Приложение № 1
к Положению об информационной безопасности информационных систем персональных данных Южного федерального университета, утвержденному приказом Южного федерального университета
от 19.04. 2012 г. № 68-01

Таблица. Соответствие функций подсистем СЗПДн классу защищенности.

№	План - перечень технических мероприятий по обеспечении безопасности ИСПДн	Класс защищенности К3	Класс защищенности К2	Класс защищенности К1
I.	В подсистеме управления доступом:			
1	Реализовать идентификацию и проверку подлинности субъектов доступа при входе в операционную систему ИСПДн по паролю условно-постоянного действия, длиной не менее шести буквенно-цифровых символов.	+	+	+
2	Реализовать идентификацию терминалов, технических средств, узлов ИСПДн, каналов связи, внешних устройств по их логическим именам.	-	-	При многопользовательском режиме
3	Реализовать идентификацию программ, томов, каталогов, файлов, записей, полей записей по именам.	-	-	При многопользовательском режиме
4	Реализовать контроль доступа пользователей к защищаемым ресурсам в соответствии с матрицей доступа.	-	-	При многопользовательском режиме и разных правах доступа

№	План - перечень технических мероприятий по обеспечении безопасности ИСПДн	Класс защищенности К3	Класс защищенности К2	Класс защищенности К1
II. В подсистеме регистрации и учета:				
5	Осуществлять регистрацию входа (выхода) пользователя в систему (из системы), либо регистрацию загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения ИСПДн. В параметрах регистрации указываются:			
	Дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы;	При однопользовательском режиме	При однопользовательском режиме	-
	Дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы, результат попытки входа (успешная или неуспешная);	При многопользовательском режиме и равных правах доступа	При многопользовательском режиме и равных правах доступа	При однопользовательском и многопользовательском режимах обработки и равных правах доступа
6	Дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы, результат попытки входа (успешная или неуспешная), идентификатор (код или фамилия) пользователя, предъявленный при попытке доступа;	При многопользовательском режиме и разных правах доступа	При многопользовательском режиме и разных правах доступа	-
	Дата и время входа (выхода) пользователя в систему (из системы) или загрузки (остановка) системы, результат попытки входа (успешная или неуспешная), идентификатор (код или фамилия) пользователя, предъявленный при попытке доступа, код или пароль, предъявленный при	-	-	При многопользовательском режиме и разных правах доступа

№	План - перечень технических мероприятий по обеспечении безопасности ИСПДн	Класс защищенности К3	Класс защищенности К2	Класс защищенности К1
	неуспешной попытке.			
7	Проводить учет всех защищаемых носителей информации с помощью их маркировки:			
	С занесением учетных данных в журнал учета;	При однопользовательском и многопользовательском режимах и равных правах доступа	При однопользовательском и многопользовательском режимах и равных правах доступа	При однопользовательском режиме
	С занесением учетных данных в журнал учета с пометкой об их выдаче (приеме);	При многопользовательском режиме и разных правах доступа	При многопользовательском режиме и разных правах доступа	При многопользовательском режиме
8	Проводить дублирующий учет защищаемых носителей информации.	-	-	При однопользовательском и многопользовательском режимах и равных правах доступа

№	План - перечень технических мероприятий по обеспечении безопасности ИСПДн	Класс защищенности К3	Класс защищенности К2	Класс защищенности К1
9	Осуществлять регистрацию выдачи печатных (графических) документов на бумажный носитель. В параметрах регистрации указываются:			
	Дата и время выдачи (обращения к подсистеме вывода), краткое содержание документа (наименование, вид, код), спецификация устройства выдачи (логическое имя (номер) внешнего устройства);	-	-	При однопользовательском режиме
	Дата и время выдачи (обращения к подсистеме вывода), спецификация устройства выдачи (логическое имя (номер) внешнего устройства), краткое содержание документа (наименование, вид, шифр, код), идентификатор пользователя, запросившего документ.	-	-	При многопользовательском режиме
10	Осуществлять регистрацию запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки персональных данных. В параметрах регистрации указываются дата и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор пользователя, запросившего программу (процесс, задание), результат запуска (успешный, неуспешный).	-	-	При многопользовательском режиме

№	План - перечень технических мероприятий по обеспечении безопасности ИСПДн	Класс защищенности К3	Класс защищенности К2	Класс защищенности К1
11	Осуществлять регистрацию попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются дата и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор пользователя, спецификация защищаемого файла.	-	-	При многопользовательском режиме
12	Осуществлять регистрацию попыток доступа программных средств к дополнительным защищаемым объектам доступа (терминалам, техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей). В параметрах регистрации указываются дата и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная), идентификатор пользователя, спецификация защищаемого объекта (логическое имя (номер)).	-	+	+
13	Осуществлять очистку (обнуление, обезличивание) освобождаемых областей оперативной памяти информационной системы и внешних носителей информации.	-	-	+

№	План - перечень технических мероприятий по обеспечении безопасности ИСПДн	Класс защищенности К3	Класс защищенности К2	Класс защищенности К1
III. В подсистеме обеспечения целостности:				
14	Обеспечить целостность программных средств защиты в составе СЗПДн, а также неизменность программной среды. При этом целостность средств защиты проверяется:			
	При загрузке системы по наличию имен (идентификаторов) компонентов СЗПДн, целостность программной среды обеспечивается отсутствием в ИСПДн средств разработки и отладки программ во время обработки и (или) хранения защищаемой информации;	При однопользовательском и многопользовательском режимах и равных правах доступа	При однопользовательском и многопользовательском режимах и равных правах доступа	При однопользовательском и многопользовательском режимах и равных правах доступа
	При загрузке системы по контрольным суммам компонентов средств защиты информации, а целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации.	При многопользовательском режиме и разных правах доступа	При многопользовательском режиме и разных правах доступа	При многопользовательском режиме обработки и разных правах доступа
15	Осуществлять физическую охрану технических средств информационной системы (устройств и носителей информации), предусматривающую постоянное наличие охраны территории и здания.	-	-	При однопользовательском и многопользовательском режимах и равных правах доступа

№	План - перечень технических мероприятий по обеспечении безопасности ИСПДн	Класс защищенности К3	Класс защищенности К2	Класс защищенности К1
16	Осуществлять физическую охрану ИСПДн (устройств и носителей информации), предусматривающую контроль доступа в помещения ИСПДн посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения ИСПДн и хранилище носителей информации.	+	+	При многопользовательском режиме обработки и разных правах доступа
17	Проводить периодическое тестирование функций СЗПДн при изменении программной среды и пользователей ИСПДн с помощью тест-программ, имитирующих попытки НСД.	+	+	+
18	Должны быть в наличии средства восстановления СЗПДн, предусматривающие ведение двух копий программных средств защиты информации, их периодическое обновление и контроль работоспособности.	+	+	+
IV. Требования к средствам межсетевого экранирования при подключении ИСПДн к сетям международного информационного обмена				
19	Фильтрация на сетевом уровне для каждого сетевого пакета независимо (решение о фильтрации принимается на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов).	+	+	+
20	Фильтрация пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств.	-	+	+

№	План - перечень технических мероприятий по обеспечении безопасности ИСПДн	Класс защищенности К3	Класс защищенности К2	Класс защищенности К1
21	Фильтрация с учетом входного и выходного сетевого интерфейса как средства проверки подлинности сетевых адресов.	-	+	+
22	Фильтрация с учетом любых значимых полей сетевых пакетов; регистрация и учет фильтруемых пакетов (в параметры регистрации включаются адрес, время и результат фильтрации).	-	+	+
23	Фильтрация на транспортном уровне запросов на установление виртуальных соединений с учетом транспортных адресов отправителя и получателя.	-	-	+
24	Фильтрация на прикладном уровне запросов к прикладным сервисам с учетом прикладных адресов отправителя и получателя.	-	-	+
25	Фильтрацию с учетом даты и времени.	-	-	+
26	Аутентификация входящих и исходящих запросов методами, устойчивыми к пассивному и (или) активному прослушиванию сети.	-	-	+
27	Идентификация и аутентификация администратора межсетевого экрана при его локальных запросах на доступ по идентификатору (коду) и паролю условно-постоянного действия.	+	+	+

№	План - перечень технических мероприятий по обеспечении безопасности ИСПДн	Класс защищенности К3	Класс защищенности К2	Класс защищенности К1
28	Идентификация и аутентификация администратора межсетевого экрана при его удаленных запросах методами, устойчивыми к пассивному и активному перехвату информации.	-	-	+
29	Регистрация входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова (регистрация выхода из системы не проводится в моменты аппаратурного отключения межсетевого экрана).	+	+	+
30	Регистрация запуска программ и процессов (заданий, задач).	-	+	+
31	Регистрация и учет фильтруемых пакетов (в параметры регистрации включаются адрес, время и результат фильтрации).	-	-	+
32	Регистрация и учет запросов на установление виртуальных соединений	-	-	+
33	Регистрация действий администратора межсетевого экрана по изменению правил фильтрации.	-	-	+
34	Локальная сигнализация попыток нарушения правил фильтрации.	-	-	+

№	План - перечень технических мероприятий по обеспечении безопасности ИСПДн	Класс защищенности К3	Класс защищенности К2	Класс защищенности К1
35	Предотвращение доступа неидентифицированного пользователя или пользователя, подлинность идентификации которого при аутентификации не подтвердилась.	-	-	+
36	Возможность дистанционного управления своими компонентами, в том числе возможность конфигурирования фильтров, проверки взаимной согласованности всех фильтров, анализа регистрационной информации.	-	-	+
37	Контроль целостности своей программной и информационной части; фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств.	+	+	+
38	Контроль целостности программной и информационной части межсетевого экрана по контрольным суммам.	-	-	+
39	Восстановление свойств межсетевого экрана после сбоев и отказов оборудования.	+	+	+
40	Регламентное тестирование реализации правил фильтрации, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления.	+	+	+

№	План - перечень технических мероприятий по обеспечении безопасности ИСПДн	Класс защищенности К3	Класс защищенности К2	Класс защищенности К1
V. При применении в ИСПДн функции голосового ввода ПДн в ИС или функции воспроизведения информации акустическими средствами ИС				
41	Реализовать организационные и технические меры для обеспечения звукоизоляции ограждающих конструкций помещений, в которых расположена информационная система, их систем вентиляции и кондиционирования, не позволяющей вести прослушивание акустической (речевой) информации при голосовом вводе персональных данных в информационной системе или воспроизведении информации акустическими средствами.	-	-	+
VI. Требования к программному обеспечению средств защиты информации и средствам вычислительной техники				
42	Применять программное обеспечение средств защиты информации, соответствующее 4 уровню контроля отсутствия недекларированных возможностей.	-	-	+
43	Использовать средства вычислительной техники, удовлетворяющие требованиям национальных стандартов по электромагнитной совместимости, по безопасности и эргономическим требованиям к средствам отображения информации, по санитарным нормам, предъявляемым к видеодисплейным терминалам средств вычислительной техники.	-	+	-

Примечание:
Для ИСПДн 4 класса перечень мероприятий по защите ПДн определяется в зависимости от ущерба, который может быть нанесен вследствие несанкционированного или непреднамеренного доступа к ПДн.