Приложение №1
к приказу от «25» 10 2024 г. № 207

# ПОЛОЖЕНИЕ
## об обеспечении безопасности информации ограниченного доступа, обрабатываемой в информационных системах СПбГИПСР

## 1. Термины и определения

1.1. Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

1.2. Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

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. Основные технические средства и системы – технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи персональных данных.

1.5. Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

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

1.7. Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

1.8. Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

1.9. Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

## 2. Общие положения

2.1. Настоящее Положение об обеспечении безопасности информации ограниченного доступа (далее – Положение), обрабатываемой в информационных системах СПбГИПСР (далее – Учреждение), разработано в соответствии с законодательством РФ об информации ограниченного доступа (далее – ИОД) и нормативно-методическими документами исполнительных органов государственной власти по вопросам безопасности ИОД при ее обработке в информационных системах (далее – ИС).

2.2. Настоящее Положение определяет состав и содержание организационных и технических мер по обеспечению безопасности ИОД при ее обработке в ИС.

2.3. Положение обязательно для исполнения всеми работниками Учреждения, непосредственно осуществляющими защиту ИОД, обрабатываемой в ИС.

## 3. Цели и задачи обеспечения безопасности информации ограниченного доступа

3.1. Основной целью обеспечения безопасности ИОД при ее обработке в ИС, является защита ИОД от неправомерного или случайного доступа к ней, уничтожения, изменения, блокирования, копирования, предоставления, распространения ИОД, а также от иных неправомерных действий в отношении ИОД.

3.2. Система защиты информации (далее – СиЗИ) включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности ИОД и информационных технологий, используемых в ИС.

## 4. Основные принципы построения системы защиты информации

4.1. СиЗИ основывается на следующих принципах:

- системности;
- комплексности;
- непрерывности защиты;
- разумной достаточности;
- гибкости СиЗИ;
- простоты применения средств защиты информации (далее – СЗИ).

4.2. Принцип системности – предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности ИОД.

4.3. Принцип комплексности – предполагает, что СиЗИ должна включать совокупность объектов защиты, сил и средств, принимаемых мер, проводимых мероприятий и действий по обеспечению безопасности ИОД от возможных угроз всеми доступными законными средствами, методами и мероприятиями.

4.4. Принцип непрерывности защиты – это процесс обеспечения безопасности ИОД, осуществляемый руководством, ответственным за защиту информации в ИС и работниками всех уровней. Это не только и не столько процедура или политика, которая осуществляется в определенный отрезок времени или совокупность средств защиты, сколько процесс, который должен постоянно идти на всех уровнях внутри организации, и каждый работник должен принимать участие в этом процессе.

4.5. Принцип разумной достаточности – предполагает соответствие уровня затрат на обеспечение безопасности ИОД ценности информационных ресурсов и величине возможного ущерба от их разглашения, утраты, утечки, уничтожения и искажения.

4.6. Принцип гибкости СиЗИ – система обеспечения безопасности ИОД должна быть способна реагировать на изменения внешней среды и условий осуществления своей деятельности.

4.7. Принцип простоты применения СЗИ – механизмы защиты должны быть интуитивно понятны и просты в применении. Применение СЗИ не должно быть связано со знанием каких-либо языков или требовать дополнительных затрат на её применение, а также не должно требовать выполнения рутинных малопонятных операций.

## 5. Основные мероприятия по обеспечению безопасности информации ограниченного доступа

5.1. Для обеспечения защиты ИОД, обрабатываемой в ИС, проводятся следующие мероприятия:

- определение ответственных лиц за обеспечение защиты ИОД;
- анализ угроз безопасности ИОД в ИС;
- определение уровня защищенности персональных данных (далее – ПДн);
- определение класса защищенности ИС;
- реализация правил разграничения доступа и введение ограничений на действия пользователей;

– ограничение доступа в помещения, где размещены основные технические средства и системы, позволяющие осуществлять обработку ИОД;

– учет и хранение съемных машинных носителей ИОД;

– организация резервирования и восстановления работоспособности программного обеспечения, баз данных ИОД и СЗИ;

– организация парольной защиты;

– организация антивирусной защиты;

– организация обновления программного обеспечения и СЗИ;

– использование СЗИ;

– использование средств криптографической защиты информации (далее – СКЗИ);

– оценка эффективности принимаемых мер по обеспечению безопасности ИОД до ввода в эксплуатацию СиЗИ;

– обнаружение фактов несанкционированного доступа к ИОД и принятие мер;

– аттестация ИС и ввод в действие;

– контроль за принимаемыми мерами по обеспечению безопасности ИОД;

– управление конфигурацией ИС и СиЗИ;

– реагирование на инциденты;

– информирование и обучение персонала ИС.

5.2. **Определение ответственных лиц за обеспечение защиты ИОД**

5.2.1. За вопросы обеспечения безопасности ИОД, обрабатываемой в ИС, отвечают:

– Ректор Учреждения.

– Ответственный за организацию обработки ПДн – работник, отвечающий за организацию и состояние процесса обработки ПДн.

– Ответственный за защиту информации в ИС – работник, отвечающий за правильность использования и нормальное функционирование установленной СиЗИ.

– Администратор ИС – работник, отвечающий за правильность использования и бесперебойное, стабильное функционирование установленных систем обработки информации.

5.3. **Анализ угроз безопасности ИОД в ИС**

5.3.1. Актуальные угрозы безопасности ИОД, обрабатываемой в ИС, определяются по результатам оценки возможностей (потенциала, оснащенности и мотивации) внешних и внутренних нарушителей, анализа возможных уязвимостей ИС, возможных способов реализации угроз безопасности ИОД и последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности).

5.3.2. Для определения угроз безопасности ИОД и разработки «Модели угроз безопасности информации ограниченного доступа…» применяются методические документы, разработанные и утвержденные ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004г. №1085.

5.4. **Определение уровня защищенности ПДн**

5.4.1. Уровень защищенности ПДн, обрабатываемых в ИС, определяется, в соответствии с постановлением Правительства Российской Федерации от 1 ноября 2012г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и оформляется в виде «Акта об определения уровня защищенности персональных данных…».

5.5. **Реализация правил разграничения доступа и введение ограничений на действия пользователей**

5.5.1. Реализация правил разграничения доступа, к ИОД, обрабатываемой в ИС, осуществляется в соответствии с «Положением о разрешительной системе доступа к ресурсам информационных систем».

5.5.2. Ограничение доступа пользователей в помещения, где размещены основные технические средства и системы, позволяющие осуществлять обработку ИОД.

5.5.3. Основные технические средства и системы ИС расположены в помещениях в пределах границ контролируемой зоны.

5.5.4. Доступ работников в помещения, в которых ведется обработка ИОД в ИС, осуществляется в соответствии с «Правилами доступа в помещения, в которых ведется обработка информации ограниченного доступа».

5.6. **Учет и хранение съемных машинных носителей ИОД**

5.6.1. Работа со съемными машинными носителями ИОД в ИС осуществляется в соответствии с «Порядком обращения со съемными машинными носителями информации ограниченного доступа в информационных системах».

5.7. **Организация резервирования и восстановления работоспособности программного обеспечения, баз данных и СЗИ**

5.7.1. Организация резервирования и восстановления работоспособности программного обеспечения, баз данных и СЗИ в ИС осуществляется в соответствии с «Инструкцией по эксплуатации информационных систем».

5.8. **Организация парольной защиты**

5.8.1. Организация парольной защиты в ИС осуществляется в соответствии с «Инструкцией по эксплуатации информационных систем».

5.9. **Организация антивирусной защиты**

5.9.1. Организация антивирусной защиты в ИС осуществляется в соответствии с «Инструкцией по эксплуатации информационных систем».

5.10. **Организация обновления программного обеспечения и СЗИ**

5.10.1. Организация обновления программного обеспечения и СЗИ в ИС осуществляется в соответствии с «Инструкцией по эксплуатации информационных систем».

5.11. **Использование СЗИ**

5.11.1. Для обеспечения защиты ИОД, обрабатываемой в ИС, применяются СЗИ, прошедшие оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации в соответствии со статьей 5 Федерального закона от 27 декабря 2002г. №184-ФЗ «О техническом регулировании».

5.11.2. Установка и настройка СЗИ в ИС проводится в соответствии с эксплуатационной документацией на СиЗИ и документацией на СЗИ.

5.12. **Использование СКЗИ**

5.12.1. Для обеспечения защиты ИОД, обрабатываемой в ИС, при ее передаче по открытым каналам связи, применяются СКЗИ. Обращение с СКЗИ, эксплуатируемыми в ИС, осуществляется в соответствии с «Инструкцией по обращению со средствами криптографической защиты информации в информационных системах».

5.13. **Оценка эффективности принимаемых мер по обеспечению безопасности ИОД до ввода в эксплуатацию СиЗИ**

5.13.1. На этапах внедрения СиЗИ проводится оценка эффективности принимаемых мер по обеспечению безопасности ИОД, которая включает в себя:

- предварительные испытания СиЗИ;

- опытную эксплуатацию СиЗИ;
- анализ уязвимостей ИС и принятие мер по их устранению;
- приемочные испытания СиЗИ.

5.14. **Обнаружение фактов несанкционированного доступа к ИОД и принятие мер**

5.14.1. Ответственному за защиту информации в ИС или администратору ИС должны сообщаться любые инциденты информационной безопасности, в которые входят:

- факты попыток и успешной реализации несанкционированного доступа в ИС;
- факты попыток и успешной реализации несанкционированного доступа в помещения, в которых ведется обработка ИОД в ИС;
- факты сбоя или некорректной работы систем обработки информации;
- факты сбоя или некорректной работы СЗИ;
- факты разглашения ИОД, обрабатываемой в ИС;
- факты разглашения информации о методах и способах защиты и обработки ИОД в ИС.

5.14.2. Разбор инцидентов информационной безопасности проводится, согласно «Регламенту реагирования на инциденты информационной безопасности в информационных системах».

5.15. **Аттестация ИС и ввод в действие**

5.15.1. Аттестация ИС включает в себя проведение комплекса организационных и технических мероприятий (аттестационных испытаний), в результате которых подтверждается соответствие СиЗИ в ИС требованиями приказа ФСТЭК России от 18 февраля 2013 г. N 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». Для проведения работ по аттестации ИС, привлекаются организации, имеющие следующие соответствующие лицензии ФСТЭК и ФСБ.

5.16. **Контроль за принимаемыми мерами по обеспечению безопасности ИОД**

5.16.1. Контроль за принимаемыми мерами по обеспечению безопасности ИОД, осуществляется в соответствии с «Регламентом проведения внутреннего контроля соответствия обработки информации ограниченного доступа требованиям к защите информации ограниченного доступа» требованиям по защите информации ограниченного доступа».

## 6. Ответственность

6.1. Все работники Учреждения, допущенные в установленном порядке к работе с ИОД, несут административную, материальную, уголовную ответственность в соответствии с действующим законодательством за обеспечение сохранности и соблюдению правил работы с ИОД.

6.2. Ответственность за доведение требований настоящего Положения до работников Учреждения и обеспечение мероприятий по их реализации несет ответственный за защиту информации в ИС.

## 7. Срок действия и порядок внесения изменений

7.1. Настоящее Положение вступает в силу с момента его утверждения и действует бессрочно.

7.2. Настоящее Положение подлежит пересмотру не реже одного раза в три года.

7.3. Изменения и дополнения в настоящее Положение вносятся приказом ректора Учреждения.