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

Инструкция
по защите информации
руководителю структурного подразделения СФУ

Руководитель структурного подразделения отвечает за организацию и проведение необходимых мероприятий по защите информации в подразделении и выполнение всех требований нормативных документов по защите информации работниками (обучающимися) подразделения.

Руководитель подразделения обязан:

1 Знать и строго выполнять требования локальных нормативных актов, других документов по защите информации; во взаимодействии с ОЗИ организовать и обеспечить функционирование системы защиты информации подразделения; все разрабатываемые документы, касающиеся вопросов защиты информации, согласовывать с ОЗИ.

2 Определять ответственному за защиту информации в подразделении его функции, исходя из своих обязанностей в части организации защиты информации.

3 Контролировать выполнение работниками подразделения (обучающимися) требований по защите информации.

4 Готовить проект приказа об организации защиты информации, другие необходимые документы и утверждать их установленным порядком; в дальнейшем при изменениях в организационной и инфраструктуре, кадровых изменениях своевременно вносить изменения в эти документы.

5 В соответствии с Перечнем сведений, составляющих конфиденциальную информацию СФУ, и номенклатурой дел подразделения формировать и периодически уточнять в подразделении Список информационных ресурсов подразделения, содержащих конфиденциальную информацию СФУ, и утверждать его установленным порядком.

6 Осуществлять подбор работников, допускаемых к работе с конфиденциальной информацией, определять, какая информация и в каком объеме необходима для исполнения ими служебных обязанностей, их полномочия. Формировать Список работников подразделения, допущенных к работе с конфиденциальной информацией, и утверждать его установленным порядком.

7 Допускать к работе с конфиденциальной информацией, необходимой для исполнения служебных обязанностей, работников, изучивших требования нормативных документов по защите информации, в соответствии со Списком.

8 Определять в каких помещениях есть служебная необходимость хранить и обрабатывать конфиденциальную информацию, формировать Список защищаемых помещений подразделения, утверждать его установленным порядком.

9 Организовать и поддерживать в подразделении режим допуска в защищаемые помещения, к техническим средствам обработки информации и к информационным ресурсам. Назначать установленным порядком ответственных за защищаемые помещения и лиц, допущенных к их вскрытию (закрытию). Оформлять технические паспорта на защищаемые помещения, своевременно вносить в них изменения.

10 Закреплять за работниками подразделения автоматизированные рабочие места, средства вычислительной техники и другие технические средства обработки и передачи информации.

11 Допускать работников к исполнению служебных обязанностей только после изучения ими Инструкции работнику (руководителю структурного подразделения) по защите информации, Перечня сведений, составляющих конфиденциальную информацию СФУ и других документов по согласованию с ОЗИ, в дальнейшем документы доводить не реже одного раза в год.

12 Определять работникам задачи и обязанности, организовать проведение инструктажей и занятий с ними по вопросам защиты информации, прививать им правила и нормы служебной этики, направленные на обеспечение информационной безопасности.

13 Принимать меры по предотвращению случаев разглашения (утечки) конфиденциальной информации и утраты документов, проводить постоянную работу по выявлению возможных каналов утечки информации и их закрытию, по совершенствованию системы защиты информации.

14 Определять порядок использования мобильных электронных устройств в ЗП, при проведении служебных совещаний, конференций, собраний, учебных занятий и других массовых мероприятий с учетом требований настоящего Положения. Перед проведением мероприятий требовать от присутствующих отключать средства мобильной связи, а в случае необходимости и другие устройства.

15 Организовать и поддерживать систему парольной защиты информации в средствах вычислительной техники в соответствии с инструкцией (Приложение М).

16 Организовать резервное копирование и архивирование конфиденциальной и открытой ценной (важной) информации.

17 Согласовывать проведение работ по созданию, модернизации и внедрению объектов информатизации, а также все проводимые мероприятия и принимаемые меры по защите информации с ОЗИ.

18 В случае нарушения технологии обработки конфиденциальной информации, обнаружения утечки или предпосылок к утечке конфиденциальной информации и несанкционированного доступа к ней информировать об этом ОЗИ, принимать меры по их пресечению.

19 Предоставлять сотрудникам ОЗИ затребованную информацию, беспрепятственно допускать их к объектам информатизации и информационным ресурсам подразделения в соответствии с их должностными обязанностями и полномочиями.

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