Приложение 1

к приказу МБУ ДО «Рыбновская ДЮСШ»

от «12» апреля 2021 г. О- № 34

**РЕГЛАМЕНТ**

**проведения внутреннего контроля соответствия обработки персональных данных в МБУ ДО «Рыбновская ДЮСШ» 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. **3Общие положения**
2. Настоящий Регламент проведения внутреннего контроля соответствия обработки персональных данных в МБУ ДО «Рыбновская ДЮСШ» 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 МБУ ДО «Рыбновская ДЮСШ» (далее – Учреждение), непосредственно осуществляющими защиту ПДн.
5. **Порядок проведения внутреннего контроля**
6. Для проведения внутреннего контроля в ИСПДн приказом Директора Учреждения 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 Учреждении.

1. Председатель комиссии организует работу комиссии, решает вопросы взаимодействия комиссии с руководителями и работниками Учреждения, готовит и ведёт заседания комиссии, подписывает протоколы заседаний. По окончании работы комиссии готовится заключение по результатам внутреннего контроля, которое передается на рассмотрение Директору Учреждения.
2. Внутренний контроль проводится в соответствии с «Планом проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных», утвержденным приказом директора Учреждения, 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 Учреждения, 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 Учреждения 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 Директору Учреждения Ответственным за организацию обработки ПДн и Ответственным за обеспечение безопасности ПДн в ИСПДн.
3. **Ответственность**
   1. Ответственный за организацию обработки ПДн в Учреждении несет ответственность за организацию проведения внутреннего контроля соответствия обработки ПДн в Учреждении 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 приказом директора Учреждения.

Приложение 1

к Регламенту проведения внутреннего контроля соответствия обработки персональных данных в МБУ ДО «Рыбновская ДЮСШ» требованиям к защите персональных данных

**ФОРМА**

**План проведения внутреннего контроля**

**соответствия обработки персональных данных**

**в МБУ ДО «Рыбновская ДЮСШ»**

| № 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 МБУ ДО «Рыбновская ДЮСШ» 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 МБУ ДО «Рыбновская ДЮСШ» 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 |
|  | 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 МБУ ДО «Рыбновская ДЮСШ»требованиям к защите персональных данных

**ФОРМА**

**АКТ**

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

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 МБУ ДО «Рыбновская ДЮСШ» 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 МБУ ДО «Рыбновская ДЮСШ» требованиям к защите персональных данных».

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