ВЫПОЛНЕНИЕ МЕР 17-ГО И 21-ГО ПРИКАЗОВ ФСТЭК ПО ЗАЩИТЕ ИНФОРМАЦИИ В ИНФОРМАЦИОННОЙ 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 информационной системе персональных данных (ИСПДн) путем применения программно-аппаратного комплекса средств 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;

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

- производить идентификацию/аутентификацию пользователей ТС для начала работы с терминальным сервером;
- 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 17-ым и 21-ым приказами ФСТЭК России по защите информации в информационной системе, путем применения ПАК СЗИ НСД «Центр-Т»

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 СЗИ НСД «Центр-Т».

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.

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.

Выражением «нет» выделены ячейки столбца «Классы защищенности ИС», которые относятся к требованиям, содержащимся только в 21-ом приказе ФСТЭК, и, следовательно, не относящимся к классам защищенности ИС.

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 СЗИ от НСД «Центр-Т»

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	ПАК СЗИ НСД «Центр-Т»	Ссылки на документацию
		Идентификация и аутентификация субъектов и объектов доступа (ИАФ)				
1	ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	+ все	+ 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. Администраторы удалённого управления СХСЗ предъявляют логин, пароль, идентификатор. Пользователи клиентского устройства идентифицируются по номерам их Клиентского устройства.	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.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	ПАК СЗИ НСД «Центр-Т»	Ссылки на документацию
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	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».
3	ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	+ все	+ 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 шаблонов настроек ПО РС.	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».
4	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		
5	ИАФ.5	Защита обратной связи при вводе аутентификационной информации	+ все	+ все	Функция аутентификации обеспечивает исключение отображения для пользователя действительного значения	1. см. п.п. 4.3, документа «Руководство по эксплуатации СХСЗ».

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	ПАК СЗИ НСД «Центр-Т»	Ссылки на документацию
					аутентификационной информации за счет отображения вводимых символов аутентификационной информации условными знаками.	
6	ИАФ.7	Идентификация и аутентификация объектов файловой системы, запускаемых и исполняемых модулей, объектов систем управления базами данных, объектов, создаваемых прикладным и специальным программным обеспечением, иных объектов доступа	нет	не входит в базовый набор мер	Обеспечивается средствами ОС, входящей в ПО СХС3 и ПО Клиента.	1. см. п.п. «Введение» документа «Руководство по эксплуатации СХС3».
		Управление доступом субъектов доступа к объектам доступа (УПД)				
7	УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	+ все	+ все	В комплексе обеспечивается поддержка учетных записей пользователей, администраторов СХС3, администраторов Клиентских устройств.	1. см. п.п. 4.5.1 документа «Руководство по эксплуатации СХС3».
8	УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	+ все	+ все	Ролевой метод реализован в виде групп пользователей: Пользователи административной группы: – Администратор СХС3; – Администратор нештатного режима работы СХС3; – Администратор ИБ СХС3; – Контролер СХС3; – Администратор Клиентских устройств; – Администратор ИБ клиентских устройств. Пользователи клиентской группы: – Пользователи Клиентских устройств.	1. см. п. 1 документа «Руководство по эксплуатации СХС3»; 2. см. п. 1 документа «Руководство по эксплуатации клиентских устройств».
9	УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц,	+ все	+ все	Комплекс обеспечивает разделение полномочий: реализованы группы пользователей:	1. см. п. 1, 2 документа «Руководство по эксплуатации СХС3»;

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	ПАК СЗИ НСД «Центр-Т»	Ссылки на документацию
		обеспечивающих функционирование информационной системы			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.	2. см. п. 1 документа «Руководство по эксплуатации клиентских устройств».
10	УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	+ все	+ все		
11	УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	+	+	Ограничение попыток доступа к ИС в рамках управления доступом регулируется СЗИ НСД серверной группы, например, СЗИ НСД «Аккорд-Win64 K» (TSE), установленном на СХСЗ.	1. см. п.п. 7.3 документа «Установка правил разграничения доступа. Программа ACED32».
12	УПД.9	Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы	Не входит в базовый набор мер	+ начиная с 1 класса защищенности ИС	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».
13	УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу	+ начиная с 3 уровня защищенности ПДн	+ все	Комплекс позволяет выполнить настройку блокирование 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».

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	ПАК СЗИ НСД «Центр-Т»	Ссылки на документацию
14	УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации	+ начиная с 3 уровня защищенности ПДн	+ все	До проведения идентификации и аутентификации пользователям административной группы запрещены любые действия кроме ввода идентификационной и аутентификационной информации, предъявления аппаратного идентификатора, смены пользователя.	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».
15	УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные связи	+ все	+ все	Подключение к СХСЗ обеспечивается по защищённому протоколу SSH.	1. см. Приложение 2 документа «Руководство по эксплуатации СХСЗ».
16	УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств	+	+	Контроль и мониторинг применения мобильных технических средств на предмет выявления их несанкционированного использования для доступа к объектам доступа ИС обеспечивается за счет средств СЗИ НСД «Аккорд».	1. см. п.п. 5.5 документа «Руководство по эксплуатации СХСЗ»; 2. см. п.п. 5.3 документа «Руководство по эксплуатации клиентских устройств».
17	УПД.17	Обеспечение доверенной загрузки средств вычислительной техники[1]	+ начиная со 2 уровня защищенности ПДн	+ начиная со 2 класса защищенности ИС	Выполнение меры УПД.17 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».
		Ограничение программной среды (ОПС)				
18	ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском	не входит в базовый набор мер	+ начиная с 1 класса защищенности ИС	Комплекс обеспечивает возможность создания замкнутой программной среды на рабочей станции, допускающей запуск в ней только фиксированного образа ПО.	1. см. п.п. 4.6, 4.8, 5.5, 5.8, 5.10 документа «Руководство по эксплуатации СХСЗ».

[1] Угроза доверенной загрузки может быть признана неактуальной в случае блокирования внешних интерфейсов системного блока компьютера, извлечения CD/DVD-приводов и пр. для исключения возможности произвести загрузку недоверенной ОС со сторонних носителей информации.

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	ПАК СЗИ НСД «Центр-Т»	Ссылки на документацию
		компонентов программного обеспечения				
19	ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения	+ начиная со 2 уровня защищенности ПДн	+ начиная со 2 класса защищенности ИС	Комплекс обеспечивает установку и управление фиксированными наборами ПО РС. Комплекс обеспечивает автоматизированную 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.	
20	ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов	+ начиная с 1 уровня защищенности ПДн	+ все		
		Защита машинных носителей персональных данных (ЗНИ)				
21	ЗНИ.2	Управление доступом к машинным носителям персональных данных	+ начиная со 2 уровня защищенности ПДн	+ все	В комплексе предусмотрена возможность создания образа ПО РС: – с возможностью проброса usb-устройств в терминальную сессию; – без возможности проброса usb-устройств в терминальную сессию.	1. см. п.п. 5.5 документа «Руководство по эксплуатации СХСЗ»; 2. см. п.п. 5.3 документа «Руководство по эксплуатации клиентских устройств».
22	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	В комплексе предусмотрена возможность создания образа ПО РС: – с возможностью проброса usb-устройств в терминальную сессию; – без возможности проброса usb-устройств в терминальную сессию.	
		Регистрация событий безопасности (РСБ)				
23	РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	+ все	+ все	Состав и содержание событий безопасности определяются для событий, которые связаны с функциональными возможностями комплекса (процедуры идентификации и	1. см. п.п. 3.9, 4.9. 5.11, 6.10, 7.9 документа «Руководство по эксплуатации СХСЗ»;

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	ПАК СЗИ НСД «Центр-Т»	Ссылки на документацию
24	РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	+ все	+ все	аутентификации, копирование лицензий, сборка образа ПО РС, создание и редактирование учетных записей пользователей и т.д.). При регистрации событий фиксируется исчерпывающий набор параметров: дата и время, идентификатор субъекта, идентификатор объекта, тип выполняемой операции, результат операции и др.	2. см. п.п. 4.7 документа «Руководство по эксплуатации клиентских устройств».
25	РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	+ все	+ все	В комплексе имеется возможность регистрации возникновения событий, относящихся к событиям безопасности. Администратор сервисного режима может просмотреть события безопасности: – собственной сессии; – 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;	

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	ПАК СЗИ НСД «Центр-Т»	Ссылки на документацию
					– 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 запись, от имени которой выполнено действие); – источник события.	
26	РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них	+ начиная со 2 уровня защищенности ПДн	+ все	Комплекс обеспечивает просмотр зарегистрированных в журнале событий безопасности администраторам СХСЗ, проведшим процедуры И/А.	
27	РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе	Не входит в базовый набор мер	+ 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.	
28	РСБ.7	Защита информации о событиях	+ все	+ все	Защита информации о событиях безопасности	

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	ПАК СЗИ НСД «Центр-Т»	Ссылки на документацию
		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 НШР; – доступ к общему журналу предоставляется администраторам удаленного управления; – доступ к локальному журналу Клиента предоставляется администратору ИБ Клиента.	
		Контроль (анализ) защищенности персональных данных (АН3)				
29	АН3.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей	+ начиная с 3 уровня защищенности ПДн	+ 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».
30	АН3.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	+ все	+ все	Комплекс обеспечивает возможность установки обновлений программного обеспечения «Центр-Т»: – обновления ПО СХСЗ; – обновления ПО Клиента; – обновления firmware носителей СХСЗ и клиента.	
31	АН3.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации	+ начиная с 3 уровня защищенности ПДн	+ все	Комплекс обеспечивает возможность регистрации информации о событиях, связанных с нарушением работоспособности комплекса и параметров настройки ПО и СЗИ. В случае обнаружения нарушения работоспособности или параметров настройки имеется возможность	1. см. п.п. 3.5, 5.11, 6.10, 7.9, документа «Руководство по эксплуатации СХСЗ»; 1. см. п.п. 4.5, 4.6, 4.7 документа «Руководство по эксплуатации клиентских

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	ПАК СЗИ НСД «Центр-Т»	Ссылки на документацию
					резервного копирования баз данных и настроек СХСЗ, локальных настроек Клиента с последующим восстановлением резервных копий.	устройств».
32	АН3.4	Контроль состава технических средств, программного обеспечения и средств защиты информации	+	+	Контроль состава технических средств, программного обеспечения и средств защиты информации обеспечивается тем, что Администратор из состава персонала «Центр-Т» на этапе сборки образов ПО РС наполняет их только проверенными и разрешенными к использованию элементами.	1. см. п.п. 4.6, 4.8, 5.5, 5.8, 5.10 документа «Руководство по эксплуатации СХСЗ».
33	АН3.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе	+ начиная со 2 уровня защищенности ПДн	+ все	Комплекс обеспечивает возможность смены паролей администратора, администратора ИБ, администратора НШР, контролера СХСЗ. Комплекс поддерживает возможность заведения и удаления пользователей. Данные процедуры выполняет администратор СХСЗ во вкладке «Пользователи». Администратор СХСЗ может удалять только те учетные записи, для которых установлена роль «Пользователь клиентского устройства». Если учетной записи присвоена роль административной группы, то при необходимости ее удаления следует сначала назначить ей роль «Пользователя клиентского устройства» (выполняется Администратором БИ или Администратором НШР) и только затем – удалить. При попытке удалить учетные записи с ролью администратора удаленного управления СХСЗ в журнале появляется сообщение «Нельзя удалить пользователя с ролью администратора!».	1. см. п.п. 3.2, 4.3, 4.5, 5.3, 6.3, 7.3 документа «Руководство по эксплуатации СХСЗ»; 2. см. п.п. 3.3, 4.2 документа «Руководство по эксплуатации клиентских устройств».
		Обеспечение целостности информационной системы и персональных данных (ОЦЛ)				

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	ПАК СЗИ НСД «Центр-Т»	Ссылки на документацию
34	ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации	+ начиная со 2 уровня защищенности ПДн	+ начиная со 2 класса защищенности ИС	Комплекс обеспечивает возможность контроля целостности образов ПО РС.	1. см. п. «Введение» «Руководство по эксплуатации СХСЗ»; 2. см. п.п. 5.3 документа «Руководство по эксплуатации клиентских устройств».
35	ОЦЛ.3	Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций	не входит в базовый набор мер	+ все	Комплекс обеспечивает возможность восстановления баз данных и настроек СХСЗ, локальных настроек Клиента.	1. см. п.п. 3.5 документа «Руководство по эксплуатации СХСЗ»; 2. см. п.п. 4.6 документа «Руководство по эксплуатации клиентских устройств».
36	ОЦЛ.6	Ограничение прав пользователей по вводу информации в информационную систему	не входит в базовый набор мер	+ начиная с 1 класса защищенности ИС	Комплекс ограничивает права пользователей по вводу информации в ИС путем обеспечения ограничения программной среды.	1. см. п. 1, 2 документа «Руководство по эксплуатации СХСЗ»; 2. см. п. 1 документа «Руководство по эксплуатации клиентских устройств».
		Обеспечение доступности персональных данных (ОДТ)				
37	ОДТ.2	Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы	не входит в базовый набор мер	+	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».
38	ОДТ.3	Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование	+ начиная с 1 уровня защищенности ПДн	+ начиная со 2 класса защищенности ИС	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».

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	ПАК СЗИ НСД «Центр-Т»	Ссылки на документацию
		Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)				
39	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 функций информационной системы	+ начиная с 1 уровня защищенности ПДн	+ начиная со 2 класса защищенности ИС	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».
40	ЗИС.5	Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств	не входит в базовый набор мер	+ все	В ПАК «Центр-Т» предусмотрена возможность контроля подключения устройств вывода и записи звука. Параметры корректируются во вкладке «Периферийные устройства». В комплексе предусмотрена возможность контроля подключения usb-устройств в рамках терминальной сессии. Образы ПО РС возможно создать: – с возможностью проброса usb-устройств в терминальную сессию; – без возможности проброса usb-устройств в терминальную сессию.	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».
41	ЗИС.11	Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов	+ начиная со 2 уровня защищенности ПДн	+ начиная со 2 класса защищенности ИС	Образы ПО РС, создаваемые на СХСЗ, сопоставляются с номерами клиентского устройств. При отправке образа на РС СХСЗ проверяет сопоставлен ли номер клиентского устройства пересылаемому образу ПО.	1. см. п.п. 5.3 документа «Руководство по эксплуатации клиентских устройств».

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	ПАК СЗИ НСД «Центр-Т»	Ссылки на документацию
					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.	
42	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	Производится контроль целостности docker-образов (образов ПО РС).	1. см. п.п. 3.7, документа «Руководство по эксплуатации СХСЗ»; 2. см. п.п. 5.3 документа «Руководство по эксплуатации клиентских устройств».
43	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	нет	+ начиная с 1 класса защищенности ИС	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 СХСЗ».
44	ЗИС.22	Защита информационной системы от угроз безопасности информации, направленных на отказ в обслуживании информационной системы	нет	+ начиная со 2 класса защищенности ИС	Комплекс «Центр-Т» контролирует подлинность ПО РС при передаче на клиентское устройство.	1. см. п.п. 5.3 документа «Руководство по эксплуатации клиентских устройств».
		Выявление инцидентов и реагирование на них (ИНЦ)				
45	ИНЦ.2	Обнаружение, идентификация и регистрация инцидентов	+ начиная со 2 уровня защищенности ПДн	нет	Комплекс поддерживает возможность хранения в журнале событий информации о неисправностях (отказах в обслуживании, сбоях в работе и т.д.).	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

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	ПАК СЗИ НСД «Центр-Т»	Ссылки на документацию
						«Руководство по эксплуатации клиентских устройств».
		Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ)				
46	УКФ.2	Управление изменениями конфигурации информационной системы и системы защиты персональных данных	+ начиная с 3 уровня защищенности ПДн	нет	Имеется возможность управления изменениями и установки только разрешенного к использованию программного обеспечения. При создании образов ПО РС к сборке допускается только разрешенное к использованию ПО. Возможность изменения состава образов ПО РС имеется только у администратора ИБ СХСЗ.	1. см. п.п. 5.5, 5.6, 5.10 документа «Руководство по эксплуатации СХСЗ».

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 СЗИ НСД «Центр-Т»

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 комплекса ПАК СЗИ НСД «Центр Т».

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 СЗИ от НСД «Центр-Т»

№	Усл. обозн.	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности ПДн	Классы защищенности ИС	ПАК СЗИ НСД «Центр-Т»	Ссылки на документацию
		Управление доступом субъектов доступа к объектам доступа (УПД)				
1	УПД.7	Предупреждение			При загрузке ПО ПАК «Центр-	

		пользователя при его входе в информационную систему о том, что в информационной системе реализованы меры защиты информации, и о необходимости соблюдения им установленных оператором правил обработки информации			Т» на экране отображается информация о том, что выполняется загрузка комплекса «Центр-Т»	
		Защита машинных носителей персональных данных (ЗНИ)				
2	ЗНИ.6	Контроль ввода (вывода) информации на машинные носители персональных данных			В комплексе предусмотрена возможность создания образа ПО РС: – с возможностью проброса usb-устройств в терминальную сессию; – без возможности проброса usb-устройств в терминальную сессию.	1. см. п.п. 5.5 документа «Руководство по эксплуатации СХСЗ»; 2. см. п.п. 5.3 документа «Руководство по эксплуатации клиентских устройств».
3	ЗНИ.7	Контроль подключения машинных носителей персональных данных				
		Ограничение программной среды (ОПС)				
4	ОПС.4	Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов			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	
		Регистрация событий безопасности (РСБ)				
5	РСБ.8	Обеспечение возможности просмотра и анализа информации о действиях отдельных пользователей в информационной системе	нет		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)	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».

					период. С помощью применения фильтра можно проанализировать работу каждого пользователя.	
		Обеспечение доступности персональных данных (ОДТ)				
6	ОДТ.6	Кластеризация информационной системы и (или) ее сегментов	нет		Кластеризация информационной системы и (или) ее сегментов возможна при условии применения ПАК «Центр-Т» с аппаратной частью сервера хранения и сетевой загрузки и терминальных станций Клиента ПАК СЗИ НСД «Центр-Т», реализованной на базе защищенного микрокомпьютера.	1. см. п.п. 3.2, 3.6, Приложение 4 документа «Руководство по эксплуатации СХСЗ».
		Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)				
7	ЗИС.4	Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации)			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».
8	ЗИС.10	Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам			ПАК «Центр-Т» обеспечивает возможность аутентификации терминального сервера аутентифицированным СХСЗ. Аутентификация терминального сервера выполняется по его сетевому адресу (IP-адресу).	1. см. п.п. Введение, 3.4, 4.2 документа «Руководство по эксплуатации СХСЗ».
9	ЗИС.14	Использование устройств терминального доступа для обработки персональных данных			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».
10	ЗИС.16	Выявление, анализ и блокирование в информационной системе скрытых каналов передачи информации в обход реализованных мер защиты информации или внутри разрешенных сетевых протоколов			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.	
11	ЗИС.18	Обеспечение загрузки и исполнения программного обеспечения с машинных носителей персональных данных, доступных только для чтения, и контроль целостности данного программного обеспечения			Комплекс обеспечивает загрузку и исполнение программного обеспечения СХСЗ, Клиента, АРМ эмиссии со специальных носителей информации (CH, выполненные в форм-факторе USB, также CH на базе защищенного микрокомпьютера), доступных только для чтения.	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».
12	ЗИС.19	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».
13	ЗИС.25	Использование в информационной системе или ее сегментах различных типов общесистемного, прикладного и специального программного обеспечения (создание гетерогенной среды)	нет		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».
14	ЗИС.26	Использование прикладного и специального программного обеспечения, имеющих возможность функционирования в средах различных операционных систем	нет			

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

ИАФ: 1, 2, 3, 4, 5;

УПД: 1, 2, 4, 5, 6, 9, 10, 11, 13, 15, 17;

ОПС: 1, 2, 3;

ЗНИ: 2, 5;

РСБ: 1, 2, 3, 5, 6, 7;

АНЗ: 1, 2, 3, 4, 5;

ОЦЛ: 1, 3, 6;

ОДТ: 2, 3;

ЗИС: 1, 5, 11, 15, 21, 22;

ИНЦ: 2;

УКФ: 2.

а также дополнительные (не включенные в базовый набор) меры:
ИАФ: 7;
УПД: 7;
ОПС: 4;
ЗНИ: 6, 7;
ОДТ: 6;
РСБ: 8;
ЗИС: 4, 10, 14, 16, 18, 19, 25, 26.

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