ВЫПОЛНЕНИЕ МЕР 31-ГО ПРИКАЗА ФСТЭК ПО ЗАЩИТЕ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННОЙ СИСТЕМЕ ПУТЕМ ПРИМЕНЕНИЯ ПРОГРАММНО-АППАРАТНОГО КОМПЛЕКСА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕНСАНКЦИОНИРОВАННОГО ДОСТУПА ЦЕНТР-Т

ОКБ САПР
2021

1 Общие положения

В настоящем документе рассматривается выполнение мер 17-го и 21-го приказов ФСТЭК по защите информации в автоматизированной системе управления путем применения программно-аппаратного комплекса средство защиты информации от несанкционированного доступа (ПАК СЗИ НСД) «Центр-Т» (далее по тексту – ПАК СЗИ НСД «Центр-Т» либо комплекс).

ПАК СЗИ НСД «Центр-Т» представляет собой комплекс программных и аппаратных средств, позволяющий осуществлять хранение и сетевую загрузку программного обеспечения (ПО) терминальных станций (ТС), которые используются в системе терминального доступа, с возможностью обработки информации ограниченного доступа.

В состав аппаратной части ПАК СЗИ НСД «Центр-Т» входит:

– специальный носитель СХСЗ (далее по тексту – СН СХСЗ), функционирующий в составе сервера хранения и сетевой загрузки;
– специальный носитель терминальной станции (далее по тексту – СН ТС), функционирующий в составе ТС;
– специальный носитель автоматизированного рабочего места (АРМ) Эмиссии, функционирующий в составе АРМ Эмиссии.

Аппаратная часть сервера хранения и сетевой загрузки и терминальных станций Клиента ПАК СЗИ НСД «Центр-Т» может быть выполнена на базе защищенного микрокомпьютера. В таком случае СХСЗ представляет собой защищенное автоматизированное рабочее место ХСЗ (далее по тексту – защищенное АРМ ХСЗ), а клиентская часть – защищенный терминал «Центр-TrusT»[1].

В состав программной части ПАК СЗИ НСД «Центр-Т» входит:

– ПО удаленного управления «Центр-Т»;
– образ резидентной ОС СХСЗ;
– образ резидентной ОС ТС;
– образ резидентной ОС АРМ Эмиссии.

Предусмотрено два варианта поставки ПАК СЗИ НСД «Центр-Т»:

ПАК СЗИ НСД «Центр-Т» функционально организует механизм взаимодействия ТС в составе системы терминального доступа (СТД) с СХСЗ, в результате чего предоставляется возможность осуществлять:

– сетевую загрузку ПО на ТС;
– контроль подлинности загружаемого ПО ТС;
– ведение журналов загрузки ПО на ТС и журналов активности пользователей ТС.

ПАК СЗИ НСД «Центр-Т» позволяет:

– проверять КА полученного образа на СХСЗ и на ТС;
– назначать на СХСЗ пользователям различные образы ПО ТС;
– производить идентификацию/аутентификацию пользователей ТС для начала работы с терминальным сервером;

[1] Вариант исполнения аппаратной части ПАК СЗИ НСД «Центр-Т» оговаривается при заказе.

– осуществлять сетевую загрузку и контроль подлинности созданных образов ПО ТС при загрузке на ТС;
– производить двухфакторную аппаратную идентификацию / аутентификацию пользователей ТС в ПАК «Аккорд» на терминальном сервере;
– предоставлять пользователю ТС возможность работы в рамках терминальной сессии, организованной средствами загруженного образа ПО ТС с заданными параметрами. В рамках терминальной сессии пользователю ТС может предоставляться возможность использования USB-принтеров и/или flash-накопителей информации, подключенных непосредственно к ТС;
– вести аудит действий пользователей и администраторов СХСЗ путем просмотра и анализа журналов загрузки образов ПО ТС и журналов активности администраторов СХСЗ.

2 Выполнение базового набора мер, определенных 31-ым приказом ФСТЭК России по защите информации в автоматизированной системе управления, путем применения ПАК СЗИ НСД «Центр-Т»

В таблице № 1 представлено описание выполнения базового набора мер 31-го приказа ФСТЭК по защите информации в автоматизированной системе управления путем применения ПАК СЗИ НСД «Центр-Т».

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

Таблица 1 – Выполнение базового набора мер по защите информации 31-го приказа ФСТЭК по защите информации в автоматизированной системе управления путем применения ПАК СЗИ НСД «Центр-Т»

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	ПАК «Центр-Т»	Ссылки на документацию
		Идентификация и аутентификация субъектов и объектов доступа (ИАФ)			
1	ИАФ.0	Разработка политики идентификации и аутентификации	+ все	В комплексе разработана политика идентификации и аутентификации.	
2	ИАФ.1	Идентификация и аутентификация пользователей и инициируемых ими процессов	+ все	Комплекс поддерживает идентификацию и идентификацию пользователей и инициируемых ими процессов. Администратор сервисного режима СХСЗ идентифицируется в СХСЗ по PIN-коду. Администратор Клиентского устройства, администратор ИБ клиентского устройства идентифицируются в ПО Клиента по PIN-коду.	1. см. п.п. 3.2, 4.3, 5.3, 6.3, 7.3 документа «Руководство по эксплуатации СХСЗ»; 2. см. п.п. 3.3, 4.2, 5.2 документа «Руководство по эксплуатации клиентских устройств».

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	ПАК «Центр-Т»	Ссылки на документацию
				Администраторы удалённого управления СХСЗ предъявляют логин, пароль, идентификатор. Пользователи клиентского устройства идентифицируются по номерам их Клиентского устройства.	
3	ИАФ.2	Идентификация и аутентификация устройств	+ все	Комплекс поддерживает идентификацию и аутентификацию устройств (мониторов, устройств вывода и записи звука). Параметры идентификации устройств задаются во вкладке «Периферийные устройства».	1. см. п.п. 4.6 документа «Руководство по эксплуатации СХСЗ».
4	ИАФ.3	Управление идентификаторами	+ все	Комплекс обеспечивает возможность управления идентификаторами, паролями и учетными записями пользователей. Возможные операции: создание, удаление, редактирование, присвоение. В случае редактирования учетных записей пользователей клиентского устройства Администраторам доступны: – смена ФИО и логина; – смена роли; – задание поля «Дополнительно»; – назначение пользователю клиентского устройства (задание серийного номера идентификатора); – настройка разрешения экрана (возможна после первого подключения пользователя к СХСЗ); – настройка параметров кэширования образа ПО РС на устройстве пользователя; – настройка параметра удаления событий безопасности на клиентском устройстве; – просмотр следующих параметров: дата и время последнего подключения, объем свободной памяти момент старта ОНЗ, настройки сети (IP-адрес клиентского устройства), интервал подключения к сервисам RMQ; – просмотр информации об используемом Клиентами оборудовании; – назначение образов и	1. см. п.п. 3.2, 4.4, 4.5, 4.8, 5.4, 5.7, 5.8, 6.4, 6.5, 6.9, 7.4 документа «Руководство по эксплуатации СХСЗ».
5	ИАФ.4	Управление средствами аутентификации	+ все		

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	ПАК «Центр-Т»	Ссылки на документацию
				шаблонов настроек ПО РС.	
6	ИАФ.7	Защита аутентификационной информации при передаче	+ все	Функция аутентификации обеспечивает исключение отображения для пользователя действительного значения аутентификационной информации за счет отображения вводимых символов аутентификационной информации условными знаками.	1. см. п.п. 4.3, документа «Руководство по эксплуатации СХСЗ».
		Управление доступом субъектов доступа к объектам доступа (УПД)			
7	УПД.0	Разработка политики управления доступом	+ все	В комплексе разработана политика управления доступом.	
8	УПД.1	Управление учетными записями пользователей	+ все	В комплексе обеспечивается поддержка учетных записей пользователей, администраторов СХСЗ, администраторов Клиентских устройств.	1. см. п.п. 4.5.1 документа «Руководство по эксплуатации СХСЗ».
9	УПД.2	Реализация политик управления доступом	+ все	Ролевой метод реализован в виде групп пользователей: Пользователи административной группы: – Администратор СХСЗ; – Администратор нештатного режима работы СХСЗ; – Администратор ИБ СХСЗ; – Контролер СХСЗ; – Администратор Клиентских устройств; – Администратор ИБ клиентских устройств. Пользователи клиентской группы: – Пользователи Клиентских устройств.	1. см. п. 1 документа «Руководство по эксплуатации СХСЗ»; 2. см. п. 1 документа «Руководство по эксплуатации клиентских устройств».
10	УПД.3	Доверенная загрузка	+ начиная со 2 класса защищенности автоматизированной системы управления	Выполнение меры УПД.3 обеспечивается за счет применения компенсирующих мер: использования в ИС защищенных терминалов, с входящим в состав резидентным компонентом безопасности (СДЗ уровня BIOS) – «Центр TrusT» или «m-TrusT» Терминал.	1. см. п.п. 1.1 документа «Модуль доверенной загрузки «Аккорд-МКТ». Руководство Администратора».
11	УПД.4	Разделение полномочий (ролей) пользователей	+ все	Комплекс обеспечивает разделение полномочий: реализованы группы пользователей:	1. см. п. 1, 2 документа «Руководство по эксплуатации СХСЗ»; 2. см. п. 1 документа
12	УПД.5	Назначение минимально	+		

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	ПАК «Центр-Т»	Ссылки на документацию
		необходимых прав и привилегий	все	Пользователи административной группы: – Администратор СХСЗ; – Администратор нештатного режима работы СХСЗ; – Администратор ИБ СХСЗ; – Контролер СХСЗ; – Администратор Клиентских устройств; – Администратор ИБ клиентских устройств. Пользователи клиентской группы: – Пользователи Клиентских устройств. Должностные полномочия определены в рамках ролей пользователей Комплекса.	«Руководство по эксплуатации клиентских устройств».
13	УПД.6	Ограничение неуспешных попыток доступа в информационную (автоматизированную) систему	+ все	Ограничение попыток доступа к ИС в рамках управления доступом регулируется СЗИ НСД серверной группы, например, СЗИ НСД «Аккорд-Win64 К» (TSE), установленном на СХСЗ.	1. см. п.п. 7.3 документа «Установка правил разграничения доступа. Программа ACED32».
14	УПД.9	Ограничение числа параллельных сеансов доступа	+ в 1 классе защищенности автоматизированной системы управления	Комплекс позволяет определить для пользователя максимальное число одновременных подключений к терминальным серверам (терминальных сессий), которые могут быть открыты на клиентском устройстве. Для задания указанного параметра Администратор БИ должен указать численное значение в поле «Максимальное число подключений». Значение «0», заданное по умолчанию, обозначает, что число одновременных подключений не ограничено.	1. см. п.п. 5.10 документа «Руководство по эксплуатации СХСЗ».
15	УПД.10	Блокирование сеанса доступа пользователя при неактивности	+ все	Комплекс позволяет выполнить настройку блокирования сеанса доступа пользователя при неактивности – изменить таймаут гашения экрана. Время, по истечении которого включится режим гашения экрана, можно задать в раскрывающемся списке значением из диапазона от 1 минуты до 5 часов или «Никогда» во вкладке «Сеть».	1. см. п.п. 3.4, 4.6 документа «Руководство по эксплуатации СХСЗ».
16	УПД.11	Управление действиями пользователей до	+	До проведения идентификации и аутентификации	1. см. п.п. 3.2, 4.3, 5.3, 6.3, 7.3 документа «Руководство

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	ПАК «Центр-Т»	Ссылки на документацию
		идентификации и аутентификации	все	пользователям административной группы запрещены любые действия кроме ввода идентификационной и аутентификационной информации, предъявления аппаратного идентификатора, смены пользователя.	по эксплуатации СХСЗ»; 2. см. п.п. 3.3, 4.2, 5.2 документа «Руководство по эксплуатации клиентских устройств».
17	УПД.13	Реализация защищенного удаленного доступа	+ все	Подключение к СХСЗ обеспечивается по защищённому протоколу SSH.	1. см. Приложение 2 документа «Руководство по эксплуатации СХСЗ».
		Ограничение программной среды (ОПС)			
18	ОПС.0	Разработка политики ограничения программной среды	+ начиная со 2 класса защищенности автоматизированной системы управления	ПАК «Центр-Т» обеспечивает возможность создания замкнутой программной среды на терминальной станции Клиента.	
19	ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения	+ в 1 классе защищенности автоматизированной системы управления	Комплекс обеспечивает возможность создания замкнутой программной среды на терминальной станции, допускающей запуск в ней только фиксированного образа ПО. Комплекс обеспечивает установку и управление фиксированными наборами ПО Клиентов. Комплекс обеспечивает автоматизированную инсталляцию и централизованное управление шаблонами образов ПО и настроек параметров компонентов ПО Клиента. Комплекс обеспечивает запуск на Клиенте только назначенного администратором СХСЗ docker образа ПО Клиента. Конкретный docker-образ ПО Клиента определяет фиксированный подлежащий установке набор ПО.	1. см. п.п. 4.6, 4.8, 5.5, 5.8, 5.10 документа «Руководство по эксплуатации СХСЗ».
20	ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения	+ начиная со 2 класса защищенности автоматизированной системы управления		
		Защита машинных носителей персональных данных (ЗНИ)			
21	ЗНИ.0	Разработка политики защиты машинных носителей информации	+ все	В ПАК «Центр-Т» реализована возможность управления доступом к носителям информации.	
22	ЗНИ.2	Управление физическим доступом к машинным	+	В комплексе предусмотрена возможность создания образа	1. см. п.п. 5.5 документа «Руководство по

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	ПАК «Центр-Т»	Ссылки на документацию
		носителям информации	все	ПО ТС: – с возможностью проброса usb-устройств в терминальную сессию; – без возможности проброса usb-устройств в терминальную сессию.	эксплуатации СХСЗ»; 2. см. п.п. 5.3 документа «Руководство по эксплуатации клиентских устройств».
23	ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации	+ все	В комплексе предусмотрена возможность создания образа ПО ТС: – с возможностью проброса usb-устройств в терминальную сессию; – без возможности проброса usb-устройств в терминальную сессию.	
24	ЗНИ.6	Контроль ввода (вывода) информации на машинные носители информации	+ в 1 классе защищенности автоматизированной системы управления		
25	ЗНИ.7	Контроль подключения машинных носителей информации	+ все		
		Аудит безопасности (АУД)			
26	АУД.0	Разработка политики аудита безопасности	+ все	Комплекс поддерживает политику аудита безопасности.	
27	АУД.2	Анализ уязвимостей и их устранение	+ все	Устранение уязвимостей ПАК «Центр-Т» выполняется путем установки обновлений программного обеспечения средств защиты информации. В ПАК «Центр-Т» предусмотрена возможность обновления ПО, в том числе ПО (firmware) носителей. Обновление ПО выполняется в сервисном центре Разработчика ПО.	1. см. Приложение 2 документа «Руководство по эксплуатации СХСЗ».
28	АУД.3	Генерирование временных меток и (или) синхронизация системного времени	+ все	В комплексе для настройки даты и времени может использоваться внешний NTP сервер. Для его использования необходимо заполнить поле «IP-адрес» раздела «Настройки NTP сервера» и нажать кнопку <Синхронизировать>. Поле «Статус» отображает текущее состояние синхронизации.	1. см. п.п. 3.9, 4.9. 5.11, 6.10, 7.9 документа «Руководство по эксплуатации СХСЗ»; 2. см. п.п. 4.7 документа «Руководство по эксплуатации клиентских устройств».
29	АУД.4	Регистрация событий безопасности	+ все	В комплексе имеется возможность регистрации возникновения событий, относящихся к событиям безопасности. Администратор сервисного режима может просмотреть события безопасности: – собственной сессии;	

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	ПАК «Центр-Т»	Ссылки на документацию
				– контейнеров СХСЗ. События безопасности собственной сессии Администратора сервисного режима отображаются на вкладке «Действия» в окне просмотра журналов. События безопасности контейнеров СХСЗ распределены по вкладкам: – «Сервис управления» – контейнер с ПО СХСЗ; – «БД» – контейнер с БД; – «Брокер» – контейнер брокера сообщений; – «Репозиторий» – контейнер с образами ПО Клиента. Для каждого события регистрируются: – время; – источник/контейнер; – сообщение. Администраторы удаленного управления СХСЗ могут просматривать события безопасности: – собственной сессии; – сессий администраторов удаленного управления СХСЗ; – сессий пользователей клиентских устройств. Все события фиксируются в общем журнале и отображаются на вкладке «Журнал событий». Общий журнал хранится в БД (внутренней или внешней, в зависимости от настроек СХСЗ) и не перезаписывается при выключении или перезагрузке как СХСЗ, так и внешней СУБД. Администратор БИ клиентского устройства может просматривать записи журнала о локальных событиях безопасности, отображающие действия администраторов и Пользователя клиентского устройства. Для каждого события фиксируются: – время; – заголовок (основная информация о событии); – сообщение; – пользователь (учетная	

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	ПАК «Центр-Т»	Ссылки на документацию
				запись, от имени которой выполнено действие); – источник события.	
30	АУД.6	Защита информации о событиях безопасности	+ все	Защита информации о событиях безопасности обеспечивается применением мер защиты информации от неправомерного доступа, уничтожения или модифицирования, и в том числе включает защиту средств ведения аудита. Доступ к записям аудита и функциям управления механизмами регистрации (аудита) предоставляется только уполномоченным должностным лицам: – доступ к журналу на СХСЗ предоставляется администратору сервисного режима СХСЗ; – доступ к общему журналу предоставляется администраторам удаленного управления; – доступ к локальному журналу Клиента предоставляется администратору ИБ Клиента.	
31	АУД.7	Мониторинг безопасности	+ все	Комплекс обеспечивает просмотр зарегистрированных в журнале событий безопасности администраторам СХСЗ, проведшим процедуры И/А.	
32	АУД.9	Анализ действий пользователей	+ в 1 классе защищенности автоматизированной системы управления	Для поиска нужной информации в событиях можно использовать функцию фильтра. Поиск с применением фильтра осуществляется с учетом регистра. Также есть возможность просмотра события за определенный период. Доступны следующие варианты: – за сегодня (по умолчанию); – за предыдущий день; – за неделю; – за месяц; – за указанный (произвольный) период. С помощью применения фильтра можно проанализировать работу каждого пользователя.	
		Обеспечение целостности (ОЦЛ)			

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	ПАК «Центр-Т»	Ссылки на документацию
33	ОЦЛ.0	Разработка политики обеспечения целостности	+ все	Комплекс обеспечивает возможность контроля целостности образов ПО ТС.	
34	ОЦЛ.1	Контроль целостности программного обеспечения	+ все		1. см. п. «Введение» «Руководство по эксплуатации СХСЗ»; 2. см. п.п. 5.3 документа «Руководство по эксплуатации клиентских устройств».
35	ОЦЛ.3	Ограничения по вводу информации в информационную (автоматизированную) систему	+ в 1 классе защищенности автоматизированной системы управления	Комплекс ограничивает права пользователей по вводу информации в ИС путем обеспечения ограничения программной среды.	1. см. п. 1, 2 документа «Руководство по эксплуатации СХСЗ»; см. п. 1 документа «Руководство по эксплуатации клиентских устройств».
		Обеспечение доступности (ОДТ)			
36	ОДТ.0	Разработка политики обеспечения доступности	+ все	Комплекс обеспечивает возможность резервного копирования баз данных и настроек СХСЗ, локальных настроек Клиента.	
37	ОДТ.2	Резервирование средств и систем	+ начиная со 2 класса защищенности автоматизированной системы управления		1. см. п.п. 3.5 документа «Руководство по эксплуатации СХСЗ»; 1. см. п.п. 4.5 документа «Руководство по эксплуатации клиентских устройств».
38	ОДТ.3	Контроль безотказного функционирования средств и систем	+ начиная со 2 класса защищенности автоматизированной системы управления	Комплекс обеспечивает фиксирование событий о неисправностях (сбоях или отказах) в функционировании ПАК «Центр-Т» в журнал событий.	1. см. п. «Введение», 3.5 «Руководство по эксплуатации СХСЗ»; 2. см. п.п. 5.3, 4.6 документа «Руководство по эксплуатации клиентских устройств».
39	ОДТ.6	Обеспечение возможности восстановления программного обеспечения при нештатных ситуациях	+ все	Комплекс обеспечивает возможность восстановления баз данных и настроек СХСЗ, локальных настроек Клиента из резервных копий.	1. см. п.п. 3.5 документа «Руководство по эксплуатации СХСЗ»; 2. см. п.п. 4.6 документа «Руководство по эксплуатации клиентских устройств».
40	ОДТ.8	Контроль предоставляемых вычислительных ресурсов и каналов связи	+ все	Контроль канала связи обеспечивается в случае, если образ начальной загрузки (ПО Клиента) включает средства защиты канала передачи данных. ПАК «Центр-Т» обеспечивает блокировку в ИС скрытых каналов передачи информации, существующих в исходной («родной») ОС терминала: блокировка обеспечивается посредством загрузки образа ПО РС с носителя «Центр-Т»,	1. см. п.п. 4.8.1, 5.5, 5.10 документа «Руководство по эксплуатации СХСЗ».

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	ПАК «Центр-Т»	Ссылки на документацию
				защищенного от перезаписи. Целостность образа ПО РС проверяется на этапе его получения Клиентом.	
		Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)			
41	ЗИС.0	Разработка политики защиты информационной (автоматизированной) системы и ее компонентов	+ все	Комплекс поддерживает политику защиты информационной (автоматизированной) системы и ее компонентов.	
42	ЗИС.1	Разделение функций по управлению (администрированию) информационной (автоматизированной) системой с иными функциями	+ все	В комплексе реализована возможность разделения функциональных возможностей по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации (функций безопасности) и функциональных возможностей эксплуатирующего персонала по обработке информации. В ПАК «Центр-Т» имеется поддержка ролей администратора сервисного режима СХСЗ, администратора СХСЗ, контролера, администратора НШР, администратора ИБ СХСЗ, администратора клиентских устройств, администратора ИБ клиентских устройств, администратора АРМ эмиссии, пользователей клиентских устройств.	1. см. п. 1 документа «Руководство по эксплуатации СХСЗ»; 2. см. п. 1 документа «Руководство по эксплуатации клиентских устройств».
43	ЗИС.13	Защита неизменяемых данных	+ начиная со 2 класса защищенности автоматизированной системы управления	Производится контроль целостности docker-образов (образов ПО ТС).	1. см. п.п. 3.7, документа «Руководство по эксплуатации СХСЗ»; 2. см. п.п. 5.3 документа «Руководство по эксплуатации клиентских устройств».
44	ЗИС.20	Обеспечение доверенных канала, маршрута	+ все	Данная мера реализована в комплексе: в случае, если образ начальной загрузки (ПО Клиента) включает средства защиты канала передачи данных.	1. см. п.п. 4.8.1, 5.5, 5.10 документа «Руководство по эксплуатации СХСЗ».
45	ЗИС.21	Запрет несанкционированной удаленной активации периферийных устройств	+ все	В ПАК «Центр-Т» предусмотрена возможность контроля подключения устройств вывода и записи звука. Параметры корректируются во вкладке «Периферийные устройства».	1. см. п.п. 4.6, 5.5 документа «Руководство по эксплуатации СХСЗ»; 2. см. п.п. 5.3 документа «Руководство по эксплуатации клиентских устройств».

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	ПАК «Центр-Т»	Ссылки на документацию
				В комплексе предусмотрена возможность контроля подключения usb-устройств в рамках терминальной сессии. Образы ПО ТС возможно создать: – с возможностью проброса usb-устройств в терминальную сессию; – без возможности проброса usb-устройств в терминальную сессию.	
46	ЗИС.27	Обеспечение подлинности сетевых соединений	+ начиная со 2 класса защищенности автоматизированной системы управления	Образы ПО РС, создаваемые на СХС3, сопоставляются с номерами клиентского устройств. При отправке образа на РС СХС3 проверяет сопоставлен ли номер клиентского устройства пересылаемому образу ПО. Если проверка завершается неудачей, то образ ПО не передается на РС. Клиентские устройства также проверяют принимаемые образы ПО РС. Если в ходе проверки Клиентом подлинность образов ПО РС не подтверждается, то образы клиентскими устройствами не принимаются.	1. см. п.п. 5.3 документа «Руководство по эксплуатации клиентских устройств».
47	ЗИС.31	Защита от скрытых каналов передачи информации	+ в 1 классе защищенности автоматизированной системы управления	ПАК «Центр-Т» обеспечивает блокировку в ИС скрытых каналов передачи информации, существующих в исходной («родной») ОС терминала: блокировка обеспечивается посредством загрузки образа ПО РС с носителя «Центр-Т», защищенного от перезаписи. Целостность образа ПО РС проверяется на этапе его получения Клиентом.	
48	ЗИС.33	Исключение доступа через общие ресурсы	+ в 1 классе защищенности автоматизированной системы управления	Исключение доступа пользователя к информации обеспечивается тем, что в рамках работы пользователь использует назначенное только ему клиентское устройство. После завершения работы клиентское устройство отключается от РС, не оставляя на ней никакой остаточной информации, соответственно, другой пользователь, работающий на этой же РС, не сможет получить данные предыдущего пользователя.	1. см. п.п. 4.8, 5.10 документа «Руководство по эксплуатации СХС3».
49	ЗИС.34	Защита от угроз отказа в обслуживании (DOS, DDOS-атак)	+ все	Комплекс «Центр-Т» контролирует подлинность ПО РС при передаче на клиентское	1. см. п.п. 5.3 документа «Руководство по эксплуатации клиентских

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	ПАК «Центр-Т»	Ссылки на документацию
				устройство.	устройств».
50	ЗИС.35	Управление сетевыми соединениями	+ начиная со 2 класса защищенности автоматизированной системы управления	Имеется возможность настройки сетевого соединения по протоколу ICA в части настройки адресов брокера Citrix. Также комплекс поддерживает возможность настройки адреса сервера службы AD, адреса сервера stunnel в сети, прокси-сервера (в случае поддержки в образе ПО ТС возможности работы со СКАД «Сигнатура-L»).	1. см. п.п. 4.8.1 документа «Руководство по эксплуатации СХСЗ».
51	ЗИС.38	Защита информации при использовании мобильных устройств	+ все	При применении в ИС ПАК «Центр-Т» совместно с СЗИ НСД «Аккорд» обеспечивается контроль и мониторинг применения мобильных технических средств на предмет выявления их несанкционированного использования для доступа к объектам доступа ИС.	1. см. п.п. 5.5 документа «Руководство по эксплуатации СХСЗ»; см. п.п. 5.3 документа «Руководство по эксплуатации клиентских устройств».
		Реагирование на компьютерные инциденты (ИНЦ)			
52	ИНЦ.0	Разработка политики реагирования на компьютерные инциденты	+ все	Комплекс поддерживает возможность хранения в журнале событий информации о неисправностях (отказах в обслуживании, сбоях в работе и т.д.).	
53	ИНЦ.2	Информирование о компьютерных инцидентах	+ все		1. см. п.п. 3.9, 4.9. 5.11, 6.10, 7.9 документа «Руководство по эксплуатации СХСЗ»; 2. см. п.п. 4.7 документа «Руководство по эксплуатации клиентских устройств».
		Управление конфигурацией (УКФ)			
54	УКФ.0	Разработка политики управления конфигурацией информационной (автоматизированной) системы	+ все	Имеется возможность управления изменениями и установки только разрешенного к использованию программного обеспечения. При создании образов ПО ТС к сборке допускается только разрешенное к использованию ПО. Возможность изменения состава образов ПО ТС имеется только у администратора ИБ СХСЗ.	
55	УКФ.2	Управление изменениями	+ все		1. см. п.п. 5.5, 5.6, 5.10 документа «Руководство по эксплуатации СХСЗ».
56	УКФ.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения	+ все	Комплекс обеспечивает установку и управление фиксированными наборами ПО РС. Комплекс обеспечивает автоматизированную	1. см. п.п. 4.6, 4.8, 5.5, 5.8, 5.10 документа «Руководство по эксплуатации СХСЗ».

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	ПАК «Центр-Т»	Ссылки на документацию
				инсталляцию и централизованное управление шаблонами образов ПО и настроек параметров компонентов ПО РС. Комплекс обеспечивает запуск на Клиенте только назначенного администратором СХСЗ docker-образа ПО. Конкретный docker-образ ПО определяет фиксированный подлежащий установке набор ПО.	
		Управление обновлениями программного обеспечения (ОПО)			
57	ОПО.0	Разработка политики управления обновлениями программного обеспечения	+ все	Комплекс обеспечивает возможность установки обновлений программного обеспечения «Центр-Т»: – обновления ПО СХСЗ; – обновления ПО Клиента; – обновления firmware носителей СХСЗ и клиента. Обновления ПО и firmware носителей выполняются в сервисном центре Разработчика.	
58	ОПО.4	Установка обновлений программного обеспечения	+ все		
		Обеспечение действий в нештатных ситуациях (ДНС)			
59	ДНС.0	Разработка политики обеспечения действий в нештатных ситуациях	+ все	«Центр-Т» обеспечивает резервное копирование и восстановление баз данных и настроек.	
60	ДНС.4	Резервирование программного обеспечения, технических средств, каналов связи на случай возникновения нештатных ситуаций	+ начиная со 2 класса защищенности автоматизированной системы управления	Комплекс обеспечивает возможность резервного копирования баз данных и настроек СХСЗ, локальных настроек Клиента	1. см. п.п. 3.5 документа «Руководство по эксплуатации СХСЗ»; 1. см. п.п. 4.5 документа «Руководство по эксплуатации клиентских устройств».
61	ДНС.5	Обеспечение возможности восстановления информационной (автоматизированной) системы в случае возникновения нештатных ситуаций	+ все	Комплекс обеспечивает возможность восстановления баз данных и настроек СХСЗ, локальных настроек Клиента из резервных копий.	1. см. п.п. 3.5 документа «Руководство по эксплуатации СХСЗ»; 2. см. п.п. 4.6 документа «Руководство по эксплуатации клиентских устройств».

3 Выполнение дополнительных (не включенных в базовый набор) мер, определенных 31-ым приказом ФСТЭК России по защите информации

в автоматизированной системе управления, путем применения ПАК СЗИ НСД «Центр-Т»

В таблице № 2 представлено описание выполнения дополнительных (не включенных в базовый набор) мер 31-го приказа ФСТЭК по защите информации в автоматизированной системе управления путем применения ПАК СЗИ НСД «Центр-Т».

Таблица 2 - Выполнение дополнительных (не включенных в базовый набор) мер по защите информации 31-го приказа ФСТЭК по защите информации в автоматизированной системе управления путем применения ПАК СЗИ НСД «Центр-Т»

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	ПАК «Центр-Т»	Ссылки на документацию
		Идентификация и аутентификация субъектов и объектов доступа (ИАФ)			
1	ИАФ.6	Двусторонняя аутентификация		Комплекс поддерживает функцию двусторонней аутентификации: При соединении с сервером Клиент аутентифицируется на СХСЗ. Аутентификация СХСЗ на клиенте выполняется при передаче образа ПО РС.	1. см. Введение документа «Руководство по эксплуатации СХСЗ».
		Управление доступом субъектов доступа к объектам доступа (УПД)			
2	УПД.7	Предупреждение пользователя при его доступе к информационным ресурсам		При загрузке ПО ПАК «Центр-Т» на экране отображается информация о том, что выполняется загрузка комплекса «Центр-Т»	
		Ограничение программной среды (ОПС)			
3	ОПС.3	Управление временными файлами		В ОС семейства Linux временные файлы сохраняются в каталог /tmp. Данный каталог имеется и в ОНЗ Клиента, и в каждом контейнере. В ОНЗ при каждой перезагрузке Клиента (средствами ОС) очистка каталога /tmp выполняется автоматически. К каталогу временных файлов, находящемуся в контейнере, доступ извне отсутствует	
		Обеспечение доступности (ОДТ)			
4	ОДТ.7	Кластеризация информационной (автоматизированной) системы		Кластеризация информационной системы и (или) ее сегментов возможна при условии применения ПАК	1. см. п.п. 3.2, 3.6, Приложение 4 документа «Руководство по эксплуатации СХСЗ».

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	ПАК «Центр-Т»	Ссылки на документацию
				«Центр-Т» с аппаратной частью сервера хранения и сетевой загрузки и терминальных станций Клиента ПАК СЗИ НСД «Центр-Т», реализованной на базе защищенного микрокомпьютера.	
		Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)			
5	ЗИС.9	Создание гетерогенной среды		Клиенты ПАК «Центр-Т» функционируют под управлением ОС семейства Linux (ОНЗ представляет собой ОС Linux). Терминальный сервер, а также АРМ администратора СХСЗ функционируют под управлением ОС семейства Windows.	1. см. Введение и Приложение 5 документа «Руководство по эксплуатации СХСЗ».
6	ЗИС.10	Использование программного обеспечения, функционирующего в средах различных операционных систем			
7	ЗИС.12	Изоляция процессов (выполнение программ) в выделенной области памяти		Изоляция процессов в ПАК «Центр-Т» выполняется за счет использования технологии контейнеризации (docker).	1. см. п.п. 3.7, 9 документа «Руководство по эксплуатации СХСЗ».
8	ЗИС.14	Использование неперезаписываемых машинных носителей информации		Образ начальной загрузки (предварительно подготовленные образы ОС, содержащие необходимое ПО для соединения с терминальным сервером) СХСЗ и Клиентов располагается на неперезаписываемых носителях ПО СХСЗ и ПО Клиента соответственно.	1. см. п.п. «Введение», 1, 2 документа «Руководство по эксплуатации СХСЗ»; 2. см. п.п. «Аннотация», 1, 2 документа «Руководство по эксплуатации клиентских устройств»; 3. см. п.п. 1.2 документа «Описание применения».
9	ЗИС.17	Защита информации от утечек		ПАК «Центр-Т» обеспечивает блокировку в ИС скрытых каналов передачи информации, существующих в исходной («родной») ОС терминала: блокировка обеспечивается посредством загрузки образа ПО РС с носителя «Центр-Т», защищенного от перезаписи. Целостность образа ПО РС проверяется на этапе его получения Клиентом.	
10	ЗИС.18	Блокировка доступа к сайтам или типам сайтов, запрещенных к использованию		Блокировка доступа к неразрешенным типам ПО обеспечивается за счет возможности создания замкнутой программной среды на терминальной станции, допускающей запуск в ней только фиксированного образа ПО, а также установки и управления фиксированными наборами ПО Клиентов.	1. см. п.п. 4.6, 4.8, 5.5, 5.8, 5.10 документа «Руководство по эксплуатации СХСЗ».
11	ЗИС.26	Подтверждение происхождения источника		ПАК «Центр-Т» обеспечивает возможность аутентификации	1. см. п.п. Введение, 3.4, 4.2 документа «Руководство по

№	Усл. обозн. и номер меры	Меры защиты информации в автоматизированных системах безопасности	Классы защищенности автоматизированной системы управления	ПАК «Центр-Т»	Ссылки на документацию
		информации		терминального сервера аутентифицированным СХСЗ. Аутентификация терминального сервера выполняется по его сетевому адресу (IP-адресу).	эксплуатации СХСЗ».
12	ЗИС.30	Использование устройств терминального доступа		Комплекс поддерживает работу с решением Citrix. Подключение к терминальному серверу выполняется по протоколу ICA.	1. см. п.п. «Введение», 4.6, 4.7, 11 документа «Руководство по эксплуатации СХСЗ».

Итак, путем применения ПАК «Центр-Т» в автоматизированной системе управления выполняются следующие меры, включенные в базовый набор мер защиты информации для соответствующего класса защищенности информационной системы:

ИАФ: 1, 2, 3, 4, 7;

УПД: 1, 2, 3, 4, 5, 6, 9, 10, 11, 13;

ОПС: 1, 2;

ЗНИ: 2, 5, 6, 7;

АУД: 2, 3, 4, 6, 7, 9;

ОЦЛ: 1, 3;

ОДТ: 2, 3, 6, 8;

ЗИС: 1, 13, 20, 21, 27, 31, 33, 34, 35, 38;

ИНЦ: 2;

УКФ: 2, 3;

ОПО: 4;

ДНС: 4, 5;

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

ИАФ: 6;

УПД: 7;

ОПС: 3;

ОДТ: 7;

ЗИС: 9, 10, 12, 14, 17, 18, 26, 30.

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