


УТВЕРЖДАЮ
Первый проректор ПетрГУ


С. П. КОРЖОВ
« 28 » _____ 2019 г.



Инструкция пользователя по обеспечению безопасности ИСПДн

СОГЛАСОВАНО

Зам. директора Регионального центра новых информационных технологий



С.А. Кипрушкин
« 28 » ноября 2019 г.

Начальник отдела телекоммуникаций и информационной безопасности регионального центра новых информационных технологий



А.А. Старикова
« 28 » ноября 2019 г.

СОГЛАСОВАНО

Начальник отдела программирования регионального центра новых информационных технологий


Я.Е. Штивельман
« 28 » ноября 2019 г.

Заведующий сектором системного программирования регионального центра новых информационных технологий


И.Л. Бурсин
« 28 » ноября 2019 г.

Петрозаводск, 2019.

1. Общие положения

Настоящая инструкция разработана для обеспечения защиты персональных данных в Петрозаводском государственном университете (ПетрГУ).

Пользователями информационной системы, предназначенной для обработки информации, содержащей персональные данные (далее ИСПДн), являются сотрудники, допущенные к работе в ИСПДн, в соответствии с приказом об утверждении списка лиц, которым необходим доступ к ПДн для выполнения служебных (трудовых) обязанностей.

Наиболее вероятными каналами утечки информации для информационных систем персональных данных (ИСПДн) являются:

- несанкционированный доступ к информации, обрабатываемой в ИСПДн;
- хищение документов или технических средств с хранящейся в них информацией, а также отдельных носителей информации;
- просмотр информации с экранов дисплеев мониторов и других средств ее отображения с помощью оптических устройств;
- воздействие на технические или программные средства в целях нарушения целостности (уничтожения, искажения) информации, работоспособности технических средств, средств защиты информации, адресности и своевременности обмена, в том числе электромагнитного, через специально внедренные электронные и программные средства («закладки»).

Работа с персональными данными строится на следующих принципах:

- принцип персональной ответственности - в любой момент времени за каждый документ (не зависимо от типа носителя: бумажный, электронный) должен отвечать и распоряжаться конкретный работник;
- принцип контроля и учета - все операции с документами должны отражаться в соответствующих журналах (передача из рук в руки, снятие копии и т.п.).

2. Обязанности работников, имеющих доступ к ПДн

Работники, получившие доступ к персональным данным, обязаны хранить в тайне сведения ограниченного распространения, ставшие им известными во время работы или иным путем, и пресекать действия других лиц, которые могут привести к разглашению такой информации. О таких фактах, а также о других причинах или условиях возможной утечки персональных данных немедленно информировать руководителя структурного подразделения, руководителя отдела информационной безопасности.

Персональные данные не подлежат разглашению (распространению). Прекращение доступа к такой информации не освобождает работника от взятых им обязательств по неразглашению сведений ограниченного распространения.

В случае оставления занимаемой должности работник обязан вернуть все документы и материалы, относящиеся к деятельности подразделения, организации. В том числе: отчеты, инструкции, переписку, списки работников, компьютерные программы, а также все прочие материалы и копии названных материалов, имеющих какое-либо отношение к деятельности ПетрГУ, полученные в течение срока работы.

Работники при работе с персональными данными обязаны:

- строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн;

- выполнять требования администратора безопасности, касающиеся защиты информации;
- знать и строго выполнять правила работы со средствами защиты информации (средствами разграничения доступа), используемыми на персональных компьютерах;
- хранить в тайне свой аутентификатор (пароль доступа в автоматизированную систему, либо ключевой носитель), а также информацию о системе защиты, установленной в ИСПДн;
- контролировать обновление антивирусных баз и в случае необходимости сообщать о необходимости обновления администратору безопасности, ответственному за антивирусную защиту автоматизированной системы;

Немедленно ставить в известность руководителя подразделения, руководителя сектора информационной безопасности:

- при подозрении компрометации личных ключей и паролей;
- нарушений целостности пломб (наклеек с защитной и идентификационной информацией, нарушении или несоответствии номеров печатей) на аппаратных средствах ПЭВМ или иных фактов совершения в его отсутствие попыток несанкционированного доступа (НСД) к защищенной ИСПДн;
- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ИСПДн.
- в случае отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию рабочей станции, выхода из строя или неустойчивого функционирования узлов ПЭВМ или периферийных устройств (принтера и т.п.), а также перебоев в системе электроснабжения, некорректного функционирования установленных в автоматизированной системе технических средств защиты ставить в известность ответственного за техническое обслуживание и (или) ответственного за обслуживание программного обеспечения.

Ставить в известность сотрудников отдела технического обслуживания компьютерной техники или сотрудников отдела информационной безопасности при:

- необходимости обновления антивирусных баз;
- обновлении программного обеспечения;
- проведении регламентных работ, модернизации аппаратных средств или изменении конфигурации ИСПДн;
- необходимости вскрытия системных блоков персональных компьютеров входящих в состав ИСПДн;
- резервном копировании информации;
- и т.д.

Вынос ПЭВМ, на которой проводилась обработка персональных данных, за пределы территории здания с целью их ремонта, замены и т. п. без согласования с руководителем подразделения, запрещен.

ПЭВМ, используемые для работы с персональными данными, должны быть размещены таким образом, чтобы исключалась возможность визуального просмотра экрана

видеомонитора, не имеющими отношения к конкретно обрабатываемой информации работниками.

Запрещается:

- передавать, кому бы то ни было (в том числе родственникам) устно или письменно сведения ограниченного распространения;
- использовать сведения ограниченного распространения при подготовке открытых публикаций, докладов, научных работ и т.д.;
- выполнять работы с документами ограниченного распространения на дому, выносить их из служебных помещений, снимать копии или производить выписки из таких документов без разрешения руководителя;
- передавать или принимать без расписки документы ограниченного распространения;
- оставлять на рабочих столах, в столах и незакрытых сейфах документы ограниченного распространения, а также оставлять незапертыми и неопечатанными после окончания работы сейфы, помещения и хранилища с документами конфиденциального характера.
- использовать компоненты программного и аппаратного обеспечения ИСПДн подразделения в неслужебных целях;
- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств рабочих станций или устанавливать дополнительно любые программные и аппаратные средства;
- осуществлять обработку персональных данных в присутствии посторонних (не допущенных к данной информации) лиц;
- записывать и хранить персональные данные на неучтенных съемных носителях информации;
- оставлять включенной без присмотра свою рабочую станцию (ПЭВМ), не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации. Об обнаружении такого рода ошибок - ставить в известность руководителя своего подразделения, ответственного за техническое и (или) программное обеспечение, сотрудников отдела информационной безопасности.

3. Ответственность

Пользователь несет ответственность за соблюдение требований настоящей инструкции, а также других нормативных документов в области защиты информации. За разглашение информации ограниченного распространения, а также за нарушение порядка работы с документами или машинными носителями, содержащими такую информацию, работники могут быть привлечены к дисциплинарной или иной, предусмотренной законодательством ответственности.

За разглашение информации ограниченного распространения, нарушение порядка работы с документами или машинными носителями, содержащими такую информацию, работники могут быть привлечены к дисциплинарной или иной, предусмотренной законодательством ответственности.