Приложение № 2
к Положению об информационной безопасности информационных систем персональных данных Южного федерального университета, утвержденному приказом Южного федерального университета
от 19.04. 2012 г. № 68-ОД

ТИПОВАЯ ИНСТРУКЦИЯ АДМИНИСТРАТОРА ИСПДН

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Администратор информационной системы персональных данных (ИСПДн) (далее – Администратор) назначается приказом ректора (руководителя обособленного структурного подразделения) Южного федерального университета.

1.2 Администратор подчиняется руководителю структурного подразделения эксплуатирующего ИСПДн.

1.3 Администратор ИСПДн в своей работе руководствуется требованиями законодательства о персональных данных, нормативными документами ФСТЭК России, локальными нормативными актами Южного федерального университета и настоящей инструкцией.

1.4 Администратор отвечает за обеспечение устойчивой работоспособности элементов ИСПДн и средств защиты при обработке персональных данных.

1.5 Методическое руководство работой Администратора осуществляется ответственным за обеспечение защиты персональных данных.

II. ФУНКЦИОНАЛЬНЫЕ ОБЯЗАННОСТИ

2.1 Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, распоряжений, регламентирующих порядок действий по защите информации.

2.2 Обеспечивать установку, настройку и своевременное обновление элементов ИСПДн:

программного обеспечения автоматизированных рабочих мест (АРМ) и серверов (операционные системы, прикладное и специальное программное обеспечение (ПО));

аппаратных средств;

аппаратных и программных средств защиты.

2.3 Обеспечивать работоспособность элементов ИСПДн и локальной вычислительной сети.

2.4 Осуществлять контроль за порядком учета, создания, хранения и использования резервных и архивных копий массивов данных, машинных (выходных) документов.

2.5 Обеспечивать функционирование и поддерживать работоспособность средств защиты.

2.6 В случае отказа работоспособности технических средств и программного обеспечения элементов ИСПДн, в том числе средств защиты информации, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

2.7 Проводить периодический контроль принятых мер по защите (в пределах возложенных на него функциональных обязанностей).

2.8 Хранить, осуществлять прием и выдачу персональных паролей пользователей, осуществлять контроль за правильностью использования персонального пароля Оператором ИСПДн.

2.9 Обеспечивать постоянный контроль за выполнением пользователями установленного комплекса мероприятий по обеспечению безопасности информации.

2.10 Информировать ответственного за обеспечение защиты персональных данных о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам ИСПДн.

2.11 Требовать прекращения обработки информации, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИСПДн или средств защиты.

2.12 Обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств и отправке их в ремонт. Техническое обслуживание и ремонт средств вычислительной техники, предназначенных для обработки персональных

данных, проводятся организациями, имеющими соответствующие лицензии. При проведении технического обслуживания и ремонта запрещается передавать ремонтным организациям узлы и блоки с элементами накопления и хранения информации. Вышедшие из строя элементы и блоки средств вычислительной техники заменяются на элементы и блоки, прошедшие специальные исследования и специальную проверку (для аттестованных по требованиям безопасности информации объектов информатизации) с обязательным уведомлением о проведенном ремонте органа по аттестации выдавшего Аттестат соответствия.

2.13 Лично присутствовать при выполнении технического обслуживания элементов ИСПДн, привлеченными специалистами и организациями.

2.14 Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий.

III. ПРАВА И ОТВЕТСТВЕННОСТЬ

3.1 Администратор ИСПДн имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн, в том числе производить установку и настройку элементов ИСПДн, контролировать и поддерживать работоспособность ИСПДн и выполнять прочие действия в рамках функциональных обязанностей.

3.2 За несоблюдение положений настоящей инструкции администратор ИСПДн несет ответственность в соответствии с действующим законодательством РФ.

Приложение № 3
к Положению об информационной безопасности информационных систем персональных данных Южного федерального университета, утвержденному приказом Южного федерального университета
от 19.04. 2012 г. № 68-01

ТИПОВАЯ ИНСТРУКЦИЯ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ ИСПДН

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Администратор безопасности информационных систем персональных данных (ИСПДн) (далее – Администратор) назначается приказом ректора (руководителя обособленного структурного подразделения) Южного федерального университета.

1.2 Администратор подчиняется руководителю структурного подразделения эксплуатирующего ИСПДн.

1.3 Администратор безопасности в своей работе руководствуется требованиями законодательства о персональных данных, нормативными документами ФСТЭК России, локальными нормативными актами Южного федерального университета и настоящей инструкцией.

1.4 Администратор отвечает за поддержание необходимого уровня безопасности объектов защиты ИСПДн.

1.5 Администратор безопасности является ответственным лицом структурного подразделения, эксплуатирующего ИСПДн, Южного федерального университета, уполномоченным на проведение работ по технической защите информации и поддержанию достигнутого уровня защиты ИСПДн и ее ресурсов при эксплуатации и модернизации.

1.6 Администратор безопасности должен иметь специальное рабочее место, размещенное в структурном подразделении, эксплуатирующим ИСПДн, таким образом, что бы исключить несанкционированный доступ к нему посторонних лиц и других пользователей.

1.7 Рабочее место Администратора безопасности должно быть оборудовано средствами физической защиты (личный сейф, шкаф или надежно закрепленный ящик, оборудованные замком и приспособлением

для опечатывания), подключением к ИСПДн, а так же средствами контроля за техническими средствами защиты (при необходимости).

1.8 Администратор безопасности осуществляет методическое руководство Операторов и Администраторов ИСПДн, в вопросах обеспечения безопасности персональных данных.

1.9 Требования администратора информационной безопасности, связанные с выполнением им своих функциональных обязанностей, обязательны для исполнения всеми пользователями ИСПДн.

1.10 Администратор безопасности несет персональную ответственность за качество проводимых им работ по контролю действий пользователей при работе в ИСПДн, состояние и поддержание установленного уровня защиты ИСПДн.

II. ФУНКЦИОНАЛЬНЫЕ ОБЯЗАННОСТИ

Администратор безопасности обязан:

знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, распоряжений, регламентирующих порядок действий по защите информации;

осуществлять установку, настройку и сопровождение технических средств защиты;

участвовать в контрольных и тестовых испытаниях и проверках элементов ИСПДн;

участвовать в приеме новых программных средств;

обеспечить доступ к защищаемой информации пользователям ИСПДн согласно их правам доступа при получении оформленного соответствующим образом разрешения;

уточнять в установленном порядке обязанности пользователей ИСПДн по обработке объектов защиты;

вести контроль над процессом осуществления резервного копирования объектов защиты;

осуществлять контроль над выполнением Плана мероприятий по защите персональных данных;

анализировать состояние защиты ИСПДн и ее отдельных подсистем;

контролировать неизменность состояния средств защиты их параметров и режимов защиты;

контролировать физическую сохранность средств и оборудования ИСПДн;

контролировать исполнение пользователями ИСПДн введенного режима безопасности, а так же правильность работы с элементами ИСПДн и средствами защиты;

контролировать исполнение пользователями парольной политики;

контролировать работу пользователей в сетях общего пользования и (или) международного обмена «Интернет» (при наличии такого подключения);

своевременно анализировать журнал учета событий, регистрируемых средствами защиты, с целью выявления возможных нарушений;

не допускать установку, использование, хранение и размножение в ИСПДн программных средств, не связанных с выполнением функциональных задач;

не допускать к работе на элементах ИСПДн посторонних лиц;

осуществлять периодические контрольные проверки рабочих станций и тестирование правильности функционирования средств защиты ИСПДн;

оказывать помощь пользователям ИСПДн в части применения средств защиты и консультировать по вопросам введенного режима защиты;

периодически представлять руководству структурного подразделения отчет о состоянии защиты ИСПДн, о нештатных ситуациях на объектах ИСПДн и допущенных пользователями нарушениях установленных требований по защите информации;

в случае отказа работоспособности технических средств и программного обеспечения ИСПДн, в том числе средств защиты принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности;

принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий.

III. ПРАВА И ОТВЕТСТВЕННОСТЬ

3.1 Администратор безопасности имеет право в отведенное ему время решать поставленные задачи в соответствии с его полномочиями в отношениях к ресурсам ИСПДн и вверенным ему техническим и

программным средствам. В частности, Администратор безопасности имеет право:

проверять электронный журнал обращений;

вносить изменения в конфигурацию аппаратно-программных средств;

проверять соблюдение условий использования средств защиты информации;

требовать прекращения обработки информации как в целом, так и отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования АРМ.

3.2 За несоблюдение положений настоящей инструкции администратор безопасности ИСПДн несет ответственность в соответствии с действующим законодательством РФ.

Приложение № 4
к Положению об информационной безопасности информационных систем персональных данных Южного федерального университета, утвержденному приказом Южного федерального университета
от 19.04. 2012 г. № 68-09

ТИПОВАЯ ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЯ АРМ ИСПДН

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Пользователь АРМ информационных систем персональных данных (ИСПДн) (далее – Пользователь) осуществляет обработку персональных данных в информационной системе персональных данных.

1.2 Пользователем является работник Южного федерального университета, участвующий в процессах обработки ПДн, имеющий доступ к аппаратным средствам, программному обеспечению и средствам защиты, установленном на АРМ, к персональным данным в рамках своих функциональных обязанностей.

1.3 Пользователь несет персональную ответственность за свои действия.

1.4 Пользователь в своей работе руководствуется требованиями законодательства о персональных данных, нормативными документами ФСТЭК России, локальными нормативными актами Южного федерального университета и настоящей инструкцией.

1.5 Методическое руководство работой пользователя осуществляется ответственным за обеспечение защиты персональных данных структурного подразделения, эксплуатирующего ИСПДн, Южного федерального университета.

II. ФУНКЦИОНАЛЬНЫЕ ОБЯЗАННОСТИ

2.1 Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций и распоряжений, регламентирующих порядок действий по защите информации.

2.2 Выполнять на автоматизированном рабочем месте (АРМ) только те процедуры, которые определены для него инструкцией.

2.3 Знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности ПДн, а также руководящих и организационно-распорядительных документов.

2.4 Соблюдать требования парольной политики.

2.5 Соблюдать установленные правила при работе в сетях общего доступа и (или) международного обмена – Интернет и других.

2.6 Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).

2.7 Обо всех выявленных нарушениях, связанных с информационной безопасностью структурного подразделения, эксплуатирующего ИСПДн, а так же для получений консультаций по вопросам информационной безопасности, необходимо обратиться к Администратору безопасности ИСПДн *(наименование структурного подразделения)* *(Фамилия, Имя, Отчество)* в *(кабинет №)* по электронной почте: *(e-mail)* или по внутреннему телефону _____.

2.8 Для получения консультаций по вопросам работы и настройке элементов ИСПДн необходимо обращаться к Администратору ИСПДн *(Фамилия, Имя, Отчество)* по внутреннему телефону _____.

2.9 При необходимости покинуть рабочее место на короткое время, немедленно заблокировать доступ к компьютеру. (Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl> <Alt> <Del> и выбрать опцию <Блокировка>).

2.10 Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий, в пределах возложенных на него функций.

2.11 Пользователям запрещается:

разглашать защищаемую информацию третьим лицам;

копировать защищаемую информацию на внешние носители без разрешения своего руководителя;

самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;

несанкционированно открывать общий доступ к папкам на своей рабочей станции;

подключать к рабочей станции и внутренней локальной информационной сети личные внешние носители и мобильные устройства;

отключать (блокировать) средства защиты информации;

обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к ИСПДн;

сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн;

привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с ответственным за обеспечение защиты персональных данных.

III. ОРГАНИЗАЦИЯ ПАРОЛЬНОЙ ЗАЩИТЫ

3.1 Личные пароли доступа к элементам ИСПДн выдаются пользователям Администратором информационной безопасности, Администратором ИСПДн или создаются самостоятельно.

3.2 Полная плановая смена паролей в ИСПДн проводится не реже одного раза в 3 месяца.

3.3 Правила формирования пароля:

пароль не может содержать имя учетной записи пользователя или какую-либо его часть;

пароль должен состоять не менее чем из 8 символов;

в пароле должны присутствовать символы трех категорий из числа следующих четырех:

- прописные буквы английского алфавита от A до Z;
- строчные буквы английского алфавита от a до z;
- десятичные цифры (от 0 до 9);
- символы, не принадлежащие алфавитно-цифровому набору (например, !, $, #, %).

запрещается использовать в качестве пароля имя входа в систему, простые пароли типа «123», «111», «qwerty» и им подобные, а так же данные которые можно определить, основываясь на информации о пользователе,

запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;

запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);

запрещается выбирать пароли, которые уже использовались ранее.

3.4 Правила ввода пароля:

ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан;

во время ввода паролей необходимо исключить возможность ознакомления с ним посторонних лиц или технических средств (видеокамеры и др.).

3.5 Правила хранение пароля:

запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах;

запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

3.6 Лица, использующие паролирование, обязаны:

четко знать и строго выполнять требования настоящей инструкции и других руководящих документов по паролированию;

своевременно сообщать Администратору информационной безопасности об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

IV. ПРАВИЛА РАБОТЫ В СЕТЯХ ОБЩЕГО ДОСТУПА И (ИЛИ) МЕЖДУНАРОДНОГО ОБМЕНА

4.1. Работа в сетях общего доступа и (или) международного обмена (сети Интернет и других) (далее – Сеть) на элементах ИСПДн, должна проводиться при необходимости.

4.2. При работе в Сети запрещается:

осуществлять работу при отключенных средствах защиты (антивирус и других);

передавать по Сети защищаемую информацию без использования сертифицированных средств шифрования;

запрещается скачивать из Сети программное обеспечение и другие файлы;

запрещается посещение сайтов сомнительной репутации (порно-сайты, сайты, содержащие нелегально распространяемое ПО и другие);

запрещается нецелевое использование подключения к Сети.

V. ПРАВА И ОТВЕТСТВЕННОСТЬ

5.1 Пользователь имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн.

5.2 За несоблюдение положений настоящей инструкции администратор ИСПДн несет ответственность в соответствии с действующим законодательством РФ.