Приложение №1
к приказу от «25» 10 2024 г. № 208

ИНСТРУКЦИЯ
ответственного за защиту информации в информационных системах СПбГИПСР

1. Термины и определения

1.1. Доступность информации – свойство безопасности информации, при котором субъекты доступа, имеющие право доступа к информации в соответствии с локальными актами и законодательством Российской Федерации, могут беспрепятственно реализовывать данное право.

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

1.3. 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.

1.4. Конфиденциальность информации – свойство безопасности информации, при котором доступ к информации осуществляют только те субъекты доступа, которые имеют на это право в соответствии с локальными актами и законодательством Российской Федерации.

1.5. 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.

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

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

1.8. Целостность информации – свойство безопасности информации, при котором изменение информации осуществляют только те субъекты доступа, которые имеют на это право в соответствии с локальными актами и законодательством Российской Федерации.

2. Общие положения

2.1. Настоящая инструкция определяет функции, обязанности и права ответственного за защиту информации в информационных системах (далее – ИС) СПбГИПСР (далее – Учреждение).

2.2. Ответственный за защиту информации в ИС назначается приказом ректора Учреждения.

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

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

3. Функции

3.1. Ответственный за защиту информации в ИС выполняет следующие функции:

- Управляет доступом пользователей в ИС;
- Управляет полномочиями пользователей в ИС;
- Поддерживает установленные правила разграничения доступа в ИС;
- Управляет (администрирует) системой защиты информации (далее – СиЗИ) информационных систем (далее – ИС):
  - управляет средствами защиты информации (далее – СЗИ) в ИС;
  - управляет программным обеспечением СЗИ;
  - восстанавливает работоспособность СЗИ;
  - устанавливает обновления программного обеспечения СЗИ, выпускаемых разработчиками (производителями) СЗИ;
  - анализирует события в ИС, связанные с защитой информации (события безопасности);
  - информирует пользователей об угрозах безопасности информации;
  - информирует пользователей о правилах эксплуатации СЗИ;
  - обучает пользователей работе со СЗИ;
- Управляет доступом к съемным машинным носителям информации, используемым в ИС (определяет должностных лиц, имеющих доступ к съемным машинным носителям информации);
- Сопровождает функционирование СиЗИ в ходе ее эксплуатации;
- Поддерживает конфигурацию СиЗИ (структуру СиЗИ, состав, места установки и параметры настройки СЗИ, программного обеспечения и технических средств) в соответствии с эксплуатационной документацией на СиЗИ (поддержание базовой конфигурации СиЗИ);
- Определяет лица, которым разрешены действия по внесению изменений в базовую конфигурацию СиЗИ;
- Управляет изменениями базовой конфигурации СиЗИ, в том числе:
  - определяет типы возможных изменений,
  - разрешает или отказывает во внесении изменений,
  - документирует действия по внесению изменений,
  - хранит данные об изменениях;
- Поддерживает конфигурацию ИС (структуру ИС, состав, места установки и параметры программного обеспечения и технических средств) в соответствии с эксплуатационной документацией на ИС;
- Анализирует потенциальные воздействия планируемых изменений в базовой конфигурации СиЗИ на обеспечение защиты информации, возникновение дополнительных угроз безопасности информации и работоспособность ИС;

- Определяет параметры настройки программного обеспечения, включая программное обеспечение СЗИ, состава и конфигурации технических средств и программного обеспечения до внесения изменений в базовую конфигурацию ИС и СиЗИ;
- Выявляет инциденты (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования ИС и (или) к возникновению угроз безопасности информации (далее – инциденты), и реагирует на них.
- Обнаруживает и идентифицирует инциденты, в том числе:
  - отказы в обслуживании,
  - сбои (перезагрузки) в работе СЗИ,
  - нарушения правил разграничения доступа,
  - неправомерные действия по сбору информации,
  - иные события, приводящие к возникновению инцидентов;
- Анализирует инциденты, в том числе определяет источники и причины возникновения инцидентов, а также оценивает их последствия;
- Планирует меры по устранению инцидентов, в том числе:
  - по восстановлению ИС и ее сегментов в случае отказа в обслуживании или после сбоев,
  - устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;
- Планирует и принимает меры по предотвращению повторного возникновения инцидентов.
- Контролирует обеспечение класса защищенности ИС:
  - контролирует события безопасности и действия пользователей в ИС;
  - контролирует (анализирует) защищенность информации, содержащейся в ИС;
  - контролирует перемещение съемных машинных носителей информации за пределы контролируемой зоны лицами, которым оно необходимо для выполнения своих должностных обязанностей (функции);
  - анализирует и оценивает функционирование СиЗИ ИС, включая выявление, анализ и устранение недостатков в функционировании системы защиты информации ИС;
  - выполняет периодический анализ изменения угроз безопасности информации в ИС, возникающих в ходе ее эксплуатации, и принятие мер защиты информации в случае возникновения новых угроз безопасности информации;
  - документирует процедуры и результаты контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в ИС;
  - принимает решения по результатам контроля (мониторинга) за обеспечением уровня защищенности информации о доработке (модернизации) СиЗИ ИС.
- Ведет учет:
  - ведет учет используемых шифровальных (криптографических) средств защиты информации в ИС, эксплуатационной и технической документации к ним;
  - ведет учет съемных машинных носителей, используемых в ИС для хранения и обработки информации.
- Обеспечивает защиту информации при выводе из эксплуатации ИС или после принятия решения об окончании обработки информации:

– обеспечивает архивирование информации, содержащейся в ИС (архивирование должно осуществляться при необходимости дальнейшего использования информации в деятельности оператора);

– обеспечивает уничтожение (стирание) данных и остаточной информации со съемных машинных носителей информации, при необходимости передачи съемного машинного носителя информации другому пользователю ИС или в сторонние организации для ремонта, технического обслуживания или дальнейшего уничтожения;

– при выводе из эксплуатации съемных машинных носителей информации, на которых осуществлялись хранение и обработка информации, осуществляет физическое уничтожение этих съемных машинных носителей информации.

- Осуществляет хранение:

  – носителей дистрибутивов СЗИ и средств криптографической защиты информации (далее – СКЗИ);

  – эксплуатационной и технической документации к СЗИ и СКЗИ.

  – лицензий, сертификатов на СЗИ и СКЗИ.

- 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;

  – по проведению проверки ИС на предмет соответствия требованиям законодательства РФ.

4. Права

4.1. Ответственный за защиту информации в ИС имеет право:

- требовать от работников – пользователей ИС соблюдения установленной технологии обработки информации и выполнения инструкций по обеспечению безопасности информации;

- инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, порчи защищаемой информации и технических средств, входящих в состав ИС;

- требовать прекращения обработки информации в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации;

- участвовать в анализе ситуаций, касающихся функционирования СЗИ и расследования фактов несанкционированного доступа;

- подавать свои предложения по совершенствованию организационных и технических мер по защите информации ограниченного доступа.

5. Ответственность

5.1. На ответственного за защиту информации в ИС возлагается персональная ответственность за качество проводимых им работ по обеспечению защиты информации.

5.2. Работник, ответственный за защиту информации в ИС, 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 ее 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.