ОГЛАВЛЕНИЕ

1 ИНСТРУМЕНТ ДЛЯ ЗАЩИЩЕННОГО ХРАНЕНИЯ И СЕТЕВОЙ ЗАГРУЗКИ КЛИЕНТСКИХ КОМПЬЮТЕРОВ: ЦЕНТР-Т

1.1 ДЛЯ ЧЕГО НУЖЕН ЦЕНТР-Т

Программно-аппаратный комплекс (ПАК) «Центр-Т» предназначен для централизованного администрирования, контроля целостности и контролируемой загрузки образов программного обеспечения (ПО) на клиентские рабочие станции. Речь идет о загрузке той вычислительной среды, из которой будет установлено соединение с системой, в которой будет работать удаленный пользователь. Это может быть как работа с терминальным сервером по терминальному протоколу, так и режим виртуального рабочего стола или работа в виртуальной машине, и так далее. Во всех этих случаях необходимо подключиться к некоторому удаленному защищенному ресурсу с клиентского рабочего места.

1.2 ЧТО НУЖНО КУПИТЬ ДЛЯ ВНЕДРЕНИЯ ЦЕНТР-Т

В общем случае использование «Центр-Т» не требует ни приобретения дополнительных СВТ, ни трудоемких работ по развертыванию инфраструктуры: ПО комплекса загружается на уже имеющиеся в системе СВТ со специальных носителей, входящих в состав комплекса.

1.3 КАК РАБОТАЕТ ЦЕНТР-Т

Защищённая сетевая загрузка образов ПО на рабочие станции (РС) производится в 2 этапа.

1) На первом с отчуждаемого USB-носителя (он называется «*Специальный носитель ПО "Клиент Центр-Т"*») загружается образ ОС, называемый образом начальной загрузки (ОНЗ). ОНЗ на отчуждаемом носителе хранится в разделе, доступном только на чтение, тем самым обеспечивается загрузка *целостной* и *аутентифицированной* ОС из *аутентифицированного источника*. Основное и единственное назначение ОНЗ – обеспечение защищенности второго этапа загрузки.

2) Второй этап – сетевая загрузка того программного обеспечения, посредством которого производится подключение к серверу (сервер может быть терминальным или, например, это может быть инфраструктура виртуализации с виртуальными рабочими столами или веб-сервер).

ПО, которое загружается на клиентские рабочие места по сети, рассылается с ***Сервера хранения и сетевой загрузки*** (СХСЗ). Это серверный элемент инфраструктуры «Центр-Т», ПО которого (включая ОС), в свою очередь, загружается на произвольное СВТ со «*Специального носителя ПО СХСЗ*».

В общем виде это и все.

1.4 ИЗ ЧЕГО СОСТОИТ ЦЕНТР-Т

Вообще, все компоненты «Центр-Т» размещены на специальных носителях информации, и могут исполняться, загружаясь с этих носителей, на любом ПК. Это обеспечивает комплексу значительную аппаратную независимость. После отключения носителей на ПК не остается никаких компонентов комплекса или используемых им данных.

Специальные носители ПО «Центр-Т» – это защищенные USB-устройства.

В зависимости от того, какое именно ПО содержится на специальном носителе, различаются:

- носитель ПО СХС3 (далее по тексту – СН СХС3), с него загружается сервер хранения и сетевой загрузки;
- носитель ПО «Клиент Центр-Т» (далее по тексту – СН РС), с которого загружаются рабочие станции (РС);
- носитель автоматизированного рабочего места (АРМ) Эмиссии, с которого загружается, соответственно, АРМ Эмиссии.

Эти носители подключаются к СВТ, которые в инфраструктуре эксплуатирующей организации будут использоваться в качестве СХС3, клиентских терминалов и АРМ Эмиссии соответственно. Именно это делает возможным использовать в развертываемой инфраструктуре уже имеющиеся СВТ[1)] .

Если же нет задачи использовать имеющиеся СВТ, все три вида аппаратных компонентов инфраструктуры «Центр-Т» можно приобрести реализованными «под ключ», на базе специализированных микрокомпьютеров с аппаратной защитой данных «m-TrusT». В таком случае СХС3 представляет собой защищенное автоматизированное рабочее место ХС3 (далее по тексту – защищенное АРМ ХС3), а клиентское рабочее место – защищенный терминал «Центр-TrusT» [2)]).

В состав программной части ПАК СЗИ НСД «Центр-Т», кроме образов резидентных ОС СХС3, РС и АРМ Эмиссии, входит ПО удаленного управления «Центр-Т» – оно нужно для того, чтобы управляющий персонал СХС3 работа не в серверной комнате, а управлял системой с нормального офисного рабочего места.

[1)] С учетом следующих ограничений:

- архитектура процессора x86-64 с поддержкой аппаратной виртуализации;

- наличие 2 гигабайт оперативной памяти;

- возможность загрузки с USB-носителей.

[2)] Вариант исполнения аппаратной части ПАК СЗИ НСД «Центр-Т» выбирается при заказе.

1.5 ФУНКЦИИ ЦЕНТР-Т

Функциональность ПАК «Центр-Т» можно объединить в следующие блоки

- ***сетевая загрузка ПО на РС:***
  - идентификация пользователей РС для начала работы с терминальным сервером по номерам клиентских устройств;
  - двухфакторная аппаратная идентификация пользователей РС в ПАК «Аккорд» на терминальном сервере;
  - передача образов ПО РС на РС по сети;
  - проверка целостности и подлинности полученного образа Клиентом;

- ***централизованное администрирование:***
  - создание учетных записей пользователей;
  - назначение учетным записям клиентских устройств;
  - сборка образов ПО РС;
  - сопоставление образов ПО РС учетным записям пользователей;
  - настройка сетевых параметров;
  - резервирование баз данных и настроек СХС3 и Клиента;
  - восстановление ПО «Центр-Т» из резервных копий при возникновении нештатных ситуаций;
  - контроль периферийного оборудования в рамках терминальной сессии: контроль использования USB-принтеров и/или flash-накопителей информации, подключенных непосредственно к РС;
  - контроль настроек образов ПО РС;

- ***централизованный аудит событий:***
  - регистрация пользователей и клиентских устройств;
  - регистрация действий пользователей и администраторов СХС3 в журналах загрузки образов ПО РС и журналах активности администраторов СХС3.

Графически распределение функций ПАК «Центр-Т» по его инфраструктурным элементам можно представить так:

Рисунок 1 – Структурная схема ПАК «Центр-Т»

2 СРАВНЕНИЕ ПАК «ЦЕНТР-Т» С РЕШЕНИЯМИ, КОТОРЫЕ ПРЕДЛАГАЮТ СИСТЕМНЫЕ ИНТЕГРАТОРЫ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1 КАК БУДЕМ СРАВНИВАТЬ

Чтобы увидеть, что применение ПАК «Центр-Т» удобно, попробуем сравнить, что требуется для того, чтобы *без использования комплекса «Центр-Т»* в ИС был реализован такой же набор защитных мер, как и *при его использовании*.

Для этого, можно, например, рассмотреть, использование каких средств и технологий предлагают системные интеграторы для того, чтобы в информационной системе Заказчика были приняты все те же меры защиты, которые обеспечил бы в ней «Центр-Т».

Тогда мы сможем оценить, насколько применение ПАК «Центр-Т» сделает ИС не только более защищенной, но и более управляемой, более простой в обслуживании и эксплуатации.

Сопоставим ПАК «Центр-Т» с альтернативными решениями в отношении следующих основных мер защиты:

- (ИАФ) идентификация и аутентификация пользователей;
- (УПД) управление доступом;
- (ОПС) ограничение программной среды;
- (АНЗ) контроль защищенности данных;
- (ОДТ) обеспечение доступности данных;
- (ОЦЛ) обеспечение целостности ИС и данных;
- (ЗИС) обеспечение защиты ИС.

Для сравнения рассматривались решения информационной безопасности, которые предлагают следующие системные интеграторы:

«Айтеко»;

«TAdviser»;

«IBS»;

«X-Com»;

«Инфосистемы Джет»;

«Астерит»;

«ДиалогНаука».

2.2 СОПОСТАВЛЕНИЕ ПАК «ЦЕНТР-Т» С ДРУГИМИ РЕШЕНИЯМИ

Таблица 1 – Выполнение мер защиты с помощью Центр-Т и с помощью альтернативных решений, предлагаемых на рынке

Меры защиты ИС	**Как реализуется с помощью «Центр-Т»**	**Какие компоненты «Центр-Т» выполняют эти функции**	**Решения (ПО и оборудование), которые предлагают системные интеграторы для реализации меры защиты**	**Без каких средств и решений из предыдущего столбца можно обойтись, применяя ПАК «Центр-Т», и почему**
Идентификация и аутентификация пользователей	(ИАФ.1-ИАФ.5) Идентификация выполняется по номерам клиентских устройств (специальных носителей), которые сопоставлены учетным записям пользователей. Двусторонняя аутентификация выполняется прозрачно для пользователей и администраторов комплекса: при соединении с сервером клиентское устройство аутентифицируется на СХС3. Аутентификация СХС3 на Клиенте выполняется при передаче образа ПО РС Для идентификации пользователей не требуется применение дополнительного	– ПО СХС3; – ПО Клиента (образ начальной загрузки); – носитель ПО СХС3; – носитель ПО Клиента.	***Принципиальные решения и работы:*** – системы идентификации и аутентификации (в том числе многофакторной аутентификации); – обеспечение интеграции предложенных решений и оборудования в ИС. ***Конкретное ПО и оборудование:*** – системы многофакторной аутентификации (Cisco DUO, Multifactor, Avanpost FAM, Biolink); – считыватели информации, подключаемые к клиентской РС либо к проходным терминалам, необходимым для пропуска сотрудников на территорию организации; – идентификаторы (ключи,	***При использовании «Центр-Т» не потребуются:*** – системы идентификации и аутентификации. *В ПАК «Центр-Т» имеется собственная система идентификации и аутентификации. Также в ПАК «Центр-Т» реализована двусторонняя аутентификация пользователей.* – услуги по обеспечению интеграции решений и оборудования; *Все средства И/А реализованы непосредственно в самом комплексе, соответственно, обеспечение интеграции не требуется.* – считыватели информации, различные идентификаторы;

Меры защиты ИС	Как реализуется с помощью «Центр-Т»	Какие компоненты «Центр-Т» выполняют эти функции	Решения (ПО и оборудование), которые предлагают системные интеграторы для реализации меры защиты	Без каких средств и решений из предыдущего столбца можно обойтись, применяя ПАК «Центр-Т», и почему
	оборудования или реализации каких-либо других методов и решений. См. «Введение» и п.п. 5.2 документа «Руководство по эксплуатации клиентских устройств».		смарт-карты, биометрические данные, одноразовые пароли, PUSH-подтверждения и т.д.), которые взаимодействуют с ОС, приложениями, Active Directory.	*Для идентификации пользователей в ПАК «Центр-Т» не требуется применение дополнительного оборудования – идентификация выполняется по номерам клиентских устройств.*
Управление доступом пользовате-лей	(УПД.1, УПД.2, УПД.4, УПД.5, УПД.11) Управление доступом пользователей (см. п. 1, 3, 4, 5 документа «Руководство по эксплуатации клиентских устройств», п. 1-7 документа «Руководство по эксплуатации СХС3»); (УПД.9) Ограничение параллельных сеансов доступа пользователей (см. п.п. 5.10 документа «Руководство по эксплуатации СХС3»); (УПД.10) Блокировка сеанса доступа в ИС после установленного времени неактивности пользователей (см. п.п. 3.4 документа «Руководство по	– ПО СХС3.	***Принципиальные решения и работы:*** – решения для обеспечения защищенного доступа; – системы управления доступом и аутентификацией пользователей; – защита сетевой инфраструктуры; – системы управления мобильными устройствами; – средства контроля периферийного оборудования (USB-устройства, видеокамеры, микрофоны и т.д.); – выполнение организационных мер, например, – зонирование территории: разбиение ИС на отдельные	***При использовании «Центр-Т» не потребуются:*** – решения для обеспечения защищенного доступа; *ПАК «Центр-Т» обеспечивает защищенное соединение при условии наличия TLS из состава СКАД «Сигнатура-L» или другого средства защиты канала на усмотрение Заказчика.* – системы управления доступом и аутентификацией пользователей; *В ПАК «Центр-Т» управление учетными записями выполняется централизованно на СХС3.* *Управление доступом пользователей реализуется на уровне, который определяется*

Меры защиты ИС	Как реализуется с помощью «Центр-Т»	Какие компоненты «Центр-Т» выполняют эти функции	Решения (ПО и оборудование), которые предлагают системные интеграторы для реализации меры защиты	Без каких средств и решений из предыдущего столбца можно обойтись, применяя ПАК «Центр-Т», и почему
	эксплуатации СХСЗ»); (ЗНИ.2, ЗНИ.5-ЗНИ.7) Управление usb-устройствами (возможность создания образа ПО Клиента с поддержкой usb-устройств или без нее, см. п.п. 6.8 документа «Руководство по эксплуатации СХСЗ»); (ЗИС.5) Управление устройствами вывода и записи звука (поддерживается И/А устройств – мониторов, устройств вывода и записи звука, см. п.п. 4.6 документа «Руководство по эксплуатации СХСЗ»). Для управления доступом пользователей не требуется применение дополнительного оборудования или реализации каких-либо других методов и решений.		сектора (участки); – физическое ограждение территорий зон (участков); – установка пропускных пунктов (КПП); – установка терминалов для И/А пользователей; – обеспечение интеграции предложенных решений и оборудования в ИС. ***Конкретное ПО и оборудование:*** – технологии VPN, SSL/TLS, IPSec и т.д. (АПКШ «Континент», Континент TLS VPN, VipNet Coordinator 4 (в совокупности с VipNet Client, VipNet Administrator, VipNet Policy Manager), UserGate Proxy&Firewall, Forcepoint Next Generation Firewall); – системы управления доступом типа IDM (например, Avanpost IDM, Solar inRights, IBM Security IM); – средства защиты сетевой инфраструктуры и межсетевые экраны (ПАК «Периметр»,	*соответствующими настройками доступа в образе ПО Клиента (ПО РС). Настройки доступа задаются Администратором удаленного управления на этапе сборки образа ПО или его администрирования в соответствии с полномочиями пользователей.* – средства контроля периферийного оборудования; *В ПАК «Центр-Т» возможность управления подключениями USB-носителей: управление учетными: предусмотрена возможность создания образа ПО РС:* *– с возможностью проброса usb-устройств в терминальную сессию;* *– без возможности проброса usb-устройств в терминальную сессию.* – услуги по обеспечению интеграции решений и оборудования; *Все средства управления*

Меры защиты ИС	Как реализуется с помощью «Центр-Т»	Какие компоненты «Центр-Т» выполняют эти функции	Решения (ПО и оборудование), которые предлагают системные интеграторы для реализации меры защиты	Без каких средств и решений из предыдущего столбца можно обойтись, применяя ПАК «Центр-Т», и почему
			RedSeal, Fortinet FortiGate, Palo Alto Networks, UserGate UTM); – средства контроля периферии (Zecurion Zlock, McAfee Devise Control, Ivanti Device Control, Secret Net Studio); – средства управления мобильными устройствами (MobileIron Enterprise Mobility Management, AirWatch Enterprise Mobility Management); – считыватели информации, подключаемые к клиентской РС; – установка КПП, ограждение периметра территории; – электронные замки, терминалы для идентификации пользователей; – идентификаторы (ключи, карты), которые взаимодействуют со считывателями информации; – дополнительные СВТ для хранения информации (серверы баз данных, хранилища данных и т.д.); – системы видеонаблюдения (например, Vocord Traffic,	*доступом в ПАК «Центр-Т» реализованы непосредственно в самом комплексе, обеспечение интеграции не требуется.* – считыватели информации, идентификаторы (ключи, карты); *Для идентификации пользователей в ПАК «Центр-Т» не требуется применение дополнительного оборудования – идентификация выполняется по номерам клиентских устройств.* – дополнительные СВТ для хранения информации (серверы баз данных, хранилища данных и т.д.); *В ПАК «Центр-Т» вся обрабатываемая информация, а также резервные копии хранятся на СХС3.*

Меры защиты ИС	Как реализуется с помощью «Центр-Т»	Какие компоненты «Центр-Т» выполняют эти функции	Решения (ПО и оборудование), которые предлагают системные интеграторы для реализации меры защиты	Без каких средств и решений из предыдущего столбца можно обойтись, применяя ПАК «Центр-Т», и почему
			Ростелеком, Securix, КОДОС GLOBOSS); – дополнительное оборудование (блоки питания, соединительные провода).	
Ограниче-ние программ-ной среды	(ОПС.1) Управление запуском компонентов ПО. (ОПС.2) Управление установкой компонентов ПО. (ОПС.3) Установка только разрешенного к использованию ПО и его компонентов. (См. п.п. 4.5, 4.6, 4.8, 5.8, 5.10, 6.6, 6.9 документа «Руководство по эксплуатации СХС3»). В рамках выполнения ограничения программной среды не требуется применение дополнительного оборудования или реализации каких-либо других методов и решений.	– ПО СХС3 (именно на СХС3 выполняется настройка образов ПО РС); – ПО Клиента (на РС настройки образов ПО исполняются).	***Принципиальные решения и работы:*** – системы управления доступом и аутентификацией; – системы управления рабочими местами пользователей; – выполнение организационных мер, например, – зонирование территории: разбиение ИС на отдельные сектора (участки); – физическое ограничение доступа к отдельным участкам ИС (установка на двери электронных замков, средств идентификации и т.д.); – обеспечение интеграции предложенных решений и оборудования в ИС.	***При использовании «Центр-Т» не потребуются:*** – системы управления доступом и аутентификацией; *Управление доступом пользователей в ПАК «Центр-Т» реализуется посредством установки соответствующих настроек доступа в образе ПО РС. Настройки доступа задаются Администратором удаленного управления на этапе сборки образа ПО или его администрирования в соответствии с полномочиями пользователей.* *Кроме того, в ПАК «Центр-Т» реализован механизм изоляции процессов (за счет использования технологии контейнеризации), что обеспечивает контроль процессов без использования других средств.*

Меры защиты ИС	Как реализуется с помощью «Центр-Т»	Какие компоненты «Центр-Т» выполняют эти функции	Решения (ПО и оборудование), которые предлагают системные интеграторы для реализации меры защиты	Без каких средств и решений из предыдущего столбца можно обойтись, применяя ПАК «Центр-Т», и почему
			Конкретное ПО и оборудование: – системы управления доступом типа IDM (например, Avanpost IDM, Solar inRights, IBM Security IM); – системы управления рабочими местами пользователей (например, Efros Config Inspector, Altiris Client Management Suite, Altiris Server Management Suite, Ivanti Unified Endpoint Manager, Symantec Ghost Solution Suite); – комплексные системы управления IT-инфраструктурой (например, Microsoft System Center Configuration Manager (SCCM), Naumen Service Desk); – дополнительное оборудование (электронные замки, идентификаторы, считыватели).	– системы управления рабочими местами пользователей; *В ПАК «Центр-Т» выполняется централизованное управление образами ПО рабочих станций пользователей. Сборка образов выполняется на СХСЗ, затем образы ПО передаются на рабочие станции посредством удаленного (терминального) соединения.* *ПАК «Центр-Т» позволяет выполнять управление установкой ПО РС: Администратор ИБ СХСЗ определяет компоненты ПО, подлежащие установке, а также настройки параметров установки компонентов.* *В рамках выполнения процедуры сборки образов ПО РС Администратор ИБ СХСЗ может включить в образ ПО, например, только те программы и сервисы, которые, разрешены к использованию на РС (в соответствии с требованиями руководящих документов и политики*

Меры защиты ИС	Как реализуется с помощью «Центр-Т»	Какие компоненты «Центр-Т» выполняют эти функции	Решения (ПО и оборудование), которые предлагают системные интеграторы для реализации меры защиты	Без каких средств и решений из предыдущего столбца можно обойтись, применяя ПАК «Центр-Т», и почему
				безопасности организации). – организационные меры; *При использовании ПАК «Центр-Т» для обеспечения ограничения программной среды применение организационных мер излишне. Все необходимые действия (администрирование ПО РС, сборка образа и т.д.) выполняются администратором ИБ на СХСЗ за счет средств ПО СХСЗ.* – услуги по обеспечению интеграции решений и оборудования; *Все средства ограничения программной среды в ПАК «Центр-Т» реализованы непосредственно в самом комплексе, соответственно, обеспечение интеграции не требуется.* – средства идентификации (идентификаторы, считыватели); *Идентификация*

Меры защиты ИС	Как реализуется с помощью «Центр-Т»	Какие компоненты «Центр-Т» выполняют эти функции	Решения (ПО и оборудование), которые предлагают системные интеграторы для реализации меры защиты	Без каких средств и решений из предыдущего столбца можно обойтись, применяя ПАК «Центр-Т», и почему
				пользователей ПАК «Центр-Т» выполняется по номерам клиентских устройств.
Контроль защищенности данных	(АН3.1) Возможность устранения уязвимостей путем установки обновлений программного обеспечения (см. п.п. 9.2.1 документа «Руководство по эксплуатации СХС3»); (АН3.2) Контроль установки обновлений программного обеспечения комплекса (в том числе и внутреннего ПО носителей комплекса, см. п.п. 9.2.1 документа «Руководство по эксплуатации СХС3»); (АН3.4) Регистрации информации о событиях, связанных с нарушением работоспособности комплекса и параметров настройки ПО и СЗИ (см. п.п. 4.9, 5.11, 6.10, 7.9 документа «Руководство по эксплуатации СХС3», п.п. 4.7	– ПО СХС3; – ПО Клиента.	***Принципиальные решения и работы:*** – системы управления уязвимостями и обновлением ПО (сканеры уязвимостей); – системы управления доступом (системы типа IDM; DLP-системы); – системы управления событиями безопасности; – применение организационных мер, например, – инвентаризация параметров настроек ПО, технических средств, средств защиты информации; – проверка корректности функционирования ПО и обновлений ПО в тестовой среде; – анализ журналов регистрации событий; – обеспечение интеграции	***При использовании «Центр-Т» не потребуются:*** – системы управления доступом и аутентификацией; *Управление доступом пользователей в ПАК «Центр-Т» реализуется посредством установки соответствующих настроек доступа в образе ПО РС. Настройки доступа задаются Администратором удаленного управления на этапе сборки образа ПО или его администрирования в соответствии с полномочиями пользователей.* – системы управления событиями безопасности; *ПАК «Центр-Т» поддерживает возможность регистрации событий. Все события фиксируются в общем журнале и отображаются во вкладке «Журнал событий».* *Общий журнал хранится в БД*

Меры защиты ИС	Как реализуется с помощью «Центр-Т»	Какие компоненты «Центр-Т» выполняют эти функции	Решения (ПО и оборудование), которые предлагают системные интеграторы для реализации меры защиты	Без каких средств и решений из предыдущего столбца можно обойтись, применяя ПАК «Центр-Т», и почему
	«Руководство по эксплуатации клиентских устройств»); (АН3.5) Смена паролей администратора, администратора ИБ, администратора НШР, контролера СХС3 (см. п.п. 3.8, 4.4, 5.4, 6.4, 7.4 документа «Руководство по эксплуатации СХС3», п.п. 4.8 «Руководство по эксплуатации клиентских устройств»); (АН3.5) Создание и удаление пользователей (см. п.п. 4.5.1, 4.5.3, 6.5.1, 6.5.3 документа «Руководство по эксплуатации СХС3»); Контроль защищенности данных обеспечивается за счет средств комплекса «Центр-Т». Введения организационных мер, применения дополнительных технологий и оборудования для		средств защиты в ИС. ***Конкретное ПО и оборудование:*** – сканеры уязвимостей (например, MaxPatrol, Network Attack Discovery, Application Inspector, Xspider); – системы управления доступом типа IDM (например, Avanpost IDM, Solar inRights, IBM Security IM); – DLP-системы (например, Zecurion Zgate, Forcepoint Data Secutity, Solar Dozor, DeviceLock DLP); – системы управления событиями безопасности (например, HP ArcSight Security Intelligence, Micro Focus, agile SI); – системы управления рабочими местами пользователей (например, Efros Config Inspector, Altiris Client Management Suite, Ivanti Unified Endpoint Manager, Symantec Ghost Solution Suite); – дополнительное	*(внутренней или внешней, в зависимости от настроек СХС3) и не перезаписывается при выключении или перезагрузке как СХС3, так и внешней СУБД.* *Администратор БИ клиентского устройства может просматривать записи журнала о локальных событиях безопасности, отображающие действия администраторов и Пользователя клиентского устройства.* – системы управления доступом; *Администраторы удаленного управления ПАК «Центр-Т» могут выполнять процедуру смены собственных паролей, а также управлять (создавать, удалять) учетными записями пользователей.* *Смена паролей администраторов и редактирование учетных записей пользователей выполняется на СХС3 за счет средств комплекса «Центр-Т.»* – услуги по обеспечению интеграции решений и

Меры защиты ИС	Как реализуется с помощью «Центр-Т»	Какие компоненты «Центр-Т» выполняют эти функции	Решения (ПО и оборудование), которые предлагают системные интеграторы для реализации меры защиты	Без каких средств и решений из предыдущего столбца можно обойтись, применяя ПАК «Центр-Т», и почему
	реализации функции не требуется.		оборудование (электронные замки, средства идентификации – терминалы, идентификаторы, считыватели).	оборудования; *Все средства контроля защищенности данных ПАК «Центр-Т» реализованы непосредственно в самом комплексе, соответственно, обеспечение интеграции не требуется.*
Обеспечение доступности данных	(ОДТ.2) Резервное копирование баз данных и настроек СХС3, локальных настроек Клиента (см. п.п. 3.5 документа «Руководство по эксплуатации СХС3», п.п. 4.5 «Руководство по эксплуатации клиентских устройств»); (ОДТ.3) Фиксация событий о неисправностях (сбоях или отказах) в функционировании ПАК «Центр-Т» в журнале событий (см. п.п. 4.9, 5.11, 6.10, 7.9 документа «Руководство по эксплуатации СХС3», п.п. 4.7 «Руководство по эксплуатации клиентских устройств»).	– ПО СХС3.	***Принципиальные решения и работы:*** – системы резервного копирования и восстановления данных; – программно-аппаратные комплексы с возможностью резервного копирования; – системы управления событиями безопасности (SIEM-системы); – обеспечение интеграции средств защиты в ИС. ***Конкретное ПО и оборудование:*** – системы резервного копирования, (например, Symantec Backup Exec, RuBackup, Acronis Защита данных, Veritas	***При использовании «Центр-Т» не потребуются:*** – системы и программно-аппаратные комплексы резервного копирования данных; *В ПАК «Центр-Т» реализована возможность резервного копирования баз данных и настроек СХС3, локальных настроек Клиента.* – системы управления событиями безопасности; *ПАК «Центр-Т» поддерживает возможность регистрации событий. Все события фиксируются в общем журнале и отображаются во вкладке «Журнал событий».*

Меры защиты ИС	Как реализуется с помощью «Центр-Т»	Какие компоненты «Центр-Т» выполняют эти функции	Решения (ПО и оборудование), которые предлагают системные интеграторы для реализации меры защиты	Без каких средств и решений из предыдущего столбца можно обойтись, применяя ПАК «Центр-Т», и почему
	Доступность данных обеспечивается за счет средств ПАК «Центр-Т». Введения организационных мер, применения дополнительных технологий и оборудования для реализации функции не требуется.		NetBackup); – облачные сервисы резервирования и хранения данных (например. Acronis Защита данных, Veeam Backup, Symantec Enterprise Vault); – системы управления событиями безопасности (например, Solar appScreener HP ArcSight Security Intelligence, Micro Focus, agile SI); – программно-аппаратные комплексы возможностью резервного копирования и восстановления данных (например, ПАК «Соболь»).	– услуги по обеспечению интеграции решений и оборудования; *Все средства обеспечения доступности данных ПАК «Центр-Т» реализованы непосредственно в самом комплексе, соответственно, обеспечение интеграции не требуется.*
Обеспечение целостности программ и данных	(ОЦЛ.3) Возможность восстановления баз данных и настроек СХС3, локальных настроек Клиента из резервных копий (см. п.п. 3.5 документа «Руководство по эксплуатации СХС3», п.п. 4.6 «Руководство по эксплуатации клиентских устройств»); (ОЦЛ.1) Контроль	– ПО СХС3; – Специальный носитель ПО «Клиент Центр-Т».	***Принципиальные решения и работы:*** – программно-аппаратные средства, обеспечивающие контроль целостности программ, данных и аппаратных составляющих СВТ; – системы резервного копирования и восстановления данных;	***При использовании «Центр-Т» не потребуются:*** – программно-аппаратные средства контроля целостности; *В ПАК «Центр-Т» реализована возможность контроля целостности образов ПО РС.* – системы и программно-

Меры защиты ИС	Как реализуется с помощью «Центр-Т»	Какие компоненты «Центр-Т» выполняют эти функции	Решения (ПО и оборудование), которые предлагают системные интеграторы для реализации меры защиты	Без каких средств и решений из предыдущего столбца можно обойтись, применяя ПАК «Центр-Т», и почему
	целостности образов ПО РС (см. п.п. «Введение» документа «Руководство по эксплуатации СХСЗ», п.п. «Введение», п.п. 5.3 «Руководство по эксплуатации клиентских устройств»). Обеспечение целостности ОНЗ за счет хранения в защищенном разделе памяти. Обеспечение целостности программ и данных выполняется с помощью средств комплекса «Центр-Т». Введения организационных мер, применения дополнительных технологий и оборудования для реализации функции не требуется.		– программно-аппаратные комплексы с возможностью резервного копирования; – обеспечение интеграции средств защиты в ИС. ***Конкретное ПО и оборудование:*** – системы резервного копирования, (например, Symantec Backup Exec, RuBackup, Acronis Защита данных, Veritas NetBackup); – облачные сервисы резервирования и хранения данных (например. Acronis Защита данных, Veeam Backup, Symantec Enterprise Vault); – программно-аппаратные средства контроля целостности (например, Dallas Lock, ПАК «Соболь», DeviceLock, Secret Net.	аппаратные комплексы резервного копирования данных. *В ПАК «Центр-Т» реализована возможность резервного копирования с последующим восстановлением баз данных и настроек СХСЗ, локальных настроек Клиента.* – услуги по обеспечению интеграции решений и оборудования; *Все средства обеспечения целостности ПАК «Центр-Т» реализованы непосредственно в самом комплексе, соответственно, обеспечение интеграции не требуется.*
Обеспече-ние защиты ИС	(ЗИС.5) Возможность запрета несанкционированной удаленной активации периферийных устройств, в	– ПО СХСЗ; – ПО Клиента (образ начальной	***Принципиальные решения и работы:*** – решения для обеспечения защищенного доступа;	***При использовании «Центр-Т» не потребуются:*** – решения для обеспечения

Меры защиты ИС	Как реализуется с помощью «Центр-Т»	Какие компоненты «Центр-Т» выполняют эти функции	Решения (ПО и оборудование), которые предлагают системные интеграторы для реализации меры защиты	Без каких средств и решений из предыдущего столбца можно обойтись, применяя ПАК «Центр-Т», и почему
	частности, устройств вывода и записи звука (см. п.п. 4.6, 6.8 документа «Руководство по эксплуатации СХСЗ»); (ЗИС.14) Возможность использования бездисковых терминалов (см. п.п. 4.8.1 документа «Руководство по эксплуатации СХСЗ»); (ЗИС.15) Защита данных, не подлежащих изменению (в том числе параметров настройки средств защиты информации и программного обеспечения) (см. п.п. «Введение» документа «Руководство по эксплуатации СХСЗ», п.п. «Введение», п.п. 5.3 «Руководство по эксплуатации клиентских устройств»); (ЗИС.19) Изоляция процессов (см. п.п. 3.7 документа «Руководство по эксплуатации СХСЗ»); (ЗИС.18) Загрузка ПО с неперезаписываемых	загрузки); – Специальный носитель ПО СХСЗ; – Специальный носитель ПО «Клиент Центр-Т».	– защита сетевой инфраструктуры; – системы управления мобильными устройствами; – средства контроля периферийного оборудования (USB-устройства, видеокамеры, микрофоны и т.д.); – системы контроля мобильного кода; – системы предотвращения утечек (DLP-системы); – системы управления доступом и аутентификацией (системы IDM); – антивирусная защита; – применение организационных мер. – обеспечение интеграции средств защиты в ИС. ***Конкретное ПО и оборудование:*** – технологии VPN, SSL/TLS, IPSec и т.д. (АПКШ «Континент», Континент TLS VPN, VipNet Coordinator 4 (в	защищенного доступа; *В ПАК «Центр-Т» реализована концепция ДСС: организация доверенного канала возможна при условии, если образ ПО РС включает средства защиты канала передачи данных – например, поддерживает работу со СКАД «Сигнатура-L» или другим средством защиты канала на усмотрение Заказчика.* – системы управления доступом и аутентификацией; *Управление доступом в ПАК «Центр-Т» реализуется посредством установки соответствующих настроек доступа в образе ПО РС. Настройки доступа задаются Администратором удаленного управления на этапе сборки образа ПО или его администрирования в соответствии с полномочиями пользователей.* *В ПАК «Центр-Т» возможность управления системой разделена между пятью ролями администраторов. Каждый из администраторов выполняет только*

Меры защиты ИС	Как реализуется с помощью «Центр-Т»	Какие компоненты «Центр-Т» выполняют эти функции	Решения (ПО и оборудование), которые предлагают системные интеграторы для реализации меры защиты	Без каких средств и решений из предыдущего столбца можно обойтись, применяя ПАК «Центр-Т», и почему
	машинных носителей (ОНЗ хранятся в памяти, недоступной для перезаписи); (ЗИС.1) Разделение функций по управлению ИС (см. п. 1 документа «Руководство по эксплуатации СХСЗ», п. 1 «Руководство по эксплуатации клиентских устройств»); (ЗИС.4) Возможность обеспечения доверенного канала (при условии наличия в образе начальной загрузки – образа ПО Клиента – средств защиты канала, см. п.п. 4.8.1 документа «Руководство по эксплуатации СХСЗ»). Защита ИС обеспечивается за счет средств комплекса «Центр-Т».		совокупности с VipNet Client, VipNet Administrator, VipNet Policy Manager), UserGate Proxy&Firewall, Forcepoint Next Generation Firewall); – системы управления доступом IDM (например, Avanpost IDM, Solar inRights, IBM Security IM); – средства защиты сетевой инфраструктуры и межсетевые экраны (ПАК «Периметр», RedSeal, Fortinet FortiGate, Palo Alto Networks, UserGate UTM); – средства контроля периферии (Zecurion Zlock, McAfee Devise Control, Ivanti Device Control, Secret Net Studio); – средства управления мобильными устройствами (например, MobileIron Enterprise Mobility Management, AirWatch Enterprise Mobility Management – AirWatch MDM, MAM, MEM, MCM); – системы контроля мобильного кода (например, Solar appScreener, FireEye Mobile Threat	*те функции, которые делегированы ему в рамках должностях обязанностей.* *Контроль процессов обеспечивается за счет наличия механизма изоляции процессов.* – системы контроля подключения периферийного оборудования; *В ПАК «Центр-Т» возможность управления подключениями USB-носителей: управление учетными: предусмотрена возможность создания образа ПО РС:* *– с возможностью проброса usb-устройств в терминальную сессию;* *– без возможности проброса usb-устройств в терминальную сессию.* – услуги по обеспечению интеграции решений и оборудования; *Все средства обеспечения целостности ПАК «Центр-Т» реализованы непосредственно в самом комплексе, соответственно,*

Меры защиты ИС	Как реализуется с помощью «Центр-Т»	Какие компоненты «Центр-Т» выполняют эти функции	Решения (ПО и оборудование), которые предлагают системные интеграторы для реализации меры защиты	Без каких средств и решений из предыдущего столбца можно обойтись, применяя ПАК «Центр-Т», и почему
			Prevention); – DLP-системы (например, Zecurion Zgate, Forcepoint Data Secutity, Solar Dozor, DeviceLock DLP); – антивирусное ПО (например, Secret Net Studio, Kaspersky Security, Kaspersky Business Space Security, Nod32 Business Edition, Dr.Web Enterprise Security Suite).	*обеспечение интеграции не требуется.*

2.3 РАССУЖДЕНИЯ

Для реализации рассматриваемых в разделе 2.1 функций защиты системные интеграторы предлагают многообразие решений.

Несомненно, что многие из предлагаемых решений смогут обеспечить защиту информационной инфраструктуры.

Но до того, как оснастить ИС многочисленными средствами, следует принять во внимание, что применение различных по назначению средств защиты разных производителей сопряжено с некоторыми проблемами. К таким, например, относится проблема стабильности совместного функционирования используемых средств. В большинстве случаев данная проблема связана с тем, что по каким-либо причинам[1] администраторам не удается увязать между собой средства защиты так, чтобы они функционировали корректно и представляли собой единый слаженный механизм защиты.

Чтобы избежать серьезных проблем, связанных с нестабильностью функционирования технических средств, можно, например, прибегнуть к помощи самих же системных интеграторов и заказать им услуги по сопровождению интеграции предлагаемых решений, если таковые предлагаются. Это отдельная статья расходов, да и ввод в эксплуатацию в силу различных причин может существенно затянуться.

Можно ли избежать проблем, связанных с интеграцией средств защиты, каким-либо иным способом? Можно, например, применяя, такие решения, в которых уже заранее реализован комплексный подход к защите ИС, которые обеспечивают выполнение сразу ряда функций защиты. К таким комплексным решениям относится ПАК «Центр-Т» компании ОКБ САПР.

Чтобы показать преимущества ПАК «Центр-Т» перед другими решениями, представленными на рынке, рассмотрим пример типовой информационной системы и сравним, что потребуется применить *вместо ПАК «Центр-Т»*, чтобы в этой ИС был реализован такой же набор мер защиты, что и при использовании «Центр-Т». Иными словами, какими средствами защиты можно «заменить» комплекс «Центр-Т».

Для этого:

1) введем пример типовой ИС, опишем ее состав и схему функционирования;

2) опишем, как можно реализовать защиту данной структуры путем применения ПАК «Центр-Т»;

3) определим, каким образом возможно защитить систему из примера, применив совокупность различных средств защиты, предлагаемых интеграторами, чтобы в рассматриваемой системе был реализован такой же набор мер защиты, как и при применении ПАК «Центр-Т».

---

[1] Средства защиты могут быть сложны в настройке; в ИС могут отсутствовать компоненты, необходимые для настройки средств защиты; персонал может не иметь необходимого опыта или квалификации.

2.3.1 Описание условной типовой информационной системы

Пусть имеется информационная система с клиент-серверной архитектурой (далее по тексту – Система, рисунок 1):

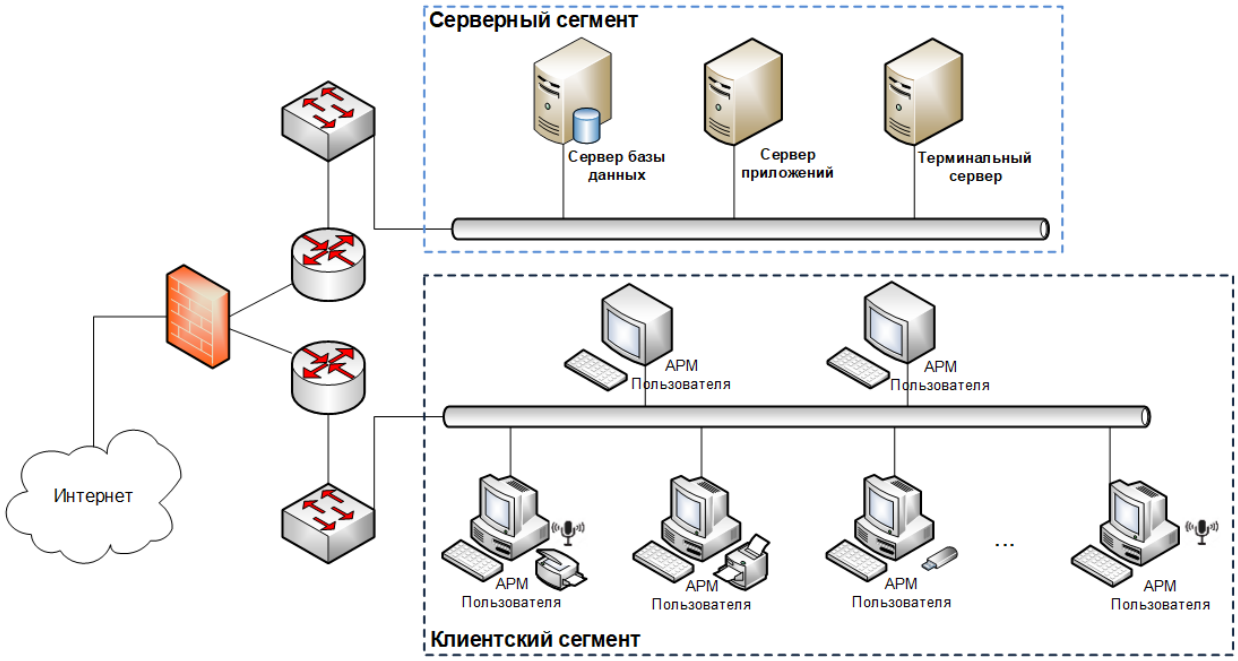

Рисунок 2 – Пример схемы информационной системы

Допустим, в Системе имеется серверный и клиентский сегменты следующего состава:

– ***серверный сегмент:***

1) 1 терминальный сервер, обеспечивающий возможность терминального доступа к серверному сегменту сети со стороны клиентов;

2) 1 сервер базы данных, обеспечивающий хранение и обработку информации, а также ее передачу (загрузку) пользователям по сети;

3) 1 сервер приложений, обеспечивающий среду выполнения для прикладных программ, а также доступ к ним со стороны пользователей;

– ***клиентский сегмент:***

1) 50 клиентских автоматизированных рабочих мест – АРМ, реализующих доступ к программному ПО в терминальном режиме (ПК, терминалы).

Для защиты сетевой инфраструктуры применяется стандартный набор средств фильтрации трафика и сетевой защиты. На границе сетевого периметра установлен межсетевой экран. Информационный обмен обеспечивается посредством маршрутизаторов. Далее посредством коммутаторов доступа информация поступает на серверы и клиентские АРМ.

Допустим, что клиентские АРМ оснащены периферийными устройствами (устройство вывода и записи звука (микрофон), принтер, сканнер и другая периферия, подключаемая к USB-портам). Предусматривается также использование пользователями USB-носителей информации.

2.3.2 Организация защиты Системы путем применения ПАК «Центр-Т»

Теперь рассмотрим, как организовать защиту вычислительной среды приведенной в примере Системы (рисунок 1) с помощью комплекса «Центр-Т».

В рамках применения ПАК «Центр-Т» вводятся ***две дополнительных единицы*** – сервер хранения и сетевой загрузки (СХС3) и автоматизированное рабочее место администратора СХС3 (АРМ Администратора СХС3). Последнее может быть оборудовано из клиентского АРМ, входящего в состав Системы.

Для обеспечения защищенного обмена данными между сегментами сети возможно использование комплекса «Центр-Т» при условии наличия в его составе средств защиты канала (включается по отдельному заказу) или применение других средств защиты канала на усмотрение Заказчика, например, VPN-технологии (в этом случае в периметр серверного сегмента устанавливается VPN-сервер, а VPN-клиенты включаются в образы ПО РС).

Добавленные в Систему компоненты выделены на рисунке оранжевым цветом (рисунок 2).

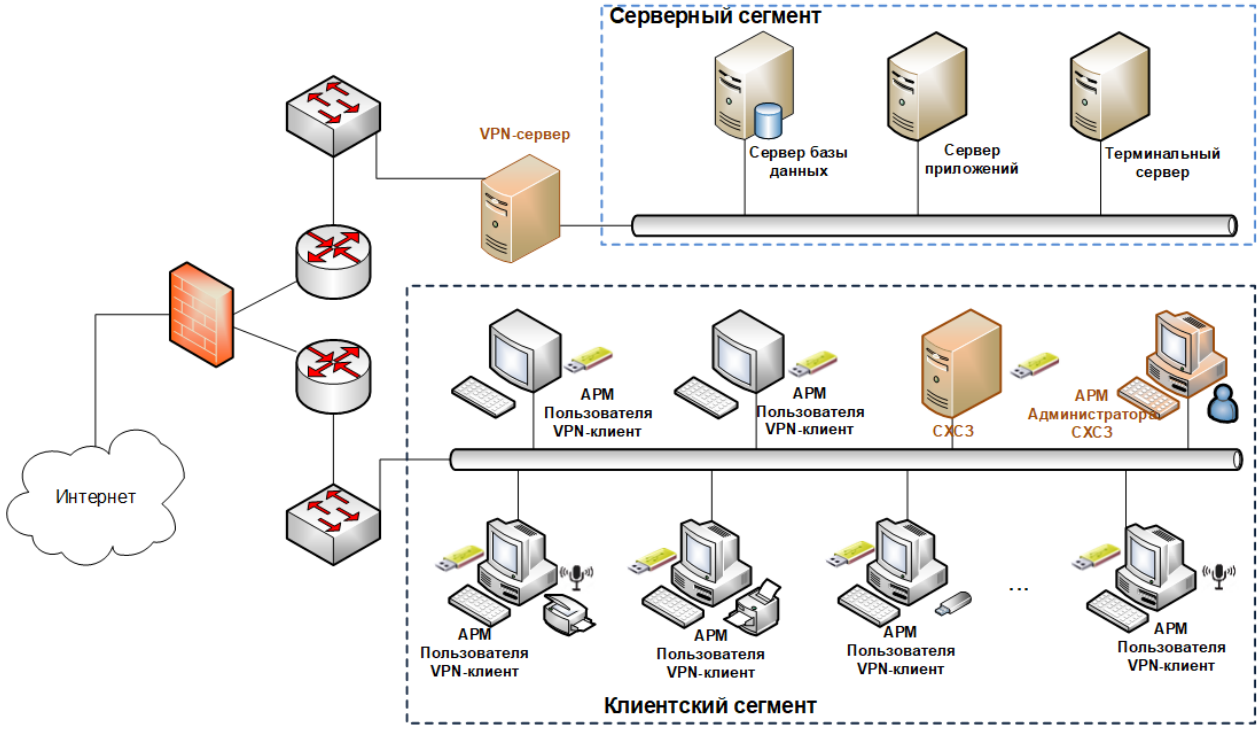

Рисунок 3 – Общий принцип защиты типовой информационной системы с применением ПАК «Центр-Т»

К СВТ (серверу, ПЭВМ или АРМ на базе m-TrusT), которые определены для выполнения функции СХСЗ, подключается специальный носитель ПО СХСЗ из состава ПАК «Центр-Т».

Администраторы из состава персонала ПАК «Центр-Т» после успешных процедур идентификации и аутентификации на выделенном рабочем месте:

- регистрируют учетные записи пользователей;
- назначают им клиентские устройства;
- выполняют сборку образов ПО РС: наполняют образ необходимым (разрешенным) ПО, устанавливают настройки согласно политике безопасности (например, разрешают/запрещают работу с USB-устройствами, устройствами записи и вывода звука), сопоставляют образы ПО РС учетной записи конкретного пользователя.

К каждому клиентскому рабочему месту подключается специальный носитель ПО рабочей станции (ПО РС или клиентское устройство) из состава ПАК «Центр-Т», с которого загружается образ начальной загрузки (ОНЗ). После этого носитель с ПО РС обращается к СХСЗ, загружает необходимый образ ПО РС по сети и проверяет его целостность.

В загрузившейся ОС производится подключение к VPN-серверу (в образ ПО РС включен VPN-клиент), и между сегментами сети устанавливается защищенное соединение.

Далее инициируется соединение клиентского АРМ с ресурсами серверного сегмента.

В результате внедрения в Систему (рисунок 5) ПАК «Центр-Т» получаем гибкую, легко администрируемую ИС, в которой возможно централизованно управлять конфигурациями клиентских АРМ (устанавливать, удалять, обновлять ПО РС), их настройками, передавать образы ПО РС по защищенному туннелю непосредственно на выбранную РС, контролировать установленное ПО РС. Каждый отдельный пользователь получает возможность доступа только к назначенному ему набору ПО. Просмотр и получение доступа к ПО, назначенному другому пользователю, невозможны.

В получившейся ИС исключается:

- несанкционированная модификация конфигурации РС и ее настроек;
- неправомерный доступ незарегистрированных пользователей к приложениям ИС;
- неконтролируемый запуск ПО РС.

2.3.3 Организация защиты Системы путем применения совокупности предлагаемых интеграторами решений

Далее рассмотрим, как защитить Систему (рисунок 1) без применения ПАК «Центр-Т», но с использованием совокупности альтернативных решений. Потребуется применить спектр средств защиты (таблица 1). Среди них:

- система идентификации и аутентификации пользователя;

– система управления рабочими местами;
– система управления доступом и аутентификацией (IDM);
– решение для защищенного доступа;
– средство контроля периферийного оборудования;
– система резервного копирования и восстановления данных;
– средство контроля целостности программ, данных и аппаратных составляющих СВТ.

При установке в Систему (рисунок 1) описанные выше средства защиты, получается (черным цветом выделены исходные компоненты Системы, оранжевым цветом – введенные, рисунок 3):

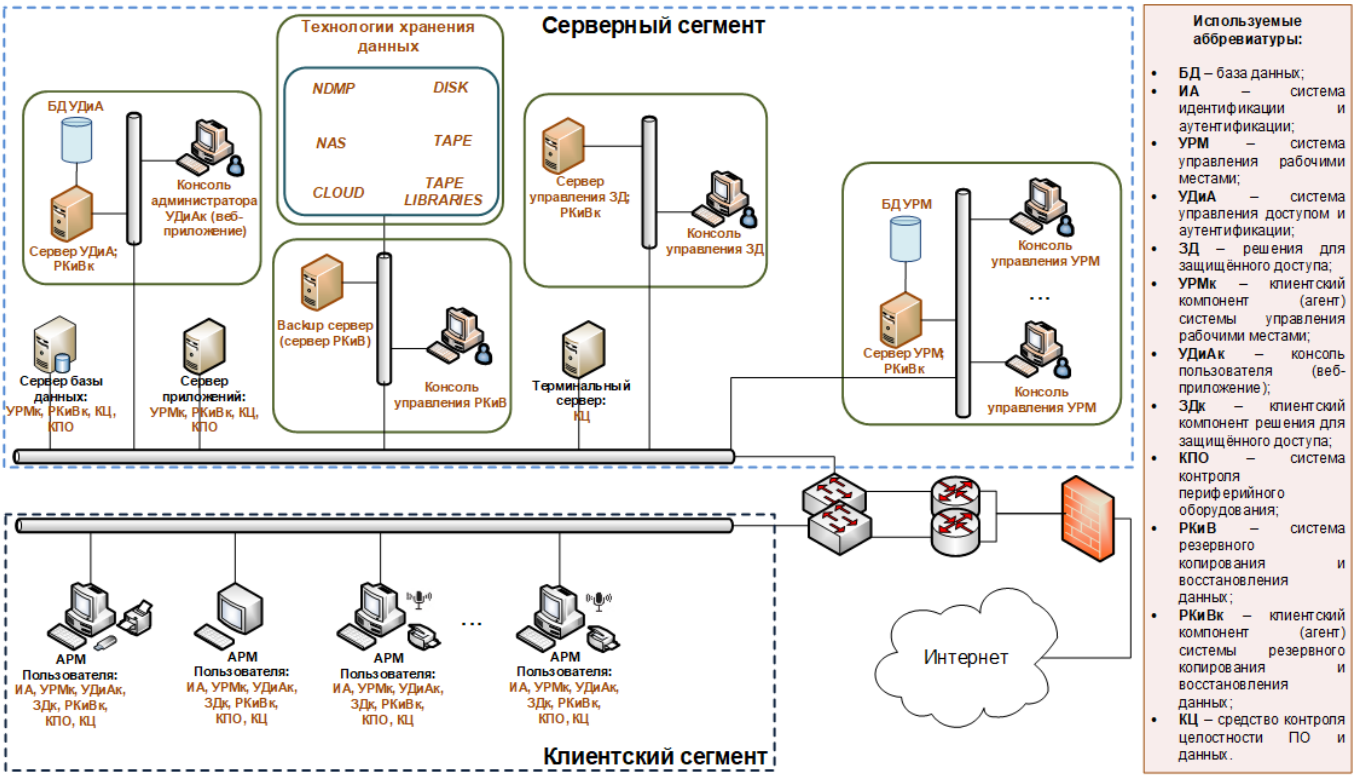

Рисунок 4 – Пример организации защиты типовой информационной системы с применением набора различных решений

В Систему в общем случае вводятся следующие компоненты (рисунок 3):

– сервер и база данных системы управления рабочими местами;
– сервер и база данных системы управления доступом и аутентификацией;
– сервер средства обеспечения защищенного доступа;
– (опционально) система хранения резервных копий данных (СХД): backup-сервер и хранилища данных;
– консоли управления внедренными серверными компонентами систем и средств (в отдельных случаях для управления тем или иным

серверным компонентом может применяться несколько консолей одновременно).

Клиентский компонент системы резервного копирования устанавливается на серверы, содержащие базы данных, на сервер приложений, а также на другие СВТ Системы, резервные копии которых необходимо сохранить.

Управление резервными копиями осуществляется с помощью backup-сервера, хранение копий реализуется в рамках выбранной технологии резервного копирования и восстановления.

Вместо системы централизованного управления резервным копированием и восстановлением могут использоваться другие средства, например, программно-аппаратные комплексы с возможностью резервного копирования и восстановления данных. В этом случае данные комплексы устанавливаются на каждое из СВТ, резервные копии которых требуется сохранить.

В случае применения «Центр-Т» в использовании систем резервного копирования нет необходимости. С помощью ПО «Центр-Т», в отличие от совокупности различных решений, возможно создание резервных копий баз данных и настроек сервера хранения и загрузки (СХС3) непосредственно на СХС3 и локальных настроек клиентских рабочих станций непосредственно на станциях, и применение дополнительных средств резервного копирования излишне.

Клиентский компонент системы управления рабочими местами устанавливается на СВТ Системы, конфигурацию которых необходимо контролировать, а также состав установленного ПО и сетевое оборудование. Контроль оборудования, инвентаризация и управление рабочими местами выполняется посредством специальной консоли (возможно использование нескольких консолей одновременно – в зависимости от количества групп персонала).

Этого бы не понадобилось при внедрении в Систему ПАК «Центр-Т», применение которого не требует использование дополнительных консолей управления и установки дополнительных клиентских компонентов в рамках управления клиентскими рабочими местами.

В рамках управления доступом применяется система централизованного управления правами доступа к данным, учетным записями и паролями (IDM).

Доступ к информационным ресурсам, использующимся в организации, осуществляется посредством специальных служб (коннекторов).

Для получения доступа к ресурсам на каждое из клиентских АРМ устанавливаются специальные консоли (веб-приложения).

Управление настройками доступа, параметрами учетных записей и паролями осуществляется с помощью консоли администратора (веб-приложения).

В отличие от совокупности решений, предлагаемых интеграторами, при использовании ПАК «Центр-Т» не потребуется применять дополнительные средства управления доступом. Комплекс «Центр-Т» контролирует доступ пользователей на основании данных о номерах клиентских устройств, сопоставленных учётным записям пользователей, а также о назначенных образах ПО РС: после загрузки ОНЗ на Клиенте на СХСЗ отправляется запрос на получение образа и шаблона настроек. СХСЗ определяет, какой образ и шаблон назначены пользователю, соответствующему указанному в запросе номеру клиентского устройства, и отправляет в ответ Клиенту имя образа и его настройки.

Для защищенного доступа внутри системы и извне используется средство обеспечения защищенного доступа (например, VPN), клиентская часть которого устанавливается на каждое из рабочих мест пользователей.

Помимо этого, на клиентские АРМ Системы устанавливаются системы идентификации и аутентификации, средства контроля периферийного оборудования и контроля целостности программ и данных.

Этого бы не потребовалось при применении ПАК «Центр-Т», так как:

а) в комплексе «Центр-Т» идентификация пользователей выполняется по номерам клиентских устройств – участия пользователей в этом процессе не требуется;

б) «Центр-Т» позволяет контролировать периферийное оборудование – предусмотрена возможность контроля подключения устройств вывода и записи звука, а также контроля подключения usb-устройств;

в) «Центр-Т» контролирует целостность образов ПО РС, а соответственно, и всех программ, настроек и данных, содержащихся в данных образах.

2.3.4 Выводы

При организации защиты с использованием совокупности различных решений Система получается довольно громоздкой и сложной в администрировании и управлении.

В отличии от ПАК «Центр-Т», при применении которого архитектура исходной Системы практически не меняется (рисунок 2), внедрение совокупности решений, предлагаемых интеграторами, меняет систему кардинально (рисунок 3): вводятся новые единицы технических средств, внедряется немалое количество нового ПО.

Расширение периметра Системы в результате увеличения числа программных компонентов и оборудования способствует росту нагрузки на сеть и на систему в целом, что приводит к значительному увеличению потребления энергии.

Нагрузка на сеть, в свою очередь, может привести к нехватке мощности, в связи с чем возможно возникновение перебоев в работе Системы, а также вероятный выход из строя какого-либо из компонентов.

Помимо этого, различные средства защиты различных производителей, как правило, никак между собой не связаны. Поэтому прежде, чем Система с рисунка 3 начнет функционировать корректно и стабильно, необходимо будет провести пуско-наладочные мероприятия. Порой, такие действия довольно продолжительны по времени, что может существенно «затянуть» запуск всей инфраструктуры Системы. Действия по «увязке» средств защиты и по их интеграции в ИС потребуют привлечения квалифицированных работников, имеющих опыт в данной сфере деятельности – вероятно, потребуется заказать услуги по сопровождению интеграции предлагаемых решений.

Теперь коснемся непосредственно категорий предлагаемого ПО.

Большинство из рассматриваемых в пункте 2.3.3 решений относятся к числу приложений централизованного управления (к ним относятся системы управления рабочими местами, системы типа IDM, а также решения для защищенного доступа и системы резервного копирования). Для корректной работы таких приложений необходимо наличие лицензии для серверного компонента, а также для каждого из клиентских рабочих мест (в случае с системами типа IDM – для каждого активного пользователя). Чем больше рабочих станций – тем больше стоимость комплекта ПО. В крупных организациях с большим количеством рабочих мест стоимость лицензирования может быть весьма существенной.

Что касается других средств защиты, установленных в Системе (комплексы контроля целостности или резервного копирования) – помимо непосредственно необходимых функций данные комплексы имеют много других функций, которые могут и вовсе не понадобиться. К слову, лицензии приобретаются на каждое отдельное средство.

Стоит также упомянуть, что различные решения могут иметь схожие функции. В некоторых системах управления рабочими местами есть функция контроля целостности конфигураций программного обеспечения. Средства контроля целостности также контролируют целостность (программ, данных и аппаратных составляющих СВТ). Применение двух категорий решений в одной ИС с наличием двух и более похожих возможностей представляется избыточным. Это просто нецелесообразно.

Еще пример – среди функций некоторых из систем управления рабочими местами имеется возможность восстановления ПО в случае сбоев. Если же в Системе установлена полноценная СХД с backup-сервером и хранилищами данных, то необходимость резервирования конфигураций и наборов ПО со стороны системы управления рабочими станциями также избыточна.

Приведем примерную стоимость некоторых категорий решений. В таблице 2 указаны цены, установленные в открытых прайс-листах на сайтах поставщиков решений или рассчитанные с помощью специальных он-лайн калькуляторов, которые также представлены на сайтах производителей.

Таблица 2 – Примеры решений, при применении которых в ИС реализуется такой же набор мер защиты, что и при использовании комплекса «Центр-Т»

Категория решений	Наименование решений	Примерная стоимость
Системы идентификации и аутентификации	Multifactor	цена предоставляется по запросу
	Avanpost FAM	цена предоставляется по запросу
	Cisco Duo	цена предоставляется по запросу
	Biolink	цена предоставляется по запросу
Системы управления рабочими местами	Altiris Client Management Suite	7 205 рублей (1 лицензия) при покупке от 1 до 50 лицензий
	Altiris Server Management Suite	31 282 (1 лицензия) при покупке от 1 до 50 лицензий
	Efros Config Inspector	цена предоставляется по запросу
	Ivanti Unified Endpoint Manager	цена предоставляется по запросу
	Symantec Ghost Solution Suite	2 739 рублей (1 лицензия) при покупке от 1 до 50 лицензий
Системы управления доступом	Avanpost IDM	цена предоставляется по запросу
	Solar inRights	цена предоставляется по запросу Примечание – продукт Solar inRights лицензируется по числу лиц, правами доступа которых требуется управлять.
	IBM Security IM	цена предоставляется по запросу
Решения для защищенного доступа	АПКШ «Континент» 3.9 (в вариации – центр управления сетью с сервером доступа)	от 174 682 рублей (цена за 1 комплект; тип технической поддержки – базовая)
	АПКШ «Континент» 4 (в вариации – Узел безопасности)	от 419 500 рублей (цена за 1 комплект; тип технической поддержки – базовая)
	АПКШ «Континент» 4 (в вариации – UTM)	от 459 500 рублей (цена за 1 комплект; тип технической поддержки – базовая)
	Континент TLS VPN	от 581 833 рублей (цена за 1 комплект; тип

		технической поддержки – базовая)
	UserGate Proxy&Firewall	цена предоставляется по запросу
	Forcepoint Next Generation Firewall	цена предоставляется по запросу
	VipNet Coordinator HW 4	от 65 500 рублей (цена за 1 комплект; тип технической поддержки – базовая)
	VipNet Client	7 010 рублей (цена за 1 комплект; тип технической поддержки – базовая) при покупке от 21 до 50 лицензий
	VipNet Administrator	от 77 880 рублей (цена за 1 комплект; тип технической поддержки – базовая)
	VipNet Policy Manager	от 80 000 рублей (цена за 1 комплект; тип технической поддержки – базовая)
Средства контроля периферийного оборудования	Zecurion Zlock	цена предоставляется по запросу
	McAfee Devise Control	цена предоставляется по запросу
	Ivanti Device Control	цена предоставляется по запросу
	Secret Net Studio	6 635-11 195 рублей (1 годовая лицензия)
Комплексы резервного копирования и восстановления данных	ПАК «Соболь»	13 725-22 758 рублей (цена за 1 комплект)
Системы резервного копирования и восстановления данных	Symantec Backup Exec	цена предоставляется по запросу
	RuBackup	цена предоставляется по запросу
	Acronis Защита данных (для физического сервера)	от 49 007 рублей
	Acronis Защита данных (для рабочей станции)	от 5 459 рублей
	Acronis Защита данных (для платформы виртуализации)	от 61 998 рублей
	Veritas NetBackup	цена предоставляется по запросу
Облачные сервисы хранения данных	Acronis Защита данных (облако)	цена предоставляется по запросу
	Veeam Backup	цена предоставляется по запросу

	Symantec Enterprise Vault	цена предоставляется по запросу
Программно-аппаратные средства, обеспечивающие контроль целостности программ, данных и аппаратных составляющих СВТ	ПАК «Соболь»	13 725-22 758 рублей (цена за 1 комплект)
	DallasLock	цена предоставляется по запросу
	DeviceLock	цена предоставляется по запросу
	Secret Net LSP	от 3 875 рублей (цена за 1 комплект с годовой лицензией)

Попробуем рассчитать примерную стоимость сборки (с учетом того, что для большинства решений цены предоставляются только по запросу КП, задача эта может быть решена только частично). Предположим, что в Системе будут установлены следующие средства защиты:

- Altiris Client Management Suite; (системы управления пользовательскими рабочими местами и серверами; обозначение – УРМк);
- Altiris Server Management Suite (система управления серверами; обозначение – УС);
- Континент TLS VPN (решение для защищенного доступа – сервер; обозначение – ЗД);
- Континент TLS VPN Клиент (решение для защищенного доступа – клиент; обозначение – ЗДк);
- Secret Net Studio (средство контроля периферийного оборудования; обозначение – КПО);
- ПАК «Соболь» в исполнении 2[1)] (комплекс резервного копирования и контроля целостности; обозначение – РКиВ, КЦ).

Техника лицензирования этих средств такова:

- для системы управления рабочими местами лицензии приобретаются на каждое их клиентских АРМ и других СВТ, конфигурациями и настройками которых требуется управлять (*в примере Системы (рисунок 3) это 2 серверных СВТ и 50 клиентских*);
- цена решения для защищенного доступа состоит из стоимости лицензии серверного компонента и стоимости лицензии клиентского компонента, умноженной на количество клиентских АРМ Системы (*в примере Системы (рисунок 3) 50 клиентских АРМ*). Также вероятно, что в Системе также придется использовать средства централизованного управления решением, а это означает, что к получившейся стоимости лицензирования серверного и клиентских компонентов нужно прибавить стоимость средств ЗДц;

[1)] При применении Континент TLS VPN в качестве дополнительного оборудования необходимо использовать ПАК «Соболь» в исполнении 2.

– комплекс резервного копирования и контроля целостности устанавливается на те СВТ, целостность данных и аппаратуры которых необходимо контролировать, а также сохранять их резервные копии; лицензии приобретаются на каждое из СВТ (*в примере Системы (рисунок 3) это 6 серверных СВТ и 50 клиентских*);
– средство контроля периферийного оборудования устанавливается на клиентские АРМ, соответственно, лицензии приобретаются на каждое из АРМ (*в примере Системы (рисунок 3) это 2 серверных СВТ и 50 клиентских*).

Итак, общая стоимость сборки решений для Системы складывается из стоимости отдельных решений, лицензии для которых приобретаются как для серверных СВТ, так и для клиентских:

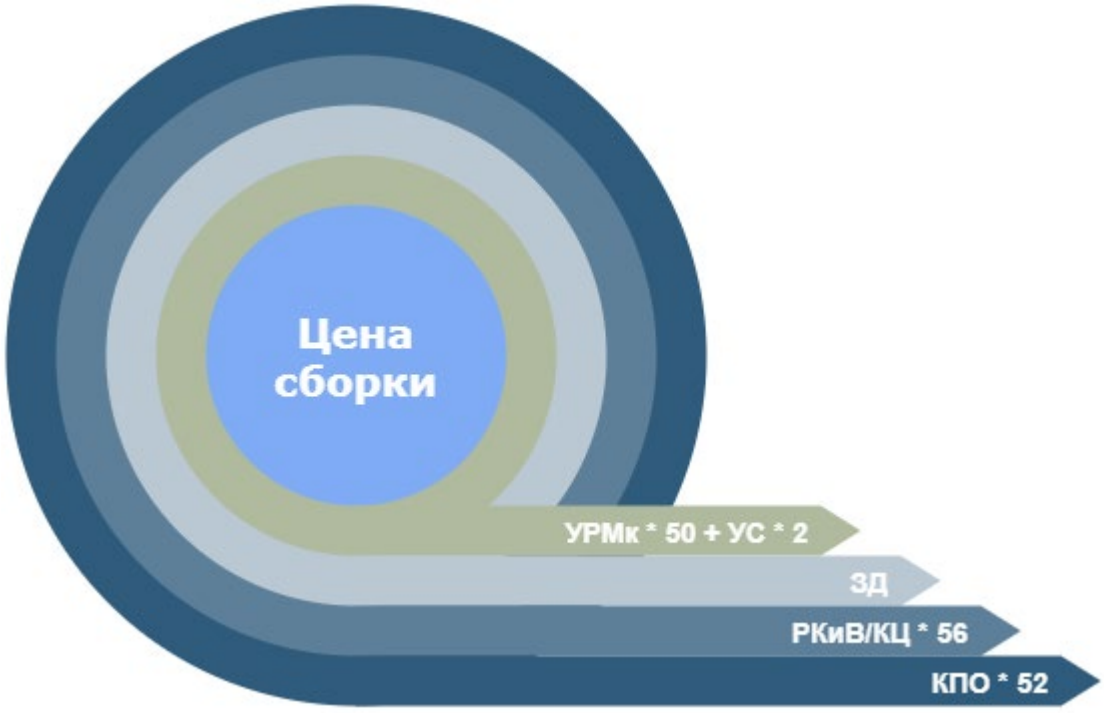

Рисунок 5 – Принцип расчета стоимости сборки решений для Системы

При подсчете даже для описанной системы совсем небольшого масштаба получается довольно значительная сумма – около 2,5 млн рублей[1)], а комплект из ПАК «Центр-Т» и СЗИ НСД для серверной группы той же системы стоит менее 1 млн рублей. Более подробно о стоимости ПАК «Центр-Т» можно узнать, написав по адресу zakaz@okbsapr.ru.

Итак, применение «Центр-Т» позволит осуществить не только рациональный, но и выгодный подход к организации защиты ИС.

Очевидным преимуществом ПАК «Центр-Т» перед совокупностью отдельных решений, предлагаемых интеграторами, является то, что «Центр-Т»,

[1)] В получившейся сумме отсутствуют цены на отдельные продукты. Стоит учитывать, что при сложении цен на все продукты из примера Системы (рисунок 3), итоговая сумма будет значительно больше.

являясь комплексным решением, позволяет организовать многостороннюю защиту ИС за счет следующих особенностей.

1. ***Наличие собственной системы идентификации и аутентификации.***

Преимущество данной системы заключается в том, что идентификация пользователей выполняется *без участия самих пользователей.* С клиентского устройства стартует ПО Клиента и отправляет запрос на СХСЗ с указанием своего серийного номера. СХСЗ сравнивает полученный номер с номерами назначенных пользователям «Центр-Т» устройств. Если СХСЗ определяет, что клиентские устройства сопоставлены учетным записям пользователей, то отправляет на Клиент данные о назначенных ему образе ПО РС и шаблоне настройках – процедура идентификации завершена успешно. Такой метод идентификации исключает действие «человеческого» фактора: не произойдет блокировки действий пользователя в случае, например, ввода некорректных данных. Идентификация выполняется прозрачно для пользователей, не требуя выполнения дополнительных действий.

2. ***Возможность организации доверенного сеанса связи (ДСС) (при условии наличия в составе загружаемого образа средства защиты канала на усмотрение Заказчика).***

Принципиальное отличие режима загрузки с помощью «Центр-Т» от ДСС состоит только в одном – в организации защищенного канала передачи данных, которая в состав основных функций Центр-Т не входит. Это связано с тем, что «Центр-Т» предполагается размещение СХСЗ и клиентов в рамках одной контролируемой зоны. Однако организация ДСС посредством ПАК «Центр-Т» возможна, если при заказе сообщить о необходимости включить в состав ПО средства защиты канала. Администратор ИБ при сборке или администрирования образов ПО РС будет добавлять в состав образов средства защиты каналов связи (например, VPN-клиенты).

Во всех остальных аспектах работа с «Центром-Т» полностью соответствует концепции доверенного сеанса связи.

3. ***Централизованное управление и администрирование ПО РС.***

ПАК «Центр-Т» позволяет:

- централизованно управлять конфигурацией ПО РС;
- удаленно развертывать рабочие места;
- обеспечивать восстановление ПО РС при нештатных ситуациях;
- резервировать баз данных и настроек компонентов ПО;
- создавать шаблоны настроек образов ПО РС и перемещать их на РС;
- контролировать целостность образов ПО РС.
- контролировать перечень компонентов ПО РС.

В ПАК «Центр-Т» реализован разумный подход к управлению ПО РС: образы собираются на СХСЗ администратором ИБ. То есть образы создаются с учетом потребностей, специфичных для эксплуатирующей

организации и даже вплоть до отдельных рабочих мест, и могут меняться оперативно по мере возникновения необходимости, но в то же время работа ведется на одном рабочем месте и не затрачивается время на доставку обновлений. Для получения актуального образа пользователю достаточно просто загрузить терминал.

Сборка допускается только из проверенных компонентов ПО, разрешенных администратором ИБ в соответствии с политикой безопасности.

Каждый образ сопоставляется конкретному зарегистрированному пользователю, для которого назначено конкретное клиентское устройство. С клиентского устройства может быть запущено только один набор ПО, недоступный другим пользователям системы.

Кроме того, ПАК «Центр-Т» позволяет управлять съемными носителями информации (разрешать или запрещать их проброс в терминальную сессию).

Путем применения комплекса полностью исключаются:

- возможность получения доступа к ПО со стороны незарегистрированных пользователей;
- возможность получения доступа к запрещенным сетевым ресурсам;
- несанкционированное копирование и перенос информации на съемных носителях;
- возможность несанкционированной установки пользователями неразрешенного ПО.

4. Резервирование и восстановление данных.

В ПАК «Центр-Т» реализована возможность резервного копирования баз данных и настроек СХСЗ, локальных настроек Клиента. Резервирование внутренней базы данных и настроек СХСЗ выполняется путем экспорта на носитель информации. Восстановление базы данных и настроек СХСЗ из резервной копии выполняется путем импорта файла резервной базы данных и настроек с носителя информации на СХСЗ.

Возможность создания резервной копии баз данных и настроек обеспечивает восстановление ПО «Центр-Т» в случае сбоев в системе защиты информации, тем самым, обеспечивая доступность технических средств, что важно, так как наличие резервной копии – это и исключение сброса (потери) настроек, и минимальное время на восстановление работоспособности всей ИС.

Для обеспечения функционирования ПАК «Центр-Т» не требуются отдельные системы его резервирования – для хранения резервных копий комплекса достаточно иметь под рукой свободный USB-накопитель – копию можно сохранить на флешку. Это удобно, просто, эргономично.

5. Контроль целостности ПО.

ПАК «Центр-Т» обеспечивает контроль целостности образов ПО РС. При скачивании образа клиентским устройством производится проверка его

целостности и аутентичности; если проверка образа завершается успешно, то он загружается в оперативную память СВТ, и ему передается дальнейшее управление ресурсами компьютера.

6. Контроль периферийного оборудования.

Комплекс «Центр-Т» поддерживает управление периферийными устройствами, что дает возможность, в частности, запрета несанкционированной удаленной активации устройств вывода и записи звука. Помимо этого, в комплексе предусмотрена возможность контроля подключения usb-устройств в рамках терминальной сессии.

7. Дополнительных возможностей комплекса.

Кроме вышесказанного (пункты 1-6), «Центр-Т» обеспечивает:

- организацию удаленного доступа за счет наличия встроенных средств терминального доступа (Citrix ICA);
- протоколирование событий безопасности, которые связаны с функциональными возможностями комплекса (процедуры идентификации и аутентификации, копирование лицензий, сборка образа ПО РС, создание и редактирование учетных записей пользователей и т.д.).
- загрузку ПО с защищенных носителей: ПО СХС3 и ПО Клиента (образ начальной загрузки) хранятся в защищенных разделах памяти специальных носителей, что исключает возможность несанкционированного изменения ПО «Центр-Т» (внесения вредоносного или удаления подлинного ПО).

Подводя итог, можно сказать, что:

во-первых, «Центр-Т» – это более разумное и выгодное решение, нежели использование нескольких других средств одновременно, так как

1. комплекс сочетает в себе не только целевые функции, но и функции управления ИС в целом;
2. механизмы защиты реализуются за счет средств самого комплекса – введения организационных мер, применения дополнительных технологий и оборудования для реализации функций не требуется.

Чтобы в Системе был реализован такой же набор мер защиты, что и при использовании комплекса «Центр-Т», потребуется применить совокупность различных решений:

- система управления рабочими местами;
- система управления доступом и аутентификацией (IDM);
- решение для защищенного доступа;
- средство контроля периферийного оборудования;
- система резервного копирования и восстановления данных;

– средство защиты, обеспечивающее контроль целостности программ, данных и аппаратных составляющих СВТ.

во-вторых, «Центр-Т» – удобное и простое решение – комплекс не сложен в настройке, удобен и прозрачен в эксплуатации, не требует от пользователей совершения множества сложных действий;

в-третьих, «Центр-Т» – экономичное решение – применяя комплекс, заметно сокращаются расходы на обслуживание и администрирование информационной системы;

в-четвертых, «Центр-Т» – рациональное решение, так как при относительно невысокой стоимости не только обеспечивает надежную защиту ИС, но делает ее управляемой, более простой в обслуживании и эксплуатации.

3 АНАЛИЗ МЕР 17-ГО И 21-ГО ПРИКАЗОВ ФСТЭК ПО ЗАЩИТЕ ИНФОРМАЦИИ, РЕАЛИЗУЕМЫХ В ИС ПУТЕМ ПРИМЕНЕНИЯ ПАК «ЦЕНТР-Т»

3.1 МЕРЫ, РЕАЛИЗУЕМЫЕ С ПОМОЩЬЮ ПАК «ЦЕНТР-Т»

В таблице 3 представлены меры 17-го и 21-го Приказов ФСТЭК по защите информации в информационной системе, входящих в базовый набор мер и реализуемых путем применения ПАК «Центр-Т».

Таблица 3 - Меры, определенные 17-ым и 21-ым приказами ФСТЭК России, входящие в базовый набор мер и реализуемые путем применения ПАК СЗИ НСД «Центр-Т»

№	Усл. обозн.	Меры обеспечения безопасности	Выполнение входящих в базовый набор мер 17 и 21 приказов ФСТЭК	Ссылки на документацию
Идентификация и аутентификация субъектов и объектов доступа (ИАФ)				
1	ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	+	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».
2	ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных	+	1. см. п.п. 4.6 документа «Руководство по эксплуатации СХСЗ».
3	ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	+	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	+	

№	Усл. обозн.	Меры обеспечения безопасности	Выполнение входящих в базовый набор мер 17 и 21 приказов ФСТЭК	Ссылки на документацию
		принятие мер в случае утраты и (или) компрометации средств аутентификации		
5	ИАФ.5	Защита обратной связи при вводе аутентификационной информации	+	1. см. п.п. 4.3, документа «Руководство по эксплуатации СХС3».
Управление доступом субъектов доступа к объектам доступа (УПД)				
6	УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	+	1. см. п.п. 4.5.1 документа «Руководство по эксплуатации СХС3».
7	УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	+	1. см. п. 1 документа «Руководство по эксплуатации СХС3»; 2. см. п. 1 документа «Руководство по эксплуатации клиентских устройств».
8	УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	+	1. см. п. 1, 2 документа «Руководство по эксплуатации СХС3»; 2. см. п. 1 документа «Руководство по эксплуатации клиентских устройств».
9	УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам,		

№	Усл. обозн.	Меры обеспечения безопасности	Выполнение входящих в базовый набор мер 17 и 21 приказов ФСТЭК	Ссылки на документацию
		обеспечивающим функционирование информационной системы		
10	УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)[1]	+ Ограничение попыток доступа к ИС в рамках управления доступом регулируется СЗИ НСД серверной группы, например, СЗИ НСД «Аккорд-Win64 K» (TSE), установленном на СХС3.	1. см. п.п. 7.3 документа «Установка правил разграничения доступа. Программа ACED32».
11	УПД.9	Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы	+	1. см. п.п. 5.10 документа «Руководство по эксплуатации СХС3».
12	УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу	+	1. см. п.п. 3.4, 4.6 документа «Руководство по эксплуатации СХС3».
13	УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации	+	1. см. п.п. 3.2, 4.3, 5.3, 6.3, 7.3 документа «Руководство по эксплуатации СХС3»; 2. см. п.п. 3.3, 4.2, 5.2 документа «Руководство по эксплуатации клиентских устройств».
14	УПД.13	Реализация защищенного удаленного доступа	+	1. см. Приложение 2 документа «Руководство по эксплуатации СХС3».

№	Усл. обозн.	Меры обеспечения безопасности	Выполнение входящих в базовый набор мер 17 и 21 приказов ФСТЭК	Ссылки на документацию
		субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные связи		
15	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».
16	УПД.17	Обеспечение доверенной загрузки средств вычислительной техники	+ 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)				
17	ОПС.1	Управление запуском (обращениями)	+	1. см. п.п. 4.6, 4.8, 5.5, 5.8, 5.10 документа

№	Усл. обозн.	Меры обеспечения безопасности	Выполнение входящих в базовый набор мер 17 и 21 приказов ФСТЭК	Ссылки на документацию
		компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения		«Руководство по эксплуатации СХСЗ».
18	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	+	
19	ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов		
Защита машинных носителей персональных данных (ЗНИ)				
20	ЗНИ.2	Управление доступом к машинным носителям персональных данных	+	1. см. п.п. 5.5 документа «Руководство по эксплуатации СХСЗ»;
21	ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители персональных данных	+	2. см. п.п. 5.3 документа «Руководство по эксплуатации клиентских устройств».
Регистрация событий безопасности (РСБ)				
22	РСБ.1	Определение событий безопасности,	+	1. см. п.п. 3.9, 4.9. 5.11, 6.10, 7.9 документа «Руководство

№	Усл. обозн.	Меры обеспечения безопасности	Выполнение входящих в базовый набор мер 17 и 21 приказов ФСТЭК	Ссылки на документацию
		подлежащих регистрации, и сроков их хранения		по эксплуатации СХСЗ»; 2. см. п.п. 4.7 документа «Руководство по эксплуатации клиентских устройств».
23	РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации		
24	РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	+	
25	РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них	+	
26	РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе	+	
27	РСБ.7	Защита информации о событиях безопасности	+	
Контроль (анализ) защищенности персональных данных (АН3)				
28	АН3.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей	+	1. см. Приложение 2 документа «Руководство по эксплуатации СХСЗ».
29	АН3.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	+	

№	Усл. обозн.	Меры обеспечения безопасности	Выполнение входящих в базовый набор мер 17 и 21 приказов ФСТЭК	Ссылки на документацию
30	АН3.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации	+	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 устройств».
31	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».
32	АН3.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе	+	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)				
33	ОЦЛ.1	Контроль целостности программного	+	1. см. п. «Введение» «Руководство по

№	Усл. обозн.	Меры обеспечения безопасности	Выполнение входящих в базовый набор мер 17 и 21 приказов ФСТЭК	Ссылки на документацию
		обеспечения, включая программное обеспечение средств защиты информации		эксплуатации СХСЗ»; 2. см. п.п. 5.3 документа «Руководство по эксплуатации клиентских устройств».
34	ОЦЛ.3	Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций	+	1. см. п.п. 3.5 документа «Руководство по эксплуатации СХСЗ»; 2. см. п.п. 4.6 документа «Руководство по эксплуатации клиентских устройств».
35	ОЦЛ.6	Ограничение прав пользователей по вводу информации в информационную систему	+	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)				
36	ОДТ.2	Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы	+	1. см. п.п. 3.5 документа «Руководство по эксплуатации СХСЗ»; 1. см. п.п. 4.5 документа «Руководство по эксплуатации клиентских устройств».
37	ОДТ.3	Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование	+ Контроль безотказного функционировани я технических средств, обнаружение и локализация отказов функционировани	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.	Меры обеспечения безопасности	Выполнение входящих в базовый набор мер 17 и 21 приказов ФСТЭК	Ссылки на документацию
			я, принятие мер по восстановлению отказавших средств обеспечивается проверкой подлинности ПО РС при передаче на клиентское устройство и возможностью восстановления баз данных СХСЗ и клиентов в случае отказов в работе. В случае если проверка подлинности прошла неуспешно, то на экране Клиента появится соответствующее сообщение.	
Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)				
38	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	+	1. см. п. 1 документа «Руководство по эксплуатации СХСЗ»; 2. см. п. 1 документа «Руководство по эксплуатации клиентских устройств».
39	ЗИС.5	Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных	+	1. см. п.п. 4.6, 5.5 документа «Руководство по эксплуатации СХСЗ»; 2. см. п.п. 5.3 документа «Руководство по

№	Усл. обозн.	Меры обеспечения безопасности	Выполнение входящих в базовый набор мер 17 и 21 приказов ФСТЭК	Ссылки на документацию
		периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств		эксплуатации клиентских устройств».
40	ЗИС.11	Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов	+ 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».
41	ЗИС.15	Защита архивных	+	1. см. п.п. 3.7, документа

№	Усл. обозн.	Меры обеспечения безопасности	Выполнение входящих в базовый набор мер 17 и 21 приказов ФСТЭК	Ссылки на документацию
		файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки персональных данных		«Руководство по эксплуатации СХСЗ»; 2. см. п.п. 5.3 документа «Руководство по эксплуатации клиентских устройств».
42	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	+	1. см. п.п. 4.8, 5.10 документа «Руководство по эксплуатации СХСЗ».
43	ЗИС.22	Защита информационной системы от угроз безопасности информации, направленных на отказ в обслуживании информационной системы	+ 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)				
44	ИНЦ.2	Обнаружение, идентификация и регистрация инцидентов	+	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 информационной системы и системы защиты персональных данных (УКФ)				
45	УКФ.2	Управление изменениями	+	1. см. п.п. 5.5, 5.6, 5.10 документа «Руководство по

№	Усл. обозн.	Меры обеспечения безопасности	Выполнение входящих в базовый набор мер 17 и 21 приказов ФСТЭК	Ссылки на документацию
		конфигурации информационной системы и системы защиты персональных данных		эксплуатации СХСЗ».

В таблице 4 представлены реализуемые путем применения ПАК «Центр-Т» меры 17-го и 21-го Приказов ФСТЭК по защите информации в информационной системе, не входящие в базовый набор мер.

Таблица 4 - Меры, определенные 17-ым и 21-ым приказами ФСТЭК России, не входящие в базовый набор мер и реализуемые путем применения ПАК СЗИ НСД «Центр-Т»

№	Усл. обозн.	Меры обеспечения безопасности	Выполнение не входящих в базовый набор мер 17 и 21-приказов ФСТЭК	Ссылки на документацию
Идентификация и аутентификация субъектов и объектов доступа (ИАФ)				
1	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	+	1. см. п.п. «Введение» документа «Руководство по эксплуатации СХСЗ».
Управление доступом субъектов доступа к объектам доступа (УПД)				
2	УПД.7	Предупреждение 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	+ При загрузке ПО ПАК «Центр-Т» на экране отображается информация о том, что выполняется загрузка комплекса «Центр-Т»	
Ограничение программной среды (ОПС)				
3	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	
Защита машинных носителей персональных данных (ЗНИ)				
4	ЗНИ.6	Контроль ввода (вывода) информации на машинные носители персональных данных	+	1. см. п.п. 5.5 документа «Руководство по эксплуатации СХСЗ»; 2. см. п.п. 5.3 документа «Руководство по эксплуатации клиентских устройств».
5	ЗНИ.7	Контроль подключения машинных носителей персональных данных	+	
Регистрация событий безопасности (РСБ)				
6	РСБ.8	Обеспечение возможности просмотра и анализа информации о действиях отдельных пользователей в информационной системе	+	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».
Обеспечение доступности персональных данных (ОДТ)				
7	ОДТ.6	Кластеризация информационной системы и (или) ее сегментов	+	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)				
8	ЗИС.4	Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации)	+	1. см. п.п. 4.8.1, 5.5, 5.10 документа «Руководство по эксплуатации СХСЗ».
9	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).	
10	ЗИС.14	Использование устройств терминального доступа для обработки персональных данных	+	1. см. п.п. «Введение», 4.6, 4.7, 11 документа «Руководство по эксплуатации СХСЗ».
11	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.	

12	ЗИС.18	Обеспечение загрузки и исполнения программного обеспечения с машинных носителей персональных данных, доступных только для чтения, и контроль целостности данного программного обеспечения	+	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».
13	ЗИС.19	Изоляция процессов (выполнение программ) в выделенной области памяти	+	1. см. п.п. 3.7, 9 документа «Руководство по эксплуатации СХСЗ».
14	ЗИС.25	Использование в информационной системе или ее сегментах различных типов общесистемного, прикладного и специального программного обеспечения (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.	
15	ЗИС.26	Использование прикладного и специального программного обеспечения, имеющих возможность функционирования в средах различных операционных систем[1)]	+	

[1)] Аналогично выполнению меры ЗИС.25.

3.2 МЕРЫ ИЗ БАЗОВОГО СПИСКА, КОТОРЫЕ ОБЕСПЕЧИВАЮТСЯ В СИСТЕМЕ НЕ СРЕДСТВАМИ «ЦЕНТР-Т»

В Объект защиты «Центр-Т» входят следующие структуры и процессы: СХСЗ, клиентские АРМ, среда их взаимодействия и протекающие в ней процессы. Мер защиты, касающиеся «области ответственности» ПАК «Центр-Т», реализуются с его помощью практически все.

Вне Объекта защиты, т. е. для других объектов системы (например, на терминальном сервере или его окружении) защита обеспечивается с помощью иных подсистем информационной безопасности.

Для того чтобы декларация полноты защитных функций «Центр-Т» не была голословной, в данном пункте рассматриваются меры защиты информации, которые «Центр-Т» не реализует, поскольку они направлены против атак, реализующихся в областях ИС, которые находятся за пределами Объекта защиты «Центр-Т».

В таблице 5 представлены меры 17-го и 21-го Приказов ФСТЭК по защите информации в информационной системе, не реализующиеся «Центром-Т» и обоснование того, что они направлены против атак, реализующихся за пределами Объекта защиты «Центр-Т».

Организационные меры в таблице не рассматриваются, так как должны выполняться эксплуатирующей организацией в рамках принятой политики безопасности, нормативных документов и требований регуляторов.

Таблица 5 - Меры по защите информации 17-го и 21-го приказов ФСТЭК из базового списка, направленные против угроз, реализующихся за пределами Объекта защиты «Центр-Т»

№	Усл. обозн.	Меры обеспечения безопасности	Меры 17 и 21 приказов ФСТЭК по защите информации в информационной системе, направленные против угроз, реализующихся за пределами Объекта защиты «Центр-Т»
Идентификация и аутентификация субъектов и объектов доступа (ИАФ)			
1	ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	- Все пользователи, работающие с ПАК «Центр-Т» являются непосредственными пользователями комплекса, зарегистрированными администраторами удаленного управления и выполняющими строго определенные задачи в рамках своих должностных обязанностей. Пример внешних пользователей – граждане, на законных основаниях через сеть Интернет получающие доступ к информационным ресурсам портала Государственных услуг Российской Федерации «Электронного правительства» или официальным сайтам в сети Интернет

			органов государственной власти. С целью идентификации и аутентификации внешних пользователей рекомендуется использовать специальные средства защиты, обеспечивающие такую функциональность, например, СПО «Аккорд-Win64 K», ПАК «Аккорд-X».
Управление доступом субъектов доступа к объектам доступа (УПД)			
2	УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами	- Угроза, закрываемая мерой УПД.3, неактуальна, так как информационные потоки «Центр-Т» не могут быть несанкционированно изменены в Объекте защиты, в пределах которого происходит сетевое взаимодействие между СХСЗ и терминалами. За пределами Объекта защиты «Центр-Т» при возникновении угроз безопасности защита должна обеспечиваться с помощью иных подсистем информационной безопасности. В рамках управления информационными потоками рекомендуется использовать специальные средства защиты, обеспечивающие такую функциональность, например, МЭ-TrusT.
3	УПД.8	Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему	- Угроза, закрываемая мерой УПД.8, неактуальна, так как пользователь не выполняет процедуру аутентификации в Объекте защиты. За пределами Объекта защиты процедура аутентификации выполняется администраторами СЗИ НСД серверной группы ИС. За пределами Объекта защиты «Центр-Т» при возникновении угроз безопасности защита должна обеспечиваться с помощью иных подсистем информационной безопасности. В рамках оповещения пользователя после успешного входа в ИС о его предыдущем входе в ИС рекомендуется использовать специальные средства защиты, обеспечивающие такую функциональность.
4	УПД.12	Поддержка и сохранение	-

		атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки	Угроза, закрываемая мерой УПД.12, неактуальна, так как Объект защиты ПАК «Центр-Т» не предназначен для управления атрибутами безопасности. За пределами Объекта защиты «Центр-Т» при возникновении угроз безопасности поддержка и сохранение атрибутов безопасности должны обеспечиваться с помощью иных подсистем информационной безопасности. В рамках поддержки и сохранения атрибутов безопасности рекомендуется использовать специальные средства защиты, обеспечивающие такую функциональность, например, СПО «Аккорд-WIN64 К» либо ПАК «Аккорд-Х», СПО «Аккорд-Х К».
5	УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)	- Комплекс «Центр-Т» не взаимодействует в процессе работы со сторонними (внешними) информационными системами. В рамках управления взаимодействием с информационными системами сторонних организаций рекомендуется использовать специальные средства защиты, обеспечивающие такую функциональность, например, криптошлюзы семейства «fin-TrusT», TrusT-in-Motion.
Регистрация событий безопасности (РСБ)			
6	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	- Реагирование на сбои в механизмах сбора информации в части переполнения объема памяти, как правило, заключается в появлении в журнале комплекса соответствующей записи и отсутствии возможности появления в журнале новых записей. В ПАК «Центр-Т» журналы событий безопасности контейнеров СХС3 перезаписываются при каждом выключении/перезагрузке сервера. При условии долгой непрерывной работы СХС3 при достижении максимального значения файлы журналов с сообщениями о событиях безопасности перезаписываются циклически.

			Таким образом, сбоев в механизмах сбора информации в части переполнения объема памяти ПАК «Центр-Т», как правило, не происходит. В рамках обеспечения реагирования на сбои при регистрации событий безопасности рекомендуется использовать специальные средства защиты, обеспечивающие такую функциональность, например, микрокомпьютеры m-TrusT.
Антивирусная защита (АВ3)			
7	АВ3.1	Реализация антивирусной защиты	- Угроза, закрываемая мерой АВ3.1, неактуальна на СХС3, так как изменение состава ОС не предусмотрено технологически, а все приносимые уполномоченными лицами файлы являются файлами данных, которые не получают управление по технологии обработки данных СХС3. На РС эта угроза также не актуальна, так как изменение состава ОС не предусмотрено технологически. За пределами Объекта защиты «Центр-Т» при возникновении угроз безопасности защита должна обеспечиваться с помощью иных подсистем информационной безопасности. С целью защиты от вирусного ПО рекомендуется использовать специальные средства защиты, обеспечивающие такую функциональность, например, решения на базе защищенных микрокомпьютеров m-TrusT.
8	АВ3.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	- База данных признаков вредоносных компьютерных программ на СХС3 и на клиентских РС не применяются.
Обнаружение вторжений (СОВ)			
9	СОВ.1	Обнаружение вторжений	- Угроза вторжений в Объект защиты ПАК «Центр-Т» неактуальна, так как при применении комплекса обеспечивается контроль и ограничение среды взаимодействия СХС3 и клиентов.

			Пользователь работает только в рамках определенного уполномоченными лицами набора ПО. Целостность ПО РС и настроек контролируется. Взаимодействие Объекта защиты «Центр-Т» с внешними системами при этом отсутствует. За пределами Объекта защиты «Центр-Т» при возникновении угроз безопасности защита должна обеспечиваться с помощью иных подсистем информационной безопасности.
10	СОВ.2	Обновление базы решающих правил	- База решающих правил на СХСЗ и на клиентских РС не применяются.
Обеспечение целостности информационной системы и персональных данных (ОЦЛ)			
11	ОЦЛ.5	Контроль содержания информации, передаваемой из информационной системы (контейнерный, основанный на свойствах объекта доступа, и контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов), и исключение неправомерной передачи информации из информационной системы	- Комплекс «Центр-Т» в процессе работы не передает информацию за пределы защищаемой ИС (Объекта защиты). За пределами Объекта защиты «Центр-Т» защита должна обеспечиваться с помощью иных подсистем информационной безопасности. С целью контроля содержания информации, передаваемой из информационной системы, и исключения неправомерной передачи информации из информационной системы рекомендуется использовать специальные средства защиты, обеспечивающие такую функциональность, например, СПО «Аккорд-Win64 К».
12	ОЦЛ.8	Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях	- В рамках работы с ПАК «Центр-Т» персонал комплекса не имеет возможности вводить данные в защищаемую ИС (Объект защиты) либо передавать данные за пределы защищаемой ИС. За пределами Объекта защиты «Центр-Т» защита должна обеспечиваться с помощью иных подсистем информационной безопасности. С целью контроля ошибочных действий

			пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях рекомендуется использовать специальные средства защиты, обеспечивающие такую функциональность, например, СПО «Аккорд-Win64 K».
Защита среды виртуализации (ЗСВ)			
13	ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации	- ПАК «Центр-Т» не предназначен для использования в инфраструктурах виртуализации. Для защиты инфраструктур виртуализации рекомендуется использовать специальные средства защиты, обеспечивающие такую функциональность, например, СПО «Аккорд-В.» (для VmWare vSphere), СПО «Аккорд-KVM» (для KVM).
14	ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин	
15	ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре	
16	ЗСВ.4	Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры	
17	ЗСВ.5	Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией	
18	ЗСВ.6	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных	

19	ЗСВ.7	Контроль целостности виртуальной инфраструктуры и ее конфигураций	
20	ЗСВ.8	Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры	
21	ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре	
22	ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей	
Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)			
23	ЗИС.2	Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом	- Угроза задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом в Объекте защиты ПАК «Центр-Т» неактуальна, так как «Центр-Т» не предназначен для управления метками безопасности. За пределами Объекта защиты «Центр-Т» при возникновении угроз безопасности защита ИС должна обеспечиваться с помощью иных подсистем информационной безопасности. В рамках предотвращения задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом рекомендуется использовать специальные средства защиты, обеспечивающие такую

			функциональность, например, СПО «Аккорд-Win64 К» либо ПАК «Аккорд-Х», СПО «Аккорд-Х К».
24	ЗИС.3	Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при её передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи	- Комплекс «Центр-Т» предназначен для управления образами ПО рабочих станций. «Центр-Т» не предназначен для управления персональными данными. Данные пользователей и администраторов комплекса в рамках работы «Центр-Т» не передаются. При возникновении необходимости обеспечения защиты персональных данных от раскрытия, модификации и навязывания при её передаче по каналам связи рекомендуется использовать специальные средства защиты, обеспечивающие такую функциональность, например, «Аккорд-АМДЗ».
25	ЗИС.6	Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с информацией, при обмене информацией с иными информационными системами	- ПАК «Центр-Т» не предназначен для управления метками безопасности. Кроме того, все пользователи, работающие с ПАК «Центр-Т» являются непосредственными пользователями комплекса. Работа с внешними пользователями в рамках Объекта защиты «Центр-Т» исключена. За пределами Объекта защиты «Центр-Т» при возникновении угроз безопасности защита должна обеспечиваться с помощью иных подсистем информационной безопасности. При возникновении необходимости передачи и контроля целостности атрибутов безопасности (меток безопасности), связанных с информацией, при обмене информацией с иными информационными системами рекомендуется использовать специальные средства защиты, обеспечивающие такую функциональность, например, СПО «Аккорд-Win64 К».
26	ЗИС.12	Исключение возможности отрицания пользователем факта отправки персональных данных другому пользователю	- Комплекс «Центр-Т» не предназначен для управления персональными данными. Данные пользователей и администраторов

27	ЗИС.13	Исключение возможности отрицания пользователем факта получения персональных данных от другого пользователя	комплекса в рамках работы «Центр-Т» не передаются. За пределами Объекта защиты «Центр-Т» при возникновении угроз безопасности защита должна обеспечиваться с помощью иных подсистем информационной безопасности. При возникновении необходимости контроля персональных данных рекомендуется использовать специальные средства защиты, обеспечивающие такую функциональность, например, «Аккорд-АМДЗ».
28	ЗИС.20	Защита беспроводных соединений, применяемых в информационной системе	- Угроза, закрываемая мерой ЗИС.20, неактуальна, так как в рамках Объекта защиты «Центр-Т» – на СХСЗ и РС – применение беспроводных соединений не предусмотрено технологически. За пределами Объекта защиты «Центр-Т» при возникновении угроз безопасности защита должна обеспечиваться с помощью иных подсистем информационной безопасности. В рамках защиты беспроводных соединений рекомендуется использовать специальные средства защиты, обеспечивающие такую функциональность, например, криптошлюзы семейства «fin-TrusT».
29	ЗИС.23	Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями	- «Центр-Т» обеспечивает защиту в рамках Объекта защиты, и не взаимодействует с иными информационными системами. За пределами Объекта защиты «Центр-Т» при возникновении угроз безопасности защита обеспечивается с помощью иных подсистем информационной безопасности.
30	ЗИС.24	Прекращение сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого соединения	- Угроза, закрываемая мерой ЗИС.24, неактуальна, так в периметре Объекта защиты «Центр-Т» сетевые соединения не могут быть несанкционированно изменены. За пределами Объекта защиты «Центр-Т» при возникновении угроз безопасности

			защита должна обеспечиваться с помощью иных подсистем информационной безопасности.

3.3 РЕЗУЛЬТАТЫ АНАЛИЗА МЕР

Выводы можно сделать относительно общего числа мер защиты из 17-го и 21-го Приказов ФСТЭК по защите информации, и отдельно – относительно тех из них, что касаются непосредственно целевых функций ПАК «Центр-Т».

Цель применения ПАК «Центр-Т» – централизованное управление и администрирование компонентов ПО РС, поэтому путем применения комплекса в ИС реализуются большинство мер, направленных на реализацию управления и администрирования ПО клиентских РС.

Это меры группы ОПС (ограничение программной среды), УПД (управление доступом), АНЗ (контроль защищенности информации) и ИАФ (идентификация и аутентификация).

Всего их 32[1)].

За счет применения ПАК «Центр-Т» выполняются 27 мер (ИАФ: 1, 2, 3, 4, 5, 7; УПД: 1, 2, 4, 5, 6, 7, 9, 10, 11, 13, 15, 17; ОПС: 1, 2, 3, 4; АНЗ: 1, 2, 3, 4, 5). Остальные 5 мер из описанных 33 (ИАФ.6, УПД.3, УПД.8, УПД.12, УПД.16), которые не выполняются Центром-Т, направлены против угроз, реализующихся за пределами Объекта защиты «Центр-Т».

Процентное соотношение выполняемых и не выполняемых мер групп ОПС, УПД, АНЗ и ИАФ показано на рисунке:

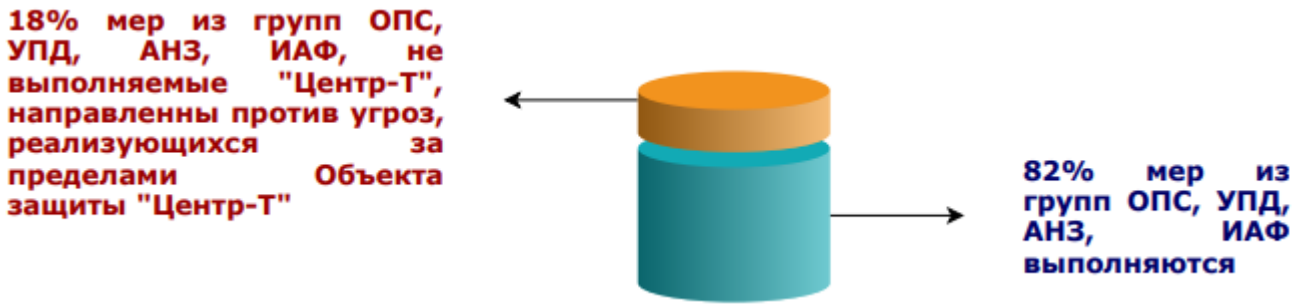

Рисунок 6 – Выполнение мер групп ИАФ, УПД, ОПС, АНЗ в ИС путем применения ПАК «Центр-Т»

Общее количество мер, выполняемых комплексом «Центр-Т» – 60. Остальные меры, которые не выполняются ПАК «Центр-Т», направлены против

[1)] Общее количество мер групп ОПС, УПД, АНЗ, ИАФ в соответствии с текстом 17-го и 21-го Приказов ФСТЭК по защите информации в информационной системе – 33. Однако мера УПД.14 является организационной, поэтому в рамках анализа мер, выполняемых путем применения «Центр-Т», не рассматривается.

угроз, реализующихся за пределами Объекта защиты «Центр-Т», их общее количество – 30.

Процентное соотношение выполняемых и невыполняемых мер к их общему количеству показано на рисунке:

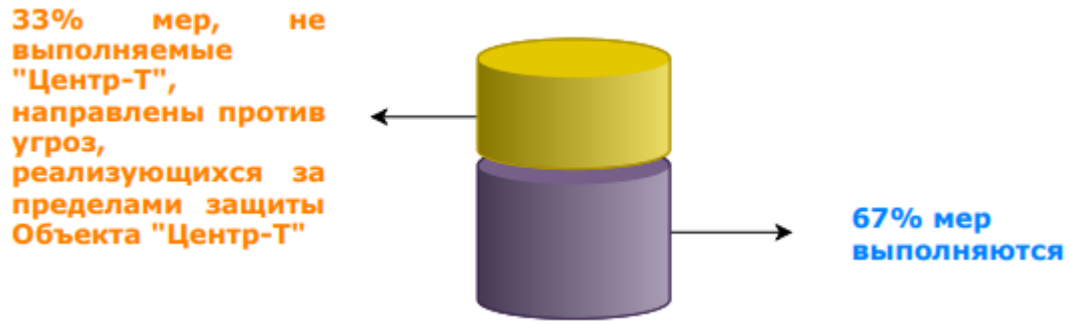

Рисунок 7 – Соотношение выполняемых и невыполняемых комплексом «Центр-Т» мер

Помимо этого, в ПАК «Центр-Т» реализованы возможности для обеспечения мер доступности технических средств (ОДТ.2, ОДТ.3, ОДТ.6), целостности ИС и данных (ОЦЛ.1, ОЦЛ.3, ОЦЛ.6), а также защиты ИС (ЗИС.1, ЗИС.4, ЗИС.5, ЗИС.10, ЗИС.11, ЗИС.14, ЗИС.15, ЗИС.16, ЗИС.18, ЗИС.19, ЗИС.21, ЗИС.22, ЗИС.25, ЗИС.26), защиты носителей информации (ЗНИ.2, ЗНИ.5, ЗНИ.6, ЗНИ.7), регистрации событий безопасности (РСБ.1, РСБ.2, РСБ.3, РСБ.5, РСБ.6, РСБ.7, РСБ.8), регистрации инцидентов (ИНЦ.2) и управления конфигурациями (УКФ.2).

Общее соотношение долей различных категорий выполняемых и невыполняемых мер к их общему количеству показано на рисунке 8.

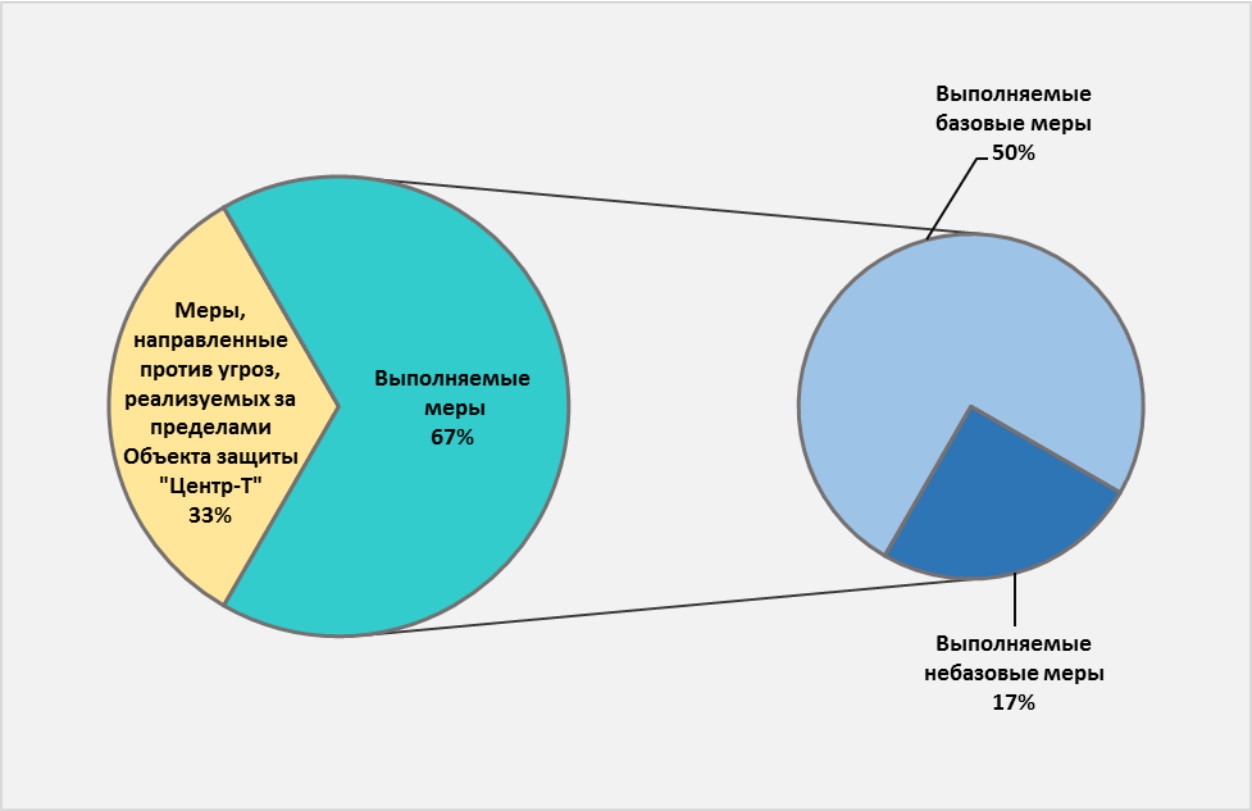

Рисунок 8 – Соотношение долей различных категорий мер к их общему количеству