

РЕГЛАМЕНТ

проведения внутреннего контроля соответствия обработки информации ограниченного доступа требованиям к защите информации ограниченного доступа в ФГБОУ ВО «Новосибирская государственная консерватория имени М.И. Глинки»

1. Общие положения

- 1.1. Регламент проведения внутреннего контроля соответствия обработки информации ограниченного доступа в ФГБОУ ВО «Новосибирская государственная консерватория имени М.И. Глинки» (далее – Консерватория) разработан в соответствии с законодательством Российской Федерации об информации ограниченного доступа (далее – ИОД) и нормативно-методическими документами федеральных органов исполнительной власти по вопросам безопасности ИОД при ее обработке в информационных системах (далее – ИС).
- 1.2. Регламент определяет порядок проведения внутреннего контроля соответствия обработки ИОД (далее – внутренний контроль) требованиям к защите ИОД.
- 1.3. Регламент обязателен для исполнения ответственным за организацию обработки персональных данных (далее – ПДн), ответственным за защиту информации в ИС, администратором ИС.

2. Порядок проведения внутреннего контроля

- 2.1. Для проведения внутреннего контроля в ИС создаётся комиссия, состоящая не менее чем из трех человек с обязательным включением в её состав:
- ответственного за организацию обработку ПДн;
 - ответственного за защиту информации в ИС.
- 2.2. Председатель комиссии организует работу комиссии, решает вопросы взаимодействия комиссии с руководителями и работниками структурных подразделений организации, готовит и ведёт заседания комиссии, подписывает протоколы заседаний. По окончании работы комиссии готовится заключение по результатам внутреннего контроля, которое передается на рассмотрение ректору Консерватории.
- 2.3. Внутренний контроль проводится в соответствии с «Планом проведения внутреннего контроля соответствия обработки информации ограниченного доступа требованиям к защите информации ограниченного доступа», утвержденным приказом ректора Консерватории, форма которого приведена в Приложении №1.
- 2.4. В Плане проведения внутреннего контроля указывается перечень проводимых мероприятий внутреннего контроля и периодичность их проведения.
- 2.5. Комиссия проводит внутренний контроль непосредственно на месте обработки ИОД, опрашивает работников, осуществляющих обработку ИОД, осматривает рабочие места.
- 2.6. Все работники обязаны по запросу контролирующих предъявить все материалы и документы, числящиеся за ними, дать устные или письменные объяснения по существу заданных вопросов.
- 2.7. По результатам проверки составляется «Акт о проведении контроля соответствия обработки информации ограниченного доступа», форма которого приведена в Приложение №2.

3. Ответственность

3.1. За организацию проведения внутреннего контроля отвечает ответственный за обработку ПДн.

4. Срок действия и порядок внесения изменений

- 4.1. Настоящий Регламент вступает в силу с момента его утверждения и действует бессрочно.
- 4.2. Настоящий Регламент подлежит пересмотру не реже одного раза в три года.
- 4.3. Изменения и дополнения в настоящий Регламент вносятся приказом ректора Консерватории.

**План проведения внутреннего контроля
соответствия обработки информации ограниченного доступа
в ФГБОУ ВО «Новосибирская государственная консерватория имени
М.И. Глинки требованиям к защите информации ограниченного доступа**

| № п/п | Мероприятие | Регулярность проведения |
|----------|---|---|
| 1. | <p>Анализ актуальности локальных актов по вопросам защиты ИОД (в т.ч. моделей угроз):</p> <ul style="list-style-type: none"> – Проверка соответствия локальных актов действующему законодательству РФ по защите ИОД; – Учет в локальных актах изменений в деятельности НГК имени М.И. Глинки по обработке и защите ИОД (изменения в ИС; появление новых ИС и т.д.). | 1 раз в три года или по мере обновления законодательства РФ |
| 2. | Проверка ознакомления работников с положениями законодательства РФ об ИОД, в том числе требованиями к защите ИОД, документами, определяющими политику НГК имени М.И. Глинки в отношении обработки персональных данных и организационно-распорядительными документами по вопросам ИОД. | 1 раз в год |
| 3. | Проверка выполнения работниками - пользователями ИС инструкций по эксплуатации ИС, положения о разрешительной системе доступа. | 1 раз в год |
| 4. | Проверка актуальности прав разграничения доступа пользователей ИС, необходимых для выполнения должностных обязанностей. | 1 раз в год |
| 5. | Проверка актуальности определенных угроз безопасности ИОД для ИС. | 1 раз в год |
| 6. | Проверка полноты реализованных технических мер по обеспечению безопасности ИОД в ИС с учетом структурно-функциональных характеристик ИС, информационных технологий, особенностей функционирования ИС. | 1 раз в год |
| 7. | Проверка наличия сертифицированных СЗИ, в случаях, когда применение таких СЗИ необходимо для нейтрализации актуальных угроз безопасности ИОД. | 1 раз в год |
| 8. | Проверка правил обращения со съемными машинными носителями ИОД. | 1 раз в год |
| 9. | Проверка актуальности информации, содержащейся в Уведомлении об обработке персональных данных, предоставленной в Роскомнадзор. | 1 раз в год |
| 10. | Проверка соответствия условий использования СКЗИ условиям, предусмотренным эксплуатационной и технической документацией на СКЗИ. | 1 раз в год |
| 11. | Выявление уязвимостей в ИС в т.ч. в системе защиты с использованием средства инструментального анализа защищенности. | 1 раз в год |

**Форма акта о проведения контроля соответствия обработки информации
ограниченного доступа**

АКТ

о проведения контроля соответствия обработки информации ограниченного доступа

« ___ » _____ 20__ г.

№ _____

О проведении контроля соответствия обработки
информации ограниченного доступа

Комиссия в составе:

Председатель:

Члены комиссии:

1. _____
2. _____
3. _____

составила настоящий акт о том, что комиссией были проведены мероприятия по контролю соответствия обработки информации ограниченного доступа требованиям к защите информации ограниченного доступа. 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 информации ограниченного доступа в НГК имени М.И. Глинки требованиям к защите информации ограниченного доступа».

Председатель:

Члены комиссии: