УТВЕРЖДЕНО
приказом ректора ПГУ
№ 521 от 19.07.21

ИНСТРУКЦИЯ

пользователя информационной системы персональных данных

Настоящая Инструкция устанавливает порядок предоставления доступа к персональным данным (далее – ПД) в информационной системе персональных данных (далее – ИСПД) и обязанности пользователя ИСПД по обеспечению безопасности обрабатываемых в ней ПД, запреты на действия пользователя в ИСПД, а также права пользователя ИСПД.

1. Порядок предоставления доступа к информационной системе персональных данных

1.1 Работник ПГУ наделяется правом доступа к ПД в ИСПД в соответствии с занимаемой должностью, должностной инструкцией и/или на основании заявления руководителя подразделения.

1.2 Лицо, ответственное за оформление допуска работников к ИСПД обеспечивает организацию учета лиц, допущенных к работе с ПД, прав и паролей доступа.

1.3 Контроль за выполнением настоящей Инструкции возлагается на администратора информационной безопасности ИСПД.

2. Обязанности пользователя ИСПД

Пользователь обязан:

2.1 не реже 1 раза в год посещать раздел сайта ПГУ - работа с персональными данными (www.psu.ru /университет/ нормативное обеспечение/ нормативные акты ПГУ) для актуализации знаний в сфере обработки и защиты ПД;

2.2 Знать и соблюдать требования федерального закона “О персональных данных” и локальных актов ПГУ в сфере обработки и защиты ПД.

2.3 Исключить возможность неконтролируемого пребывания посторонних лиц в помещениях, где ведутся работы с ПД.

2.4 Руководствоваться требованиями организационно-распорядительных документов ИСПД. Строго соблюдать установленные правила обеспечения безопасности ПД при работе с программными и техническими средствами ИСПД.

2.5 Использовать ИСПД исключительно для выполнения служебных задач.

2.6 Использовать для доступа к ИСПД собственную уникальную учетную запись (логин и пароль).

2.7 Не допускать при работе с ИСПД просмотр посторонними лицами ПД, отображаемых на дисплее автоматизированного рабочего места (далее – АРМ ИСПД) или иных носителях.

2.8 Блокировать экран дисплея АРМ ИСПД парольной заставкой при оставлении рабочего места.

2.9 По всем вопросам, связанным с обеспечением защиты ПД, содержащихся в базах данных, и работе со средствами защиты информации, возникающими при работе в ИСПД, обращаться к администратору информационной безопасности.

2.10 Немедленно прекращать обработку ПД и ставить в известность администратора информационной безопасности при подозрении компрометации пароля, а также при обнаружении:

- несанкционированных изменений в конфигурации программных или аппаратных средств АРМ ИСПД;
- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ ИСПД, выхода из строя или неустойчивого функционирования АРМ ИСПД;
- непредусмотренных конфигурацией АРМ ИСПД отводов кабелей и подключенных устройств;
- сообщений от программного обеспечения антивирусной защиты о возможном вирусном заражении АРМ ИСПД или возникновении неисправностей (сбоев) в работе сервисов и информационных ресурсов ПГУ.
- других попыток несанкционированного доступа к ИСПД.

3. Действия, запрещенные пользователю ИСПД

Пользователю ИСПД запрещается:

3.1 Предоставлять доступ к информации, содержащей ПД, лицам, не допущенным к их обработке. Обрабатывать ПД в присутствии лиц, не допущенных к их обработке.

3.2 Осуществлять ввод ПД под диктовку.

3.3 Сообщать (или передавать) посторонним лицам личные ключи или атрибуты доступа к ресурсам ИСПД.

3.4 Копировать информацию, содержащую ПД на узлы сети, не входящие в ИСПД.

3.5 Выводить на печать информацию, содержащую ПД на принтеры, печать на которых не согласована с администратором информационной безопасности.

3.6 Осуществлять доступ к ИСПД с узлов сети, не назначенных администратором информационной безопасности в качестве АРМ ИСПД.

3.7 Самостоятельно изменять конфигурацию аппаратно-программных средств ИСПД.

3.8 Осуществлять действия по преодолению установленных ограничений на доступ к ИСПД.

3.9 Устанавливать на АРМ ИСПД программное обеспечение, не связанное с исполнением служебных обязанностей.

3.10 Привлекать посторонних лиц для производства ремонта или настройки АРМ ИСПД, без согласования с администратором информационной безопасности ИСПД.

4. Права пользователя ИСПД

Пользователь ИСПД имеет право:

4.1 Получать помощь по вопросам эксплуатации ИСПД от администратора информационной безопасности.

4.2 Обращаться к администратору информационной безопасности по вопросам дооснащения АРМ ИСПД техническими и программными средствами, не входящими в штатную конфигурацию АРМ ИСПД, необходимыми для автоматизации деятельности в соответствии с возложенными на него должностными обязанностями.

5. Правила работы в информационно-телекоммуникационных сетях международного информационного обмена

5.1 Работа в информационно-телекоммуникационных сетях международного информационного обмена - сети Интернет и других (далее – Сеть) на элементах ИСПД должна проводиться только при служебной необходимости.

5.2 При работе в Сети запрещается:

- осуществлять работу при отключенных средствах защиты (антивирусных, межсетевых экранов и других);
- передавать по Сети защищаемую информацию;
- скачивать из Сети программное обеспечение и другие файлы в неслужебных целях;
- посещать сайты сомнительной репутации (сайты, содержащие нелегально распространяемое программное обеспечение, сайты знакомств, онлайн игры и другие).

СОГЛАСОВАНО:

Проректор по учебной работе

Начальник правового отдела

Директор УЦИ