись |
| 1 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  |
| 2 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  |
| 3 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  |
| 4 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  |
| 5 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  |
| 6 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  |
| 7 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  |
| 8 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  |
| 9 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  |
| 10 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  |
| 11 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  |
| 12 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  |
| 13 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  |
| 14 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  |
| 15 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  |
| 16 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  |
| 17 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  |
| 18 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  |
| 19 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  |
| 20 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  |