УТВЕРЖДЕНО
приказом СПбГИПСР
от 28.05 2021 № 111

ИНСТРУКЦИЯ
по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных

1. Общие положения

1.1. Настоящая инструкция по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных (далее – Инструкция) в Санкт-Петербургском государственном автономном образовательном учреждении высшего образования «Санкт-Петербургский государственный институт психологии и социальной работы» (далее – Институт) определяет:

– права, обязанности и ответственность пользователей, допущенных к обработке персональных данных (далее – ПДн) в информационной системе персональных данных (далее – ИСПДн);

– функции, задачи и порядок эксплуатации пользователями средств вычислительной техники (далее - СВТ), входящих в состав ИСПДн.

1.2. Под персональными данными в соответствии с законодательством РФ понимается любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, необходимая Институту в связи с трудовыми отношениями и организацией образовательного процесса.

1.3. Пользователями ИСПДн являются все сотрудники Института, допущенные к обработке ПДн.

1.4. Требование обеспечения конфиденциальности при обработке персональных данных означает обязательное для соблюдения сотрудниками Института, допущенными к обработке персональных данных, и иными получившими доступ к персональным данным лицами, требование не допускать их распространения без согласия Субъекта персональных данных или наличия иного законного основания.

1.5. Должностные лица Института, работающие с персональными данными, обязаны использовать информацию о персональных данных исключительно для целей, связанных с выполнением своих трудовых обязанностей.

2. Меры по обеспечению безопасности

2.1. Пользователю ИСПДн устанавливаются соответствующие его полномочиям атрибуты управления доступом к ресурсу (диску, каталогу, файлу, принтеру, коммуникационным портам).

2.2. Начальными процедурами управления регистрацией пользователей в системе являются процедуры идентификации и аутентификации.

Каждому пользователю ИСПДн администратором безопасности информационных систем (далее – администратор безопасности ИС) назначается персональный идентификатор и пароль.

2.3. Для обеспечения необходимого уровня защищенности персональных данных при их обработке в информационных системах применяются следующие организационные меры:

2.3.1. обеспечение безопасности помещений, в которых размещены ИСПДн;

2.3.2. обеспечение сохранности носителей персональных данных;

2.3.3. утверждение перечня лиц, доступ которых к персональным данным, обрабатываемым в ИСПДн, необходим для выполнения ими служебных обязанностей;

2.3.4. использование средств защиты информации, которые прошли процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации;

2.3.5. проведение не реже 1 раза в 3 года проверки эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных, и регулярный контроль за выполнением требований к защите ПДн при обработке их в ИСПДн.

2.4. Устройства отображения и вывода информации (дисплей, принтер) в процессе эксплуатации ИСПДн устанавливаются с учетом исключения несанкционированного доступа к выводимой информации лицами, не имеющими к ней соответствующего допуска.

В случае невозможности выполнения указанных требований по размещению технических средств ИСПДн, должны приниматься дополнительные организационные и технические меры по исключению несанкционированного доступа к информации.

2.5. Изменение места расположения основных технических средств ИСПДн без согласования с администратором безопасности ИС запрещено.

2.6. При эксплуатации ИСПДн должно быть обеспечено непрерывное функционирование установленных средств защиты информации (при наличии) и антивирусного программного обеспечения.

2.7. В процессе работы с ПДн используются исключительно штатные технические средства ИСПДн.

2.8. Внесение пользователем самостоятельных изменений в аппаратно-программную конфигурацию ИСПДн категорически запрещено.

3. Права и обязанности пользователя

3.1. Пользователь обязан:

– выполнять требования настоящей Инструкции, а также требования организационно-технических и распорядительных документов в области защиты персональных данных;

– осуществлять обработку информации, содержащей персональные данные только на рабочих местах, принадлежащих Институту;

– соблюдать правила работы со средствами защиты информации в ИСПДн;

– докладывать администратору безопасности ИС о фактах нарушения требований настоящей Инструкции;

– знать штатные режимы работы программного обеспечения;

– использовать доступные защитные механизмы для обеспечения конфиденциальности и целостности своей информации;

– помнить личные пароли и идентификаторы;

– присутствовать при работах по внесению изменений в аппаратною программную конфигурацию закрепленного за ним автоматизированного рабочего места (далее – АРМ);

– ставить в известность администратора безопасности ИС, непосредственного руководителя при необходимости внесения изменений в состав аппаратных и программных средств АРМ;

– не допускать использования в ИСПДн неучтенных машинных носителей (флеш-дисков, CD, DVD, дискет);

– осуществлять уничтожение информации, содержащей персональные данные, цель обработки, которой достигнута, с машинных носителей информации и из памяти АРМ;

– ставить в известность администратора безопасности ИС, непосредственного руководителя в случае появления сведений или подозрений о фактах несанкционированного доступа к информации, своей или чужой, а также отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования узлов АРМ или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения;

– при прекращении выполнения трудовой функции, связанной с обработкой персональных данных, все носители информации, содержащие персональные данные (оригиналы и копии документов, машинные и бумажные носители и пр.), которые находились в распоряжении должностного лица в связи с выполнением должностных обязанностей, данный работник должен передать своему непосредственному руководителю.

3.2. Пользователь имеет право:

– использовать штатные программно-аппаратные средства ИСПДн для решения профессиональных задач;

– в случае необходимости передавать ПДн только с помощью корпоративных информационных систем;

– обращаться к администратору безопасности ИС с просьбой об оказании технической и методической помощи в работе по обеспечению безопасности информации;

– обращаться к администратору безопасности ИС с требованием о прекращении обработки ПДн в случаях нарушения установленной технологии обработки информации или выхода из строя средств защиты.

3.3. Пользователю запрещается:

– разглашать сведения о применяемых средствах защиты ПДн и содержание документов лицам, не имеющим отношения к проводимым работам;

– использовать служебные машинные носители информации для хранения информации, не имеющей отношения к выполняемым работам;

– выполнять работы с информацией на дому, выносить, отправлять, распечатывать, делать выписки из ИСПДн без согласования руководителя структурного подразделения;

– оставлять служебные машинные носители информации и документы бесконтрольно;

– передавать персональные данные по телефону, факсу, электронной почте за исключением случаев, установленных законодательством и действующими в Институте локальными нормативными актами;

– разрабатывать и/или использовать программы, с помощью которых можно получить несанкционированный доступ к ПДн, разработка и использование которых квалифицируется как попытка преднамеренного несанкционированного доступа к обрабатываемым данным;

– изменять или тиражировать установленное в ИСПДн программное обеспечение;

– фиксировать на любых носителях персональный пароль;

– передавать персональный идентификатор сторонним лицам;

– подключать к СВТ нештатные блоки и устройства;

– использовать компоненты программного и аппаратного обеспечения ИСПДн в неслужебных целях;

– проводить обработку информации в ИСПДн при неработоспособных или отключенных средствах защиты информации;

– оставлять свое рабочее место без присмотра, предварительно не заблокировав экран монитора (штатными средствами операционной системы Windows или Linux – комбинацией клавиш [WIN] + [L] или [CTRL] + [ALT] + [DEL] с дальнейшим нажатием кнопки «Блокировка» появившегося меню, либо при помощи штатных средств защиты информации от несанкционированного доступа при их наличии);

– самовольно подключать компьютер к корпоративной сети, изменять IP-адрес, MAC-адрес и иные настройки сети компьютера;

– разрешать работать под своей учетной записью на АРМ;

– получать доступ к сети Интернет любыми способами, например, при помощи несанкционированно установленных на АРМ модемов и т. п.

3.4 Оперативный контроль за действиями пользователей при работе в ИСПДн осуществляет администратор безопасности ИС, который имеет право приостановить обработку информации в случае выявления нарушений настоящей инструкции.

4. Порядок работы пользователя в ИСПДн

4.1. Доступ сотрудников СПбГИПСР осуществляется в следующем порядке:

4.1.1. Принимаемый сотрудник в соответствии с занимаемой должностью, должностной инструкцией, перечнем лиц, имеющих право доступа к персональным данным, наделяется приказом ректора правом доступа к персональным данным;

4.1.2. Начальник кадровой службы должен ознакомить работника с локальными нормативными актами СПбГИПСР в области персональных данных:

– Политикой в отношении обработки персональных данных;

– Положением об обработке и защите персональных данных абитуриентов и обучающихся;

– Положением об обработке и защите персональных данных работников;

– Порядком доступа в помещения Санкт-Петербургского государственного института психологии и социальной работы;

– Инструкцией по обработке персональных данных, осуществляемой без использования средств автоматизации;

– настоящей Инструкцией;

– обязательством о неразглашении персональных данных;

– иными локальными нормативными актами Института в области об обработке и защите персональных.

4.1.3. Принимаемый сотрудник должен под роспись ознакомится с документами, указанными в п. 4.1.2.

4.2. Пользователь обязан:

– перед началом обработки информации убедиться в том, что средства защиты включены и работоспособны;

– осуществлять вход в ИСПДн используя только личные идентификатор и пароль;

– при оставлении своего рабочего места блокировать экран монитора;

– после окончания работы в ИСПДн произвести полное выключение СВТ.

4.3. В случае поступления из сторонних организаций необходимой для работы информации на неучтенных электронных носителях пользователю необходимо:

– перед использованием произвести проверку электронного носителя на наличие вредоносного программного обеспечения с помощью установленных

средств антивирусного контроля;

– при выявлении наличия вредоносного программного обеспечения незамедлительно прекратить использование электронного носителя и доложить администратору безопасности ИС о данном факте.

5. Ответственность

5.1 Пользователь отвечает за соблюдение правил эксплуатации ИСПДн, сохранность информации, документов и электронных носителей информации, с которыми он работает.

5.2. Пользователь несет персональную ответственность за:

– соблюдение установленных законом и локальными нормативными актами Института требований по безопасности информации при обработке, копировании (уничтожении) персональных данных;

– использование неучтенных электронных носителей информации;

– несоблюдение правил использования электронных носителей информации, поступающих из сторонних организаций;

– правильность и полноту выполнения целей, задач, функций, прав и обязанностей, возложенных на него;

– сохранность сведений ограниченного распространения в соответствии с требованиями законодательства в области защиты персональных данных;

– выполнение указаний администратора безопасности ИС, касающихся работы в ИСПДн и защиты информации;

– обеспечение сохранности и неразглашение сведений о парольной защите ИСПДн;

– соблюдение технологии обработки защищаемой информации, неизменность условий обработки информации (размещение и/или состав технических средств обработки и защиты информации, состав используемого в ИСПДн программного обеспечения) в соответствии с организационно-технической документацией на ИСПДн;

– неисполнение или ненадлежащее исполнение обязанностей, предусмотренных настоящей инструкцией, в пределах, установленных законодательством Российской Федерации, а также за действия (бездействия), нарушающие права и законные интересы граждан и юридических лиц.

5.3. В случае выявления нарушений настоящей инструкции, учетная запись пользователя блокируется. Восстановление доступа производится по письменному распоряжению ректора Института.

5.4. Лица, виновные в нарушении норм в области персональных данных, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с действующим законодательством Российской Федерации.

5.5. С положениями настоящей Инструкции должны быть ознакомлены под роспись все работники структурных подразделений Института и лица, выполняющие работы по договорам и контрактам, имеющие отношение к обработке персональных данных.