САНКТ-ПЕТЕРБУРГСКОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ ИНСТИТУТ ПСИХОЛОГИИ И СОЦИАЛЬНОЙ РАБОТЫ»
(СПбГИПСР)

ПРИНЯТО	УТВЕРЖДЕНО
Ученым советом СПбГИПСР	приказом ректора СПбГИПСР
(протокол от 22.02.2022 № 07)	от 22.02.2022 № 046

Положение

об обеспечении безопасности информации ограниченного доступа, обрабатываемой на абонентском пункте информационной системы «Федеральная информационная система обеспечения проведения государственной итоговой аттестации» в институте

1. Общие положения

1.1. Положение об обеспечении безопасности информации ограниченного доступа, обрабатываемой на абонентском пункте информационной системы «Федеральная информационная система обеспечения проведения государственной итоговой аттестации» в институте (далее – Положение), разработано в соответствии с законодательством Российской Федерации об информации ограниченного доступа (далее – ИОД) и нормативно-методическими документами исполнительных органов государственной власти по вопросам безопасности ИОД при ее обработке на абонентском пункте информационной системы «Федеральная информационная система обеспечения проведения государственной итоговой аттестации» (далее – АП ФИС ГИА).

1.2. Положение определяет состав и содержание организационных и технических мер по обеспечению безопасности ИОД при ее обработке на АП ФИС ГИА.

1.3. Положение обязательно для исполнения всеми работниками института, непосредственно осуществляющими защиту ИОД, обрабатываемой на АП ФИС ГИА.

Все работники института, 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.

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

1.4. Положение подлежит пересмотру не реже одного раза в три года.

2. Цели и задачи обеспечения безопасности информации ограниченного доступа

2.1. Основной целью обеспечения безопасности ИОД при ее обработке в информационных системах (далее – 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.

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

3. Основные принципы построения системы защиты информации

3.1. СиЗИ основывается на следующих принципах:

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

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

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

3.4. 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.

3.5. 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.

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

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

4. Основные мероприятия по обеспечению безопасности информации ограниченного доступа

4.1. Для обеспечения защиты ИОД, обрабатываемой на АП ФИС ГИА, проводятся следующие мероприятия:

- определение ответственных лиц за обеспечение защиты ИОД;
- определение актуальных угроз безопасности ИОД;
- определение уровня защищенности персональных данных (далее – ПДн);

- определение класса защищенности АП ФИС ГИА;
- 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 АП ФИС ГИА и ввод в действие;
- контроль за принимаемыми мерами по обеспечению безопасности ИОД.

4.2. Определение ответственных лиц за обеспечение защиты ИОД.

4.2.1. За вопросы обеспечения безопасности ИОД, обрабатываемой на АП ФИС ГИА, отвечают:

- ответственный за организацию обработки ПДн – работник, отвечающий за организацию и состояние процесса обработки ПДн;
- оветственный 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.

4.3. Определение актуальных угроз безопасности ИОД.

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

4.3.2. Для определения угроз безопасности ИОД и разработки «Модели угроз безопасности информации ограниченного доступа при ее обработке на абонентском пункте информационной системы «Федеральная информационная система обеспечения проведения государственной итоговой аттестации» 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.

4.4. Определение уровня защищенности ПДн.

4.4.1. Уровень защищенности ПДн, обрабатываемых на АП ФИС ГИА, 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 при их обработке на абонентском пункте информационной системы «Федеральная информационная система обеспечения проведения государственной итоговой аттестации».

4.5. Определение класса защищенности АП ФИС ГИА.

4.5.1. Класс защищенности АП ФИС ГИА определяется в соответствии с приказом ФСТЭК России №17 от 11 февраля 2013г. «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и оформляется в виде «Акта об определении класса защищенности абонентского пункта информационной системы «Федеральная информационная система обеспечения проведения государственной итоговой аттестации».

4.6. Реализация правил разграничения доступа и введение ограничений на действия пользователей.

4.6.1. Реализация правил разграничения доступа, к ИОД, обрабатываемой на АП ФИС ГИА, осуществляется в соответствии с «Положением о разрешительной системе доступа к ресурсам абонентского пункта информационной системы «Федеральная информационная система обеспечения проведения государственной итоговой аттестации».

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

4.6.3. Основные технические средства и системы АП ФИС ГИА расположены в помещениях в пределах границ контролируемой зоны.

4.6.4. Доступ работников в помещения, в которых ведется обработка ИОД на АП ФИС ГИА, осуществляется в соответствии с «Правилами доступа в помещения абонентского пункта информационной системы «Федеральная информационная система обеспечения проведения государственной итоговой аттестации».

4.7. Учет и хранение съемных машинных носителей ИОД.

4.7.1. Работа со съемными машинными носителями ИОД на АП ФИС ГИА осуществляется в соответствии с «Порядком обращения со съемными машинными носителями информации ограниченного доступа на абонентском пункте информационной системы «Федеральная информационная система обеспечения проведения государственной итоговой аттестации».

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

4.8.1. Организация резервирования и восстановления работоспособности программного обеспечения, баз данных и СЗИ на АП ФИС ГИА осуществляется в соответствии с «Инструкцией по эксплуатации абонентского пункта информационной системы «Федеральная информационная система обеспечения проведения государственной итоговой аттестации».

4.9. Организация парольной защиты.

4.9.1. Организация парольной защиты на АП ФИС ГИА осуществляется в соответствии с «Инструкцией по эксплуатации абонентского пункта информационной системы «Федеральная информационная система обеспечения проведения государственной итоговой аттестации».

4.10. Организация антивирусной защиты.

4.10.1. Организация антивирусной защиты на АП ФИС ГИА осуществляется в соответствии с «Инструкцией по эксплуатации абонентского пункта информационной системы «Федеральная информационная система обеспечения проведения государственной итоговой аттестации».

4.11. Организация обновления программного обеспечения и СЗИ.

4.11.1. Организация обновления программного обеспечения и СЗИ на АП ФИС ГИА осуществляется в соответствии с «Инструкцией по эксплуатации абонентского пункта информационной системы «Федеральная информационная система обеспечения проведения государственной итоговой аттестации».

4.12. Использование СЗИ.

4.12.1. Для обеспечения защиты ИОД, обрабатываемой на АП ФИС ГИА, 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».

4.12.2. Установка и настройка СЗИ на АП ФИС ГИА проводится в соответствии с эксплуатационной документацией на СиЗИ и документацией на СЗИ.

4.13. Использование СКЗИ.

4.13.1. Для обеспечения защиты ИОД, обрабатываемой на АП ФИС ГИА, при ее передаче по открытым каналам связи, применяются СКЗИ. Обращение с СКЗИ, эксплуатируемыми на АП ФИС ГИА, осуществляется в соответствии с «Инструкцией по обращению со средствами криптографической защиты информации на абонентском пункте информационной системы «Федеральная информационная система обеспечения проведения государственной итоговой аттестации».

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

4.14.1. 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.

4.15. Обнаружение фактов несанкционированного доступа к ИОД и принятие мер.

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

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

4.16. Аттестация АП ФИС ГИА и ввод в действие.

4.16.1. Аттестация АП ФИС ГИА включает в себя проведение комплекса организационных и технических мероприятий (аттестационных испытаний), в результате которых подтверждается соответствие СиЗИ на АП ФИС ГИА требованиями приказа ФСТЭК России от 11 февраля 2013г. №17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах». Для проведения работ по аттестации

АП ФИС ГИА, привлекаются организации, имеющие следующие соответствующие лицензии ФСТЭК и ФСБ.

4.17. Контроль за принимаемыми мерами по обеспечению безопасности ИОД.

4.17.1. 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».