САНКТ-ПЕТЕРБУРГСКОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ ИНСТИТУТ ПСИХОЛОГИИ И СОЦИАЛЬНОЙ РАБОТЫ»

(СПбГИПСР)

ПРИНЯТО
Ученым советом СПбГИПСР
(протокол от 29.09.2021 № 2)

УТВЕРЖДЕНО
приказом ректора СПбГИПСР
от 29.09.2021 № 235

Положение об информационной безопасности

1. Общие положения

1.1. Настоящее положение разработано в соответствии с Трудовым кодексом РФ от 30.12.2001 №197-ФЗ, Федеральный законом от 07.07.2003 №126-ФЗ «О связи», Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных», Федеральным законом от 28.12.2010 № 390-ФЗ «О безопасности».

1.2. Информационная безопасность является одним из составных элементов комплексной безопасности. Под информационной безопасностью «Санкт-Петербургского Государственного института психологии и социальной работы» (далее – Институт) следует понимать состояние защищенности информационных ресурсов, технологий их формирования и использования, а также прав субъектов информационной деятельности. Система информационной безопасности направлена на предупреждение угроз, их своевременное выявление, обнаружение, локализацию и ликвидацию.

1.3. К объектам информационной безопасности в Институте относятся:

• информационные ресурсы, содержащие документированную информацию, в соответствии с перечнем сведений конфиденциального характера;

• информация, защита которой предусмотрена законодательными актами РФ, в т.ч. персональные данные;

• средства и системы информатизации, программные средства, автоматизированные системы управления, системы связи и передачи данных, осуществляющие прием, обработку, хранение и передачу информации с ограниченным доступом.

1.4. Система информационной безопасности должна обеспечивать:

• конфиденциальность (защиту информации от несанкционированного раскрытия или перехвата);

• целостность (точность и полноту информации и компьютерных программ);

• доступность (возможность получения пользователями информации в пределах их компетенции).

1.5. Обеспечение информационной безопасности осуществляется по следующим направлениям:

• правовая защита – специальные законы, другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе;

• организационная защита – регламентация деятельности Института и взаимоотношений исполнителей на нормативно-правовой основе, исключающая или ослабляющая нанесение какого-либо ущерба;

• инженерно-техническая защита – использование различных технических средств, препятствующих нанесению ущерба.

2. Цели и задачи обеспечения безопасности информации

2.1. Главной целью обеспечения безопасности информации, циркулирующей в Институте, является реализация положений законодательных актов Российской Федерации и нормативных требований по защите информации ограниченного доступа (далее по тексту - конфиденциальной или защищаемой информации) и предотвращение ущерба в результате разглашения, утраты, утечки, искажения и уничтожения информации, ее незаконного использования и нарушения работы информационной среды Института.

2.2. Основными целями обеспечения безопасности информации являются:

• предотвращение утечки, хищения, искажения, подделки информации, циркулирующей в Институте;

• предотвращение нарушений прав личности обучающихся, работников Института на сохранение конфиденциальности информации;

• предотвращение несанкционированных действий по блокированию информации.

2.3. Основными задачами обеспечения безопасности информации являются:

• соответствие положениям законодательных актов и нормативным требованиям по защите информации;

• своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба интересам Института, нарушению нормального функционирования и развития Института;

• создание механизма оперативного реагирования на угрозы информационной безопасности и негативные тенденции в системе информационных отношений;

• эффективное пресечение незаконных посягательств на информационные ресурсы, технические средства и информационные технологии, в том числе с использованием организационно-правовых и технических мер и средств защиты информации;

• развитие системы защиты, совершенствование ее организации, форм, методов и средств предотвращения, парирования и нейтрализации угроз информационной безопасности и ликвидации последствий ее нарушения;

• развитие и совершенствование защищенного юридически значимого электронного документооборота;

• создание механизмов, обеспечивающих контроль системы информационной безопасности и гарантии достоверности выполнения установленных требований информационной безопасности;

• создание механизмов управления системой информационной безопасности.

3. Правовые нормы обеспечения информационной безопасности

3.1. Институт имеет право определять состав, объем и порядок защиты сведений конфиденциального характера, персональных данных обучающихся, работников Института, требовать от своих сотрудников обеспечения сохранности и защиты этих сведений от внешних и внутренних угроз.

3.2. Институт обязан обеспечить сохранность конфиденциальной информации.

3.3. Администрация Института:

• назначает ответственного за обеспечение информационной безопасности;

• имеет право включать требования по обеспечению информационной безопасности в коллективный договор;

• имеет право включать требования по защите информации в договоры по всем видам деятельности;

• разрабатывает перечень сведений конфиденциального характера;

• имеет право требовать защиты интересов Института со стороны государственных и судебных инстанций.

3.4. Организационные и функциональные документы по обеспечению информационной безопасности:

• приказ ректора Института о назначении ответственного за обеспечение информационной безопасности;

• перечень защищаемых информационных ресурсов и баз данных;

• положения об обработке персональных данных работников и обучающихся Института, определяющие порядок предоставления информации сторонним организациям по их запросам, а также по правам доступа к ней сотрудников Института и др.

3.5. Порядок допуска сотрудников Института к информации предусматривает:

• принятие работником обязательств о неразглашении доверенных ему сведений конфиденциального характера;

• ознакомление работника с нормами законодательства РФ и Института об информационной безопасности и ответственности за разглашение информации конфиденциального характера;

• инструктаж работника специалистом по информационной безопасности;

4. Организация системы обеспечения информационной безопасности

4.1. В целях реализации стоящих перед системой обеспечения информационной безопасности задач в Институте устанавливаются:

• защита интеллектуальной собственности Института;

• защита компьютеров, локальных сетей и сети подключения к системе Интернета;

• всё программное обеспечение устанавливается только с разрешения ответственного за информационную безопасность;

• организация защиты конфиденциальной информации, в т. ч. персональных данных работников и обучающихся Института;

• учет всех носителей конфиденциальной информации;

• контроль за использованием электронных средств информационного обеспечения деятельности Института по прямому назначению;

• противодействие фактам использования при работе на электронных средствах информационного обеспечения деятельности Института нелицензированных программных продуктов и электронных носителей информации способных произвести заражение программного обеспечения вирусами;

• принятие мер к воспрещению доступа к информационным материалам, признанным в соответствии с действующим законодательством экстремистскими;

• обучение работников Института по вопросам обеспечения информационной безопасности.

5. Организация работы с информационными ресурсами и технологиями

5.1. Делопроизводство в Институте ведется работниками Общего отдела на основании инструкции по организации делопроизводства. Контроль за порядком его ведения возлагается на начальника общего отдела.

5.2. Система организации делопроизводства:

• учет всей документации Института, в т.ч. и на электронных носителях, с классификацией по сфере применения, дате, содержанию и т.п.;

• регистрация и учет всех входящих (исходящих) документов Института в специальном журнале информации о дате получения (отправления) документа, откуда поступил или куда отправлен, классификация (письмо, приказ, распоряжение и т. д.);

• особый режим уничтожения документов.

5.3. Всё программное обеспечение устанавливается только с разрешения ответственного за информационную безопасность.