Приложение №1
к приказу от «25» 10 2024 г. № 211

ИНСТРУКЦИЯ
администратора информационных систем 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. Настоящая инструкция определяет функции, обязанности и права администратора информационных систем (далее – ИС) СПбГИПСР (далее – Учреждение).

2.2. Администратор ИС назначается приказом ректора Учреждения.

2.3. Настоящая инструкция является дополнением к действующим нормативным документам по вопросам обеспечения безопасности информации ограниченного доступа (далее – ИОД), и не исключает обязательного выполнения их требований.

2.4. На время отсутствия (болезнь, отпуск, пр.) администратора ИС его обязанности возлагаются на работника, назначенного и допущенного в установленном порядке.

3. Функции

3.1. Администратор ИС выполняет следующие функции:

- Управляет параметрами ИС:
  - управляет заведением и удалением учетных записей пользователей;
  - управляет полномочиями пользователей ИС;
  - поддерживает в актуальном состоянии правила разграничения доступа в ИС;
  - управляет параметрами настройки программного обеспечения;
  - управляет учетными записями пользователей программных средств обработки ИОД;
  - оказывает помощь в смене и восстановлении паролей;
  - управляет установкой программного обеспечения, в т.ч. обновлений;
  - регистрирует события в ИС, связанные с защитой ИОД (события безопасности);
  - управляет обновлениями программных и программно-аппаратных средств.
- Принимает участие в выявлении инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования ИС и (или) к возникновению угроз безопасности ИОД:
  - отказы в обслуживании;
  - сбои (перезагрузки) в работе технических средств, программного обеспечения;
  - нарушения правил разграничения доступа;
  - неправомерные действия по сбору ИОД;
  - внедрения вредоносных компьютерных программ (вирусов);
  - иные события, приводящие к возникновению инцидентов;
- Своевременно информирует ответственного за защиту информации в ИС, о возникновении инцидентов в ИС;
- Принимает меры по устранению инцидентов, в том числе:
  - по восстановлению ИС и ее сегментов в случае отказа в обслуживании или после сбоев;
  - по устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору ИОД, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов.
- Ведет учет пользователей ИС;
- Проводит первоначальный, плановый и внеплановый инструктаж обслуживающего и эксплуатирующего персонала ИС, а также отвечает на вопросы по работе с общесистемным и прикладным программным обеспечением, аппаратным обеспечением, сетевым оборудованием.
- Участвует в обучении персонала ИС правилам эксплуатации отдельных средств защиты информации.
- Доводит до персонала ИС требований по защите информации, а также положений организационно-распорядительных документов по защите информации с учетом внесенных в них изменений.
- Осуществляет хранение:
  - Носителей дистрибутивов общесистемного и прикладного программного обеспечения, программного обеспечения сетевого оборудования.

– Эксплуатационной и технической документации к общесистемному и прикладному программному обеспечению, аппаратному обеспечению, сетевому оборудованию.

– Лицензий, сертификатов на общесистемное и прикладное программное обеспечение, аппаратное обеспечение, сетевое оборудование.

- Принимает участие в деятельности:
  - по подготовке, пересмотру, уточнению локальных актов по защите ИОД;
  - по аттестации объектов информатизации;
  - по анализу угроз безопасности информации в ИС;
  - по управлению конфигурацией ИС и ее системы защиты;
  - по планированию мероприятий по защите информации в информационных системах.

4. Права

4.1. Администратор имеет право:

- Требовать от работников – пользователей ИС соблюдения установленной технологии обработки ИОД и выполнения инструкций по обеспечению безопасности ИОД;
- Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, порчи, защищаемой ИОД и технических средств, входящих в состав ИС;
- Требовать прекращения обработки ИОД в случае нарушения установленного порядка работ или нарушения функционирования средств защиты информации и системы защиты информации;
- Участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа.

5. Ответственность

5.1. На администратора возлагается персональная ответственность за качество проводимых им работ по обеспечению бесперебойного и стабильного функционирования ИС.

5.2. Администратор несет ответственность по действующему законодательству за разглашение сведений ограниченного доступа, ставших известными ему по роду работы.

6. Срок действия и порядок внесения изменений

6.1. Настоящая инструкция вступает в силу с момента его утверждения и действует бессрочно.

6.2. Настоящая инструкция подлежит пересмотру не реже одного раза в три года.

6.3. Изменения и дополнения в настоящую инструкцию вносятся приказом ректора Учреждения.