Приложение
к приказу директора
ГАУК НСО НГОДНТ
от «27» октября 2023 г. № 286о/д

Сведения о реализуемых требованиях к защите персональных данных в Государственном автономном учреждении культуры Новосибирской области «Новосибирский государственный областной Дом народного творчества»

Защита персональных данных, обрабатываемых ГАУК НСО НГОДНТ (далее - Учреждение) обеспечивается реализацией правовых, организационных и технических мер, необходимых и достаточных для обеспечения требований законодательства в области защиты персональных данных.

1. **Правовые меры включают в себя:**

- разработку локальных актов Учреждения, реализующих требования российского законодательства, в том числе Политики в отношении обработки персональных данных, и размещение ее на сайте Учреждения;
- реализация требований о соблюдении конфиденциальности персональных данных;
- реализация требований об обеспечении реализации субъектом персональных данных своих прав, включая право на доступ к информации;
- реализация требований к защите персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных;
- реализация иных требований законодательства Российской Федерации;
- отказ от любых способов обработки персональных данных, не соответствующих целям, заранее предопределенным Учреждением.

2. **Организационные меры включают в себя:**

- назначение лица, ответственного за организацию обработки персональных данных;
- назначение лица, ответственного за обеспечение безопасности персональных данных в информационных системах;
- ограничение числа работников Учреждения, имеющих доступ к персональным данным и организацию разрешительной системы доступа к ним;
- ознакомление работников Учреждения с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, с локальными актами Учреждения по вопросам обработки персональных данных, обучение указанных работников;
- определение в должностных инструкциях работников Учреждения обязанностей по обеспечению безопасности обработки персональных данных и ответственности за нарушение установленного порядка;
- регламентацию процессов обработки персональных данных;
- организацию учёта материальных носителей персональных данных и их хранения, обеспечивающих предотвращение хищения, подмены, несанкционированного копирования и уничтожения;
- определение угроз безопасности персональных данных при их обработке в информационных системах, формирование на их основе моделей угроз;

- введение режима безопасности обработки и обращения с персональными данными, размещение технических средств обработки персональных данных в пределах охраняемой территории;
- ограничение допуска посторонних лиц в помещения Учреждения, недопущение их нахождения в помещениях, где ведется работа с персональными данными и размещаются технические средства их обработки, без контроля со стороны работников Учреждения.

3. **Технические меры включают в себя:**
- определение типа угроз безопасности персональных данных, актуальных для информационных систем персональных данных с учетом оценки возможного вреда субъектам персональных данных, который может быть причинен в случае нарушения требований безопасности, определение уровня защищенности персональных данных и реализация требований к защите персональных данных при их обработке в информационных системах, исполнение которых обеспечивают установленные уровни защищенности персональных данных;
- разработку на основе модели угроз системы защиты персональных данных для установленных Правительством Российской Федерации уровней защищенности персональных данных при их обработке в информационных системах;
- использование для нейтрализации актуальных угроз средств защиты информации, прошедших процедуру оценки соответствия;
- оценку эффективности принимаемых мер по обеспечению безопасности персональных данных;
- реализацию системы разграничения доступа работников к информации, содержащей персональные данные, обрабатываемой в информационных системах, и программно-аппаратным и программным средствам защиты информации;
- регистрацию и учёт действий с персональными данными пользователей информационных систем, где обрабатываются персональные данные;
- выявление вредоносного программного обеспечения (применение антивирусных программ) на всех узлах информационной сети Учреждения, обеспечивающих соответствующую техническую возможность;
- безопасное межсетевое взаимодействие (применение межсетевого экранирования);
- передача информации с использованием информационно - телекоммуникационных сетей осуществляется при помощи средств криптографической защиты информации;
- обнаружение вторжений в информационную систему Учреждения, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности персональных данных;
- регулярное резервное копирование информации и баз данных, содержащих персональные данные субъектов персональных данных;
- периодическое проведение мониторинга действий пользователей, разбирательств по фактам нарушения требований безопасности персональных данных;
- регулярные проверки соответствия системы защиты персональных данных, аудит уровня защищенности персональных данных в информационных системах персональных данных, функционирования средств защиты информации, выявления изменений в режиме обработки и защиты персональных данных.