Приложение Б
к Положению о защите
информации СФУ
(утверждено приказом
от 25.02.2015 № 200)

Инструкция
по защите информации работнику СФУ

Работник обязан:

1 Знать и строго выполнять требования по эксплуатации технических средств, вверенных ему в пользование, нормативных документов по ведению делопроизводства, технологии обработки (передачи) и защиты информации.

2 Работать только с теми служебными документами и сведениями, а также техническими средствами, к которым он получил доступ в силу своих служебных обязанностей.

3 Не разглашать ставшую известной ему по службе или иным путём конфиденциальную информацию СФУ.

4 Обеспечить сохранность доверенных ему по службе документов, как на бумажной основе, так и машинных носителей информации (флэш-накопители, внешние накопители на жестких дисках, компакт-диски, иные устройства, фото-, кино-, видео- и аудиопленки, и др.), вести их учёт и хранение в установленном порядке.

5 Обеспечить сохранность ключевого носителя (электронного идентификатора), периодически менять на нем пароль, не передавать ключ другим лицам, не оставлять его без присмотра, в случае утраты ключа необходимо немедленно сообщить об этом администратору.

6 Соблюдать требования Инструкция по парольной защите при работе на средствах вычислительной техники (Приложение М).

7 Содержать на рабочем месте мониторы, печатающие устройства, а также конфиденциальные документы таким образом, чтобы исключить визуальный просмотр информации посторонними (посетителями).

8 Перед началом работы на ПЭВМ проверять наличие и работоспособность антивирусных программ, следить за их своевременным обновлением. Все электронные носители информации перед их применением проверять на наличие вирусов.

9 Оставляя рабочее место независимо от времени, активизировать временную блокировку экрана монитора и клавиатуры ПЭВМ.

10 Ставить в известность руководителя подразделения и сетевого администратора (администратора АС) обо всех подозрительных ситуациях (нарушение функционирования средств вычислительной техники, АС, изменение конфигурации программного обеспечения, наличие вируса и т. п.).

11 Передавать служебные документы только своему руководителю, адресату, ответственному за делопроизводство или другим лицам по указанию своего руководителя. Конфиденциальные документы передавать только под подпись установленным порядком.

12 Служебный электронный документооборот вести только с ящиков электронной почты, зарегистрированных в домене университета.

13 По согласованию с руководителем подразделения установленным порядком создавать и хранить резервные копии конфиденциальной и открытой ценной (важной) информации.

14 Пресекать действия посторонних лиц (посетителей) и других работников, направленные на разглашение конфиденциальной информации, создание предпосылок к нарушению ее безопасности, а также на несанкционированный доступ к доверенной ему

служебной информации, требовать от них соблюдения установленного порядка в служебном помещении. В случае невыполнения этих требований сообщать своему руководителю и в дежурно-диспетчерскую службу.

15 Не выносить из служебного помещения конфиденциальные документы и другие носители конфиденциальной информации без разрешения (распоряжения) своего руководителя.

16 Не допускать без разрешения (распоряжения) своего руководителя к работе на технических средствах (вычислительная и оргтехника, средства связи и др.), а также к контрольно-техническим, ремонтно-строительным и другим работам в служебном помещении посторонних (посетителей, работников не своего подразделения).

17 Не оставлять в служебном помещении при выходе из него посторонних (посетителей) одних, а конфиденциальные документы – доступными для других работников и посторонних (посетителей).

18 Никому не сообщать конфиденциальную информацию по телефону, факсу, электронной почте.

19 Не устанавливать, не удалять, не копировать, не переименовывать программное обеспечение без согласования с руководителем своего подразделения и системным администратором.

20 Не сообщать свои пароли и идентификаторы другим лицам, хранить их записанными только в местах, недоступных для других.

21 Использовать мобильные электронные устройства (ноутбук, блокнотный, планшетный, портативный компьютер, личный цифровой помощник (персональный цифровой секретарь), радиоприемники, радиопередатчики, средства аудио, фото, видеозаписи, средства мобильной связи и др.) при проведении служебных совещаний, конференций, собраний, учебных занятий и других массовых мероприятий в помещениях университета только с разрешения руководителя подразделения или проводимого мероприятия. Перед проведением мероприятий указанные средства отключать.

22 Не осуществлять действия, направленные на несанкционированный доступ в другие средства вычислительной техники, вычислительные и радиосети, воздействие на инфракрасные и другие электронные системы.

За нарушение требований настоящей инструкции работник несёт ответственность в соответствии с действующим законодательством Российской Федерации.