Приложение № 1
к приказу
от «21» 12. 2017 г. № 62

Правила
осуществления внутреннего контроля соответствия организации обработки и защиты персональных данных требованиям законодательства в МБОУ ДО «Гавриловская школа искусств»

1. Общие положения

Правила осуществления внутреннего контроля соответствия организации обработки и защиты персональных данных требованиям законодательства в МБОУ ДО «Гавриловская школа искусств»
(далее – Правила) определяют план и порядок проведения внутренних проверок организации обработки и защиты персональных данных при их обработке в информационных системах персональных данных (далее – ИСПДн) МБОУ ДО «Гавриловская школа искусств»

1.1 .

Целью внутренних проверок является определение соответствия организации обработки и защиты персональных данных субъектов действующему законодательству РФ, а также локальным актам МБОУ ДО «Гавриловская школа искусств»

1.2 по защите персональных данных.

1.3 Основные понятия, используемые в настоящих Правилах, соответствуют основным понятиям, установленным Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных».

2. План проведения внутренних проверок

2.1 План содержит перечень внутренних проверок и определяет для каждой из них:

- название проверки;
- периодичность проведения проверки;
- методику (программу) проверки
- ответственного исполнителя.

Внутренние проверки проводятся в МБОУ ДО «Гавриловская школа искусств»

2.2 .

2.3 Общий срок проведения проверки не должен превышать 30 рабочих дней.

2.4 Информация о проведенной проверке, дата ее начала и окончания, а также ее результаты, фиксируются в «Журнале периодического тестирования средств защиты информации» и, при необходимости, в «Журнале учета нештатных ситуаций ИСПДн, выполнения профилактических работ, установки и модификации программных средств на АРМ ИСПДн».

2.5 План проведения внутренних проверок приведен в Приложении к настоящим Правилам.

3. Порядок проведения внутренних проверок

3.1. Порядок проведения контроля установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации.

В ходе проведения проверки необходимо:

3.1.1 Проверить соответствие версий общесистемного, прикладного и специального программного обеспечения, включая программное обеспечение средств защиты информации.

3.1.2 Проверить наличие отметок в эксплуатационной документации (формуляр, паспорт) об установке (применении) обновлений.

3.2 Порядок проведения контроля работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации

В ходе проведения проверки необходимо:

3.2.1 Проверить работоспособность (неотключение) программного обеспечения и средств защиты информации.

3.2.2 Проверить правильность функционирования (тестирование на тестовых данных, приводящих к известному результату) программного обеспечения и средств защиты информации.

3.2.3 Проверить соответствие настроек программного обеспечения и средств защиты информации параметрам настройки, приведенным в эксплуатационной документации на систему защиты информации и средства защиты информации.

3.2.4 В случае возникновения необходимости восстановить работоспособность, правильное функционирование, а также параметры настройки программного обеспечения и средств защиты информации, в том числе с использованием резервных копий и (или) дистрибутивов.

3.3 Порядок проведения контроля состава технических средств, программного обеспечения и средств защиты информации

В ходе проведения проверки необходимо:

Проверить соответствие состава программного обеспечения, технических средств и средств защиты информации приведенному в локальных документах МБОУ ДО «Гавриловская школа искусств»

3.3.1 и эксплуатационной документации.

3.3.2 Исключить из состава информационной системы несанкционированно установленные (удаленные) технические средства, программное обеспечение и средства защиты информации.

3.3.3 Проверить выполнение условий и сроков действия сертификатов соответствия на средства защиты информации

3.3.4 В случае возникновения необходимости принять меры, направленные на устранения выявленных недостатков.

3.4 Порядок проведения контроля правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в ИСПДн

В ходе проведения проверки необходимо:

3.4.1 Проверить соблюдение пользователями и ответственными лицами правил генерации и смены паролей пользователей.

Проверить соответствие заведенных и удаленных учетных записей пользователей локальным документам МБОУ ДО «Гавриловская школа искусств»

3.4.2 .

3.4.3 Осуществить проверку реализации правил разграничения доступа и полномочий пользователей в соответствии с утвержденной матрицей доступа.

3.4.4 Провести контроль наличия документов, подтверждающих разрешение изменения учетных записей пользователей, их параметров, правил разграничения доступа, установленных

полномочий пользователей.

3.4.5 В случае возникновения необходимости принять меры, направленные на устранения выявленных недостатков.

3.5 Порядок проведения проверки соблюдения режима защиты персональных данных при их обработке в ИСПДн

В ходе проведения проверки необходимо:

3.5.1 Определить соблюдают ли работники, участвующие в процессе обработки персональных данных в информационной системе персональных данных, принятые меры по обеспечению безопасности персональных данных.

3.5.2 Произвести контроль над соблюдением режима защиты при подключении к сетям общего пользования и (или) международного обмена.

3.5.3 Осуществить проверку наличия машинных носителей персональных данных.

3.5.4 Проверить наличие и ведение журналов, используемых для контроля (анализа) защищенности персональных данных.

3.5.5 Произвести контроль над выполнением резервного копирования и архивирования информации ограниченного доступа.

3.6 Порядок проведения анализа и пересмотра существующих мер по обеспечению безопасности персональных данных в ИСПДн

В ходе проведения проверки необходимо:

3.6.1 Определить изменения в базовой конфигурации информационной системы, проверить наличие данных о внесении изменений в документацию на систему защиты информации информационной системы персональных данных.

3.6.2 Провести анализ произведенных изменений на предмет возникновения дополнительных угроз безопасности персональных данных в информационной системе персональных данных.

3.6.3 В случае выявления новых источников угроз провести уточнение и дополнение модели угроз безопасности.

3.6.4 Провести соотношение выявленных угроз информационной безопасности с реализованными мерами по обеспечению безопасности персональных данных, в случае необходимости применить дополнительные меры по обеспечению безопасности.

3.6.5 По результатам анализа изменённой модели угроз и выбора необходимых дополнительных мер по обеспечению безопасности – принять решение об обновлении либо модернизации системы защиты информации.

3.6.6 Принять решение о необходимости переаттестации информационной системы персональных данных или проведении дополнительных аттестационных испытаний.

3.7 Порядок проведения проверки наличия и актуальности внутренней нормативной документации по защите персональных данных

В ходе проведения проверки необходимо:

Проверить наличие в МБОУ ДО «Гавриловская школа искусств»

3.7.1 и соответствие действующему законодательству РФ необходимой внутренней нормативной базы, регулирующей вопросы защиты персональных данных.

Проверить наличие доказательств ознакомления работников МБОУ ДО «Гавриловская школа искусств»

с внутренними нормативными документами (приказами, инструкциями и т.п.),

регулирующими вопросы защиты персональных данных в МБОУ ДО «Гавриловская школа искусств»

3.7.2 .

3.7.3 Принять решение о необходимости актуализации внутренней нормативной базы.

Приложение к Правилам
осуществления внутреннего контроля
соответствия обработки персональных данных
требованиям к защите персональных данных
в МБОУ ДО «Гавриловская школа искусств»

План проведения внутренних проверок

Проверка	Периодичность	Методика (программа) проверки	Ответственный исполнитель
Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	1 раз в 3 месяца	Пункт 3.1 настоящих Правил	Ответственный за обеспечение безопасности персональных данных в ИСПДн
Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации	1 раз в 3 месяца	Пункт 3.2 настоящих Правил	Ответственный за обеспечение безопасности персональных данных в ИСПДн
Контроль состава технических средств, программного обеспечения и средств защиты информации	1 раз в 3 месяца	Пункт 3.3 настоящих Правил	Ответственный за обеспечение безопасности персональных данных в ИСПДн
Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в ИСПДн	1 раз в полгода	Пункт 3.4 настоящих Правил	Ответственный за обеспечение безопасности персональных данных в ИСПДн
Проверка соблюдения режима защиты персональных данных при их обработке в ИСПДн	1 раз в полгода	Пункт 3.5 настоящих Правил	Ответственный за обеспечение безопасности персональных данных в ИСПДн
Анализ и пересмотр существующих мер по обеспечению безопасности персональных данных в ИСПДн	1 раз в год	Пункт 3.6 настоящих Правил	Ответственный за обеспечение безопасности персональных данных в ИСПДн
Проверка наличия и актуальности внутренней нормативной документации по защите персональных данных	1 раз в год, а также перед проверками регуляторов	Пункт 3.7 настоящих Правил	Ответственный за обеспечение безопасности персональных данных в ИСПДн