ВЫПОЛНЕНИЕ МЕР

17-ГО И 21-ГО ПРИКАЗОВ ФСТЭК ПО ЗАЩИТЕ

ИНФОРМАЦИИ В ИНФОРМАЦИОННОЙ СИСТЕМЕ

ПУТЕМ ПРИМЕНЕНИЯ

ПРОГРАММНО-АППАРАТНОГО КОМПЛЕКСА

«СЕКРЕТ ОСОБОГО НАЗНАЧЕНИЯ»

ОКБ САПР
2021

1 Общие положения

В настоящем документе рассматривается выполнение мер 17-го и 21-го приказов ФСТЭК по защите информации в информационной системе (автоматизированной системе) путем применения программно-аппаратного комплекса «Секрет Особого Назначения» (далее – ПАК «Секрет Особого Назначения», «Секрет Особого Назначения» либо комплекс).

ПАК «Секрет Особого Назначения» представляет собой это защищенный служебный носитель информации, предназначенный для таких задач, когда данные, конфиденциальность которых должна контролироваться, должны храниться на служебном носителе и переноситься сотрудником в рамках его должностных обязанностей на различные компьютеры.

ПАК «Секрет Особого Назначения» включает:

- специальный носитель «Секрет Особого Назначения» (СН);
- программное обеспечение (ПО) рабочей станции (РС) – консоль администратора и консоль пользователя.

Консоль администратора необходима для администрирования СН (установки списка разрешенных РС, длины пароля, возможного числа попыток аутентификации пользователя и т.д.). Консоль пользователя предназначена для выполнения авторизации пользователя и получения доступа к закрытому разделу диска СН.

ПАК «Секрет Особого Назначения» предназначен как для корпоративного, так и для личного использования.

Основные особенности:

- диск ПАК «Секрет Особого Назначения» состоит из двух разделов: открытого и закрытого. ПО РС размещается на открытом диске СН, на котором и исполняется (без установки на жесткий диск РС). Закрытый раздел диска предназначен для хранения и переноса данных пользователя;
- доступ к закрытому разделу диска СН предоставляется только после успешного завершения контрольных процедур;
- ведется аппаратный журнал работы СН, содержащийся на закрытом разделе диска СН. Журнал работы СН недоступен для пользователя и позволяет увидеть все случаи подключения устройства к каким-либо компьютерам, даже те, что закончились неуспешно;
- предусмотрена возможность задания списка РС, на которых разрешено использование СН. На неразрешенных компьютерах – будь то в корпоративной сети или вне ее, «Секрет Особого Назначения» не примонтируется.

2 Выполнение базового набора мер, определенных 17-ым и 21-ым приказами ФСТЭК России по защите информации в информационной системе, путем применения ПАК «Секрет Особого Назначения»

В таблице № 1 представлено описание выполнения базового набора мер 17-го и 21-го приказов ФСТЭК по защите информации в информационной системе путем применения ПАК «Секрет Особого Назначения» (ТУ 4012-033-11443195-2012).

Выражение «все» в ячейках столбца «Уровни защищенности ПДн» означает, что рассматриваемая мера должна быть реализована в информационной системе с любым уровнем защищенности персональных данных.

Выражение «все» в ячейках столбца «Классы защищенности ИС» означает, что рассматриваемая мера должна быть реализована в информационной системе с любым классом защищенности.

Таблица 1 – Выполнение базового набора мер по защите информации 17-го и 21-го приказов ФСТЭК по защите информации в информационной системе путем применения ПАК «Секрет Особого Назначения»

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Секрет Особого Назначения»	Ссылки на документацию
		Идентификация и аутентификация субъектов и объектов доступа (ИАФ)				
1	ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	+ все	+ все	Идентификация администратора производится по логину, а аутентификация – по паролю. Идентификация пользователя производится по логину пользователя а аутентификация – по коду авторизации (КА).	1. п.п. 3.1 документа «Секрет Особого Назначения. Руководство администратора»; 2. п.п. 3.2 документа «Секрет Особого Назначения. Руководство пользователя».
2	ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных	+ начиная со 2 уровня защищенности ПДн	+ начиная со 2 класса защищенности ИС	Идентификация РС в ПАК «Секрет Особого Назначения» выполняется по следующим параметрам: серийный номер «Аккорд-АМДЗ», серийный номер материнской платы компьютера, серийный номер дистрибутива ОС, идентификатор домена Active Directory, имя компьютера в домене.	1. п.п. 3.2.2 документа «Секрет Особого Назначения. Руководство администратора».
3	ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	+ все	+ все	Создание и смена пароля администратора, разблокировка СН, установка длины КА пользователя, установка числа ошибок авторизации пользователя выполняется администратором СН в консоли администратора. Создание и смена КА пользователя выполняется пользователем СН в консоли пользователя.	1. п.п. 3.1, 3.2, 3.5, 3.6, 3.10 документа «Секрет Особого Назначения. Руководство администратора»; 2. п.п. 3.1, 3.2, 3.4, 3.5 документа «Секрет Особого Назначения. Руководство пользователя».
4	ИАФ.5	Защита обратной связи при вводе аутентификационной информации	+ все	+ все	При вводе пароль администратора и КА пользователя отображаются символами.	
		Управление доступом				

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Секрет Особого Назначения»	Ссылки на документацию
		субъектов доступа к объектам доступа (УПД)				
5	УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	+ все	+ все	Комплекс обеспечивает управление учетными записями пользователей СН. Возможные операции с пользователями: создание, редактирование настроек доступа учетной записи, аннулирование регистрации пользователя, разблокирование.	1. п.п. 3 документа «Секрет Особого Назначения. Руководство администратора»; 2. п.п. 3 документа «Секрет Особого Назначения. Руководство пользователя».
6	УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	+ все	+ все	В комплексе реализован ролевой метод разграничения доступа.	1. п.п. 2.2, 3.1 документа «Секрет Особого Назначения. Руководство администратора»; 2. п.п. 3.1 документа «Секрет Особого Назначения. Руководство пользователя».
7	УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	+ все	+ все	В случае личного использования СН пользователь является также администратором устройства. В этом случае пользователю доступны функции управления устройством (посредством консоли администратора). Администратору доступны функции управления устройством (создание списка разрешенных РС, установка типа доступа к СН, установка типа заполнения журнала, числа ошибок авторизации пользователя и т.д.). Пользователю данные функции не доступны. Пользователю после успешного завершения авторизации доступен закрытый раздел диска СН, к которому администратор получить доступ не может.	1. п.п. 3, 6 документа «Секрет Особого Назначения. Руководство администратора»; 2. п.п. 3 документа «Секрет Особого Назначения. Руководство пользователя».
8	УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	+ все	+ все		
9	УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	+ все	+ все	Администратор СН может установить для пользователя необходимое количество неуспешных попыток авторизации. Это число может варьироваться в пределах от 1 до 255 (по умолчанию установлено значение 3).	1. п.п. 3.2.4 документа «Секрет Особого Назначения. Руководство администратора».
10	УПД.9	Ограничение	не входит в	+	Для каждой учетной записи	

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Секрет Особого Назначения»	Ссылки на документацию
		числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы	базовый набор мер	в 1 классе защищенности ИС	возможен только один сеанс доступа. При попытке запустить консоль пользователя при работающей консоли администратора на экране появляется следующее сообщение	
11	УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации	+ начиная с 3 уровня защищенности ПДн	+ все	До проведения идентификации и аутентификации пользователю запрещены любые действия кроме ввода идентификационной и аутентификационной информации.	1. п.п. 4 документа «Секрет Особого Назначения. Руководство пользователя».
12	УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)	+ все	+ все	В ПАК «Секрет Особого Назначения» имеется возможность настройки параметров взаимодействия с иными информационными системами. Для случаев, когда для СН установлен доступ с ограничением по доменам и РС, но предполагается его временное использование на компьютерах, не включенных в список разрешенных, в ПАК «Секрет Особого Назначения» предусмотрена функция временного снятия ограничений на доступ к СН на РС.	1. п.п. 3.2.2 документа «Секрет Особого Назначения. Руководство администратора».
		Защита машинных носителей персональных данных (ЗНИ)				
13	ЗНИ.2	Управление доступом к машинным носителям персональных данных	+ начиная со 2 уровня защищенности ПДн	+ все	ПАК «Секрет Особого Назначения» позволяет управлять доступом к СН: ограничить работу СН на РС (настройка «Доступ с ограничением по доменам и рабочим станциям») – создать список разрешенных РС, временно снять все ограничения на доступ к СН на РС, редактировать список разрешенных РС, настроить политику использования КА пользователя.	1. п.п. 3.2, 3.3 документа «Секрет Особого Назначения. Руководство администратора».
14	ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители персональных данных	не входит в базовый набор мер	+ начиная со 2 класса защищенности ИС	При выборе настройки «Доступ с ограничением по доменам и рабочим станциям» возможно ограничить использование СН на РС (создать список РС, на которых разрешено использование СН), тем самым, можно контролировать перенос информации на СН между РС корпоративной сети или вне ее.	1. п.п. 3.3 документа «Секрет Особого Назначения. Руководство администратора».
15	ЗНИ.8	Уничтожение	+	+	Комплекс обеспечивает полное	1. п.п. 3.6, 3.8

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Секрет Особого Назначения»	Ссылки на документацию
		(стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания	начиная с 3 уровня защищенности ПДн	все	удаление информации пользователя с закрытого раздела диска СН, а также аннулирование регистрации администратора, сброс всех настроек СН, удаление журнала событий, аннулирование регистрации пользователя СН (функция «Общий сброс СН»). При выборе данной функции выполняется возврат устройства к заводским настройкам.	документа «Секрет Особого Назначения. Руководство администратора».
		Регистрация событий безопасности (РСБ)				
16	РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	+ все	+ все	Журнал регистрации событий содержит следующую информацию: – дата и время регистрации события; – тип события – имеются следующие типы событий Сообщение», «Ошибка», «Предупреждение»; – описание события.	1. п.п. 3.4 документа «Секрет Особого Назначения. Руководство администратора».
17	РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	+ все	+ все	В ПАК «Секрет Особого Назначения» ведется аппаратный журнал регистрации событий СН, который содержит информацию о событиях, зафиксированных в процессе работы с ПАК «Секрет Особого Назначения» на конкретной РС.	
18	РСБ.4	Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти	не входит в базовый набор мер	+ все	В журнале событий фиксируются ошибки, которые могут возникнуть при работе СН. Запись в журнале с сообщением об ошибке содержит номер ошибки, позволяющий разработчикам продукта определить её причину при обращении в техническую поддержку изготовителя.	1. п.п. 3.2.3, 3.4 документа «Секрет Особого Назначения. Руководство администратора».
19	РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации	+ начиная со 2 уровня защищенности ПДн	+ все	Комплекс обеспечивает просмотр администратору зарегистрированных в журнале событий безопасности, экспорт журнала в текстовый файл и	1. п.п. 3.4, 7 документа «Секрет Особого Назначения. Руководство администратора».

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Секрет Особого Назначения»	Ссылки на документацию
		событий безопасности и реагирование на них			очистку журнала.	
20	РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе	не входит в базовый набор мер	+ все	В ПАК «Секрет Особого Назначения» имеется возможность установки внутреннего времени (в том случае, если СН снабжен внутренними часами). Если СН снабжен внутренними часами, события регистрируются в журнале в соответствии с установленным на них временем.	1. п.п. 3.9 документа «Секрет Особого Назначения. Руководство администратора».
21	РСБ.7	Защита информации о событиях безопасности	+ все	+ все	Доступ к журналу событий ПАК «Секрет Особого Назначения» имеет только администратор устройства. Пользователь имеет доступ к журналу событий только при личном использовании СН. Для доступа к журналу событий предоставляется только после успешного выполнения процедуры авторизации.	1. п.п. 3.4 документа «Секрет Особого Назначения. Руководство администратора».
		Контроль (анализ) защищенности персональных данных (АН3)				
22	АН3.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей	+ все	+ все	Устранение уязвимостей комплекса выполняется путем установки обновлений программного обеспечения средств защиты информации. Обновление прошивки СН выполняется в сервисном центре Разработчика ПО.	1. п. 6 документа «Секрет Особого Назначения. Формуляр».
23	АН3.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	+ все	+ все	Комплекс обеспечивает возможность установки обновлений внутреннего программного обеспечения СН (прошивки).	
24	АН3.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил	+ начиная со 2 уровня защищенности ПДн	+ все	ПАК «Секрет Особого Назначения позволяет задать следующие параметры: – тип доступа к СН на рабочих станциях («без ограничений», «с ограничением по доменам и рабочим станциям»); – реакция при заполнении объема, выделенного для хранения журнала;	1. п.п. 3.2 документа «Секрет Особого Назначения. Руководство администратора».

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Секрет Особого Назначения»	Ссылки на документацию
		разграничения доступа, полномочий пользователей в информационной системе			– длина КА пользователя; – число ошибок авторизации пользователя до блокирования.	
		Обеспечение целостности информационной системы и персональных данных (ОЦЛ)				
25	ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации	+ начиная со 2 уровня защищенности ПДн	+ начиная со 2 класса защищенности ИС	Целостность встраиваемого ПО обеспечивается технологически в процессе производства ПАК «Секрет Особого Назначения»: контроль пользователя и консоль администратора из состава ПО ПАК «Секрет Особого Назначения» располагаются на открытом разделе диска СН, защищенном от записи (в режиме «только чтение»).	1. п.п. 2.2 документа «Секрет Особого Назначения. Руководство администратора».
26	ОЦЛ.6	Ограничение прав пользователей по вводу информации в информационную систему	не входит в базовый набор мер	+ в 1 классе защищенности ИС	Администратору доступны функции управления устройством (создание списка разрешенных РС, установка типа доступа к СН, установка типа заполнения журнала, числа ошибок авторизации пользователя и т.д.). Пользователю данные функции не доступны. Пользователю после успешного завершения авторизации доступен закрытый раздел диска СН, к которому администратор получить доступ не может.	1. п.п. 3 документа «Секрет Особого Назначения. Руководство администратора»; 2. п.п. 3 документа «Секрет Особого Назначения. Руководство пользователя».
		Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)				
27	ЗИС.1	Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты персональных данных, функций по обработке персональных данных и иных	+ на 1 уровне защищенности ПДн	+ начиная со 2 класса защищенности ИС	Имеется возможность разделения функций по управлению информационной системой: поддерживаются роли администратора и пользователя устройства.	1. п.п. 2.2, 3.1 документа «Секрет Особого Назначения. Руководство администратора»; 2. п.п. 3.1 документа «Секрет Особого Назначения. Руководство пользователя».

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Секрет Особого Назначения»	Ссылки на документацию
		функций информационной системы				
28	ЗИС.15	Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки персональных данных	+ начиная со 2 уровня защищенности ПДн	+ начиная со 2 класса защищенности ИС	Технологически в процессе производства ПАК «Секрет Особого Назначения» обеспечивается целостность встраиваемого ПО.	
29	ЗИС.21	Исключение доступа пользователя к информации, возникшей в результате действий предыдущего пользователя через реестры, оперативную память, внешние запоминающие устройства и иные общие для пользователей ресурсы информационной системы	+ на 1 уровне защищенности ПДн	нет	В случае необходимости возврата устройства к заводским настройкам имеется функция общего сброса СН.	1. п.п. 3.8 документа «Секрет Особого Назначения. Руководство администратора».
		Выявление инцидентов и реагирование на них (ИНЦ)				
30	ИНЦ.2	Обнаружение, идентификация и регистрация инцидентов	+ начиная со 2 уровня защищенности ПДн	нет	В ПАК «Секрет Особого Назначения» реализованы механизмы регистрации и предупреждения (сигнализации) о событиях, относящихся к возможным нарушениям безопасности. Выполняется регистрация следующих событий: – начало сеанса работы СН с рабочей станции; – установка внутренних часов СН; – установка описания рабочей станции; – регистрация администратора; – смена пароля администратора; – установка политик КА; – установка политик доступа к	

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Секрет Особого Назначения»	Ссылки на документацию
					рабочей станции; – установка политик записи журнала СН; – очистка журнала СН; – полный сброс СН; – получение доступа к журналу событий; – обновление внутреннего ПО СН; – регистрация пользователя; – аннулирование регистрации пользователя; – смена КА; – блокирование СН; – разблокирование СН; – авторизация пользователя.	

3 Выполнение дополнительных (не включенных в базовый набор) мер, определенных 17-ым и 21-ым приказами ФСТЭК России по защите информации в информационной системе, путем применения ПАК «Секрет Особого Назначения»

В таблице № 2 представлено описание выполнения дополнительных (не включенных в базовый набор) мер 17-го и 21-го приказов ФСТЭК по защите информации в информационной системе путем применения ПАК «Секрет Особого Назначения» (ТУ 4012-033-11443195-2012).

Выражением «нет» выделены ячейки столбца «Уровни защищенности ПДн», которые относятся к требованиям, содержащимся только в 17-ом приказе ФСТЭК, и, следовательно, не относящимся к уровням защищенности ПДн.

Таблица 2 - Выполнение дополнительных (не включенных в базовый набор) мер по защите информации 17-го и 21-го приказов ФСТЭК по защите информации в информационной системе путем применения ПАК «Секрет Особого Назначения»

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Секрет Особого Назначения»	Ссылки на документацию
		Защита машинных носителей персональных данных (ЗНИ)				
1	ЗНИ.3	Контроль перемещения машинных носителей информации за			В ПАК «Секрет Особого Назначения» имеется возможность установки политики доступа к СН с ограничением по доменам и	1. п.п. 3.2 документа «Секрет Особого Назначения. Руководство администратора».

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Секрет Особого Назначения»	Ссылки на документацию
		пределы контролируемой зоны			рабочим станциям.	
2	ЗНИ.4	Исключение возможности несанкционированного ознакомления с содержанием персональных данных, хранящихся на машинных носителях, и (или) использования носителей персональных данных в иных информационных системах			На РС из списка разрешенных доступ к закрытому разделу диска СН, на котором хранятся пользовательские данные, предоставляется только после успешного завершения контрольных процедур. На неразрешенных компьютерах «Секрет Особого Назначения» не примонтируется, соответственно, несанкционированное ознакомление с содержанием персональных данных исключается.	1. п.п. 3.2.2, 3.3 документа «Секрет Особого Назначения. Руководство администратора».
3	ЗНИ.6	Контроль ввода (вывода) информации на машинные носители информации			При выборе настройки «Доступ с ограничением по доменам и рабочим станциям» возможно ограничить использование СН на РС (создать список РС, на которых разрешено использование СН), тем самым, можно контролировать перенос информации на СН между РС корпоративной сети или вне ее.	1. п.п. 3.3 документа «Секрет Особого Назначения. Руководство администратора».
4	ЗНИ.7	Контроль подключения машинных носителей информации				
		Регистрация событий безопасности (РСБ)				
5	РСБ.8	Обеспечение возможности просмотра и анализа информации о действиях отдельных пользователей в информационной системе	нет		Администратору доступна функция фильтрации событий по следующим параметрам: – период времени. Можно задать начало и/или конец интересующего периода времени, используя строки «С:» и «По:»; – тип события. Доступен просмотр событий типов «Сообщение», «Ошибка», «Предупреждение», а также одновременный просмотр событий всех типов (значение параметра «Все»); – исполнитель. Доступен просмотр событий, связанных с работой ПО, администратора или пользователя, а также одновременный просмотр событий для всех исполнителей (значение параметра «Все»); – имя РС; – домен; — описание события.	1. п.п. 3.4 документа «Секрет Особого Назначения. Руководство администратора».

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Секрет Особого Назначения»	Ссылки на документацию
		Обеспечение целостности информационной системы и персональных данных (ОЦЛ)				
6	ОЦЛ.2	Контроль целостности персональных данных, содержащихся в базах данных информационной системы			Посредством применения СН исключаются раскрытие, несанкционированная модификация данных пользователя на РС, не входящих в список разрешенных.	1. п.п. 3.3 документа «Секрет Особого Назначения. Руководство администратора».
7	ОЦЛ.8	Контроль ошибочных действий пользователей по вводу и (или) передаче персональных данных и предупреждение пользователей об ошибочных действиях			При ошибочных действиях пользователя возникают соответствующие предупреждения.	1. п.п. 3.2 документа «Секрет Особого Назначения. Руководство администратора»; 2. п. 3 документа «Секрет Особого Назначения. Руководство пользователя».
		Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)				
8	ЗИС.4	Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации)			В ПАК «Секрет Особого Назначения» имеется возможность создания списка разрешенных РС. Администратор и пользователь выполняют функции безопасности на рабочей станции из числа разрешенных.	1. п.п. 3.2.2, 3.3 документа «Секрет Особого Назначения. Руководство администратора».
9	ЗИС.18	Обеспечение загрузки и исполнения программного обеспечения с машинных носителей персональных данных, доступных только для чтения, и контроль			ПО РС располагается на открытом разделе диска СН, доступном только для чтения. ПАК «Секрет Особого Назначения» обеспечивает исполнение ПО РС непосредственно со СН. Установки на РС не требуется.	1. п.п. 1.1 документа «Секрет Особого Назначения. Руководство администратора».

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	«Секрет Особого Назначения»	Ссылки на документацию
		целостности данного программного обеспечения				
10	ЗИС.19	Изоляция процессов (выполнение программ) в выделенной области памяти			Диск ПАК «Секрет Особого Назначения» разделен на открытый (в режиме «только чтение») и закрытый разделы. На открытом разделе диска СН, защищенном от записи, располагается и исполняется ПО ПАК «Секрет Особого Назначения». Закрытый раздел диска СН предназначен для хранения и переноса данных. Доступ к закрытому разделу диска СН получает только пользователь СН после прохождения процедур авторизации.	1. п.п. 2.2 документа «Секрет Особого Назначения. Руководство администратора».
11	ЗИС.26	Использование прикладного и специального программного обеспечения, имеющих возможность функционирования в средах различных операционных систем		нет	ПАК «Секрет Особого Назначения» может использоваться в ОС семейства Windows, Linux.	1. п.п. 1.1 документа «Секрет Особого Назначения. Руководство администратора».

Итак, путем применения ПАК «Секрет Особого Назначения» в информационной системе выполняются следующие меры, включенные в базовый набор мер защиты информации для соответствующего класса защищенности информационной системы:

ИАФ: 1, 2, 4, 5;

УПД: 1, 2, 4, 5, 6, 9, 11, 16;

ЗНИ: 2, 5, 8;

РСБ: 2, 3, 4, 5, 6, 7;

АНЗ: 1, 2, 5;

ОЦЛ: 1, 6;

ЗИС: 1, 15, 21;

ИНЦ: 2;

а также дополнительные (не включенные в базовый набор) меры:

ЗНИ: 3, 4, 6, 7;

РСБ: 8;

ОЦЛ: 2, 8;

ЗИС: 4, 18, 19, 26.

ОКБ САПР
www.okbsapr.ru
okbsapr@okbsapr.ru
Россия, 115114, Москва, 2-ой Кожевнический переулок, д. 12
Тел.: +7 (495) 994-72-62