Приложение №1
к приказу от «25» 10 2024 г. № 206

РЕГЛАМЕНТ
проведения внутреннего контроля соответствия обработки информации ограниченного доступа требованиям к защите информации ограниченного доступа в СПбГИПСР

1. Термины и определения

1.1. Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих её обработку информационных технологий и технических средств.

1.2. 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.

1.3. 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.

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

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

2. Общие положения

2.1. Регламент проведения внутреннего контроля соответствия обработки информации ограниченного доступа в СПбГИПСР (далее – Учреждение) 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).

2.2. Регламент определяет порядок проведения внутреннего контроля соответствия обработки ИОД (далее – внутренний контроль) требованиям к защите ИОД.

2.3. Регламент обязателен для исполнения ответственным за организацию обработки персональных данных (далее – ПДн), ответственным за защиту информации в ИС, администратором ИС.

3. Порядок проведения внутреннего контроля

3.1. Для проведения внутреннего контроля в ИС создаётся комиссия, состоящая не менее чем из трех человек с обязательным включением в её состав:

– ответственного за организацию обработки ПДн;

– ответственного за защиту информации в ИС.

3.2. 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 Учреждения.

3.3. Внутренний контроль проводится в соответствии с «Планом проведения внутреннего контроля соответствия обработки информации ограниченного доступа требованиям к защите информации ограниченного доступа», утвержденным приказом ректора Учреждения, форма которого приведена в Приложении №1.

3.4. В Плане проведения внутреннего контроля указывается перечень проводимых мероприятий внутреннего контроля и периодичность их проведения.

3.5. Комиссия проводит внутренний контроль непосредственно на месте обработки ИОД, опрашивает работников, осуществляющих обработку ИОД, осматривает рабочие места.

3.6. Все работники обязаны по запросу контролирующих предъявить все материалы и документы, числящиеся за ними, дать устные или письменные объяснения по существу заданных вопросов.

3.7. По результатам проверки составляется «Акт о проведении контроля соответствия обработки информации ограниченного доступа», форма которого приведена в Приложение №2.

4. Ответственность

4.1. За организацию проведения внутреннего контроля отвечает ответственный за организацию обработки ПДн.

5. Срок действия и порядок внесения изменений

5.1. Настоящий Регламент вступает в силу с момента его утверждения и действует бессрочно.

5.2. Настоящий Регламент подлежит пересмотру не реже одного раза в три года.

5.3. Изменения и дополнения в настоящий Регламент вносятся приказом ректора Учреждения.

Приложение №1
к Регламенту проведения внутреннего контроля
соответствия обработки информации
ограниченного доступа
требованиям к защите информации
ограниченного доступа

План проведения внутреннего контроля соответствия обработки информации ограниченного доступа в СПбГИПСР требованиям к защите информации ограниченного доступа

№ п/п	Мероприятие	Регулярность проведения
1.	Анализ актуальности локальных актов по вопросам защиты ИОД (в т.ч. моделей угроз): -Проверка соответствия локальных актов действующему законодательству РФ по защиты ИОД; -Учет в локальных актах изменений в деятельности СПбГИПСР по обработке и защите ИОД (изменения в ИС; появление новых ИС и т.д.).	1 раз в два 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 СПбГИПСР 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 средств криптографической защиты информации условиям, предусмотренным эксплуатационной и технической документацией на средства криптографической защиты информации.	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
12.	Обучение персонала ИС правилам эксплуатации средств защиты информации	1 раз в два года
13.	Контроль осведомленности персонала ИС об угрозах безопасности информации и уровня знаний персонала по вопросам обеспечения защиты информации.	1 раз в два года
14.	Проведение периодического контроля уровня защиты информации на аттестованном объекте информатизации (проводится самостоятельно или с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации)	1 раз в два года

Приложение №2
к Регламенту проведения внутреннего контроля
соответствия обработки информации
ограниченного доступа
требованиям к защите информации
ограниченного доступа

ФОРМА

АКТА

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 СПбГИПСР требованиям к защите информации ограниченного доступа».

Председатель:

_____ _____ _____

Члены комиссии:

_____ _____ _____

_____ _____ _____

_____ _____ _____