Краснодарское высшее военное училище имени генерала армии С.М. Штеменко

Доклад на тему:

«Поиск новых технических решений по маскированию структуры информационных систем на основе реконфигурирования их сетевых параметров»

Подготовил: Каплин Максим Андреевич

Приказ ФСТЭК РФ от 18.02.2013 № 21 **«Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»** (в ред. Приказа ФСТЭК РФ от 23.03.2017 № 49)

Планирование и принятие мер по предотвращению повторного возникновения инцидентов (ИНЦ.6)

Приказ ФСТЭК РФ от 15.02.2017 № 27 **«О внесении изменений в Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом ФСТЭК РФ от 11 февраля 2013 № 17»**

Воспроизведение ложных и/или скрытие истинных отдельных ИТ и/или структурно-функциональных характеристик ИС или ее сегментов, обеспечивающее навязывание нарушителю ложного представления об истинных ИТ и/или структурно-функциональных характеристиках ИС (ЗИС.28)

Перевод информационной системы или ее устройств (компонентов) в заранее определенную конфигурацию, обеспечивающую защиту информации, в случае возникновения отказов (сбоев) в системе защиты информации информационной системы (ЗИС.29)

Приказ ФСТЭК РФ от 16.07.2019 № 135 **«Об утверждении Перечня нормативных правовых актов или их отдельных частей, оценка соблюдения которых является предметом государственного контроля (надзора) в области обеспечения безопасности значимых объектов КИИ РФ»**

При проведении мероприятий государственного контроля, **соблюдение Приказа** ФСТЭК РФ от 25.12.2017 № 239 **оценивается в полном объеме**

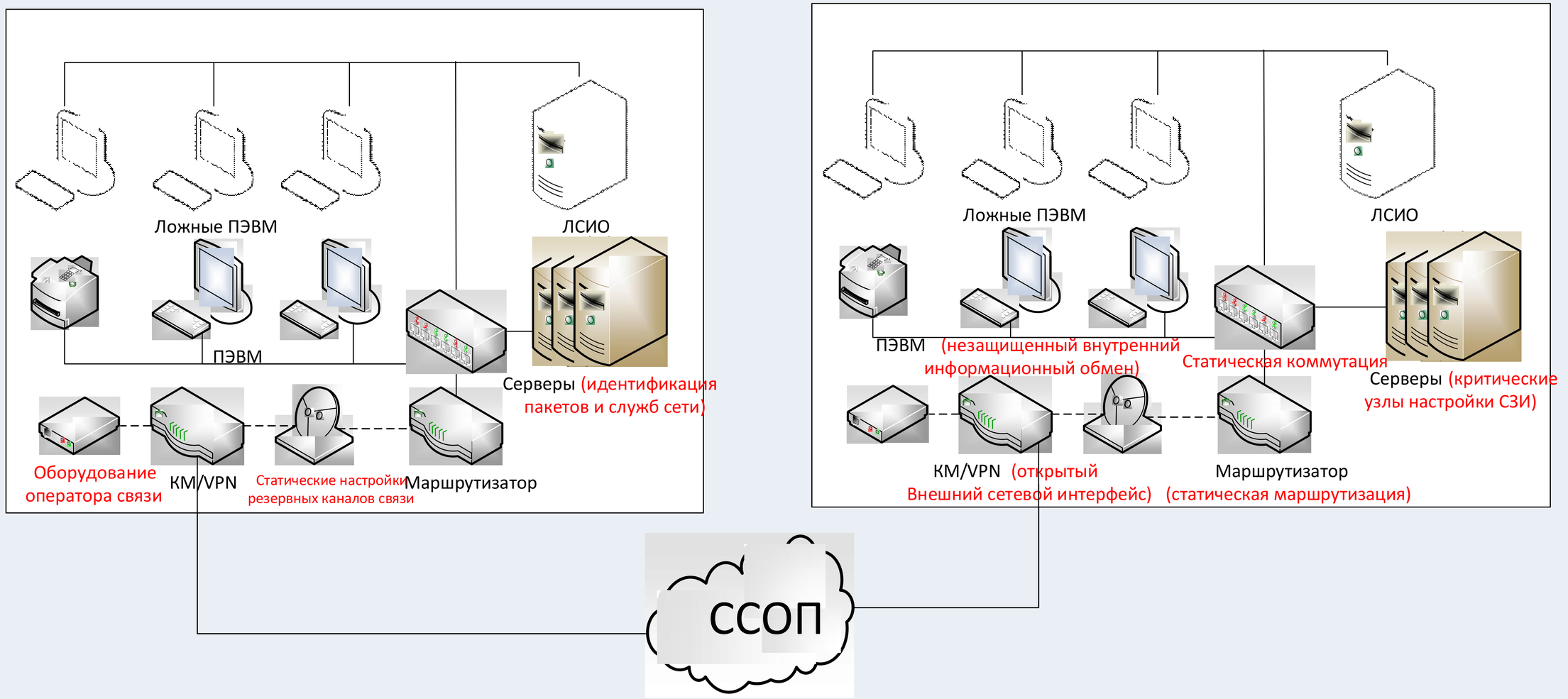
Приказ ФСТЭК РФ от 25.12.2017 № 239 **«Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры РФ»** (в ред. Приказа ФСТЭК РФ от 26.03.2019 № 60)

Сокрытие архитектуры и конфигурации информационной (автоматизированной) системы (ЗИС.8)

Перевод информационной системы в безопасное состояние при возникновении отказов (сбоев) (ЗИС.37)

Управление изменениями конфигурации информационной системы и системы защиты персональных данных (УКФ.2)

Логическая структурная схема распределенных сегментов ИС



Наименование угроз безопасности информации (внутренний нарушитель)

1. Угроза изменения компонентов информационной (автоматизированной) системы (УБИ.025)
2. Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации (УБИ.216)

Наименование угроз безопасности информации (внешний нарушитель)

1. Угроза определения топологии вычислительной сети (УБИ.106)
2. Угроза получения предварительной информации об объекте защиты (УБИ.134)
3. Угроза обнаружения хостов (УБИ.101)

ЗАДАЧА СЕРВЕРА– перевод санкционированных клиентов на новые СФХ при поступлении штатных заявок на их смену, а также в случае обнаружения средствами СОА попыток сканирования средствами СР

Эта задача выполняется посредством перераспределения DHCP-сервером сетевых параметров клиентам ИС, таких как *IP*-адреса и времени его аренды

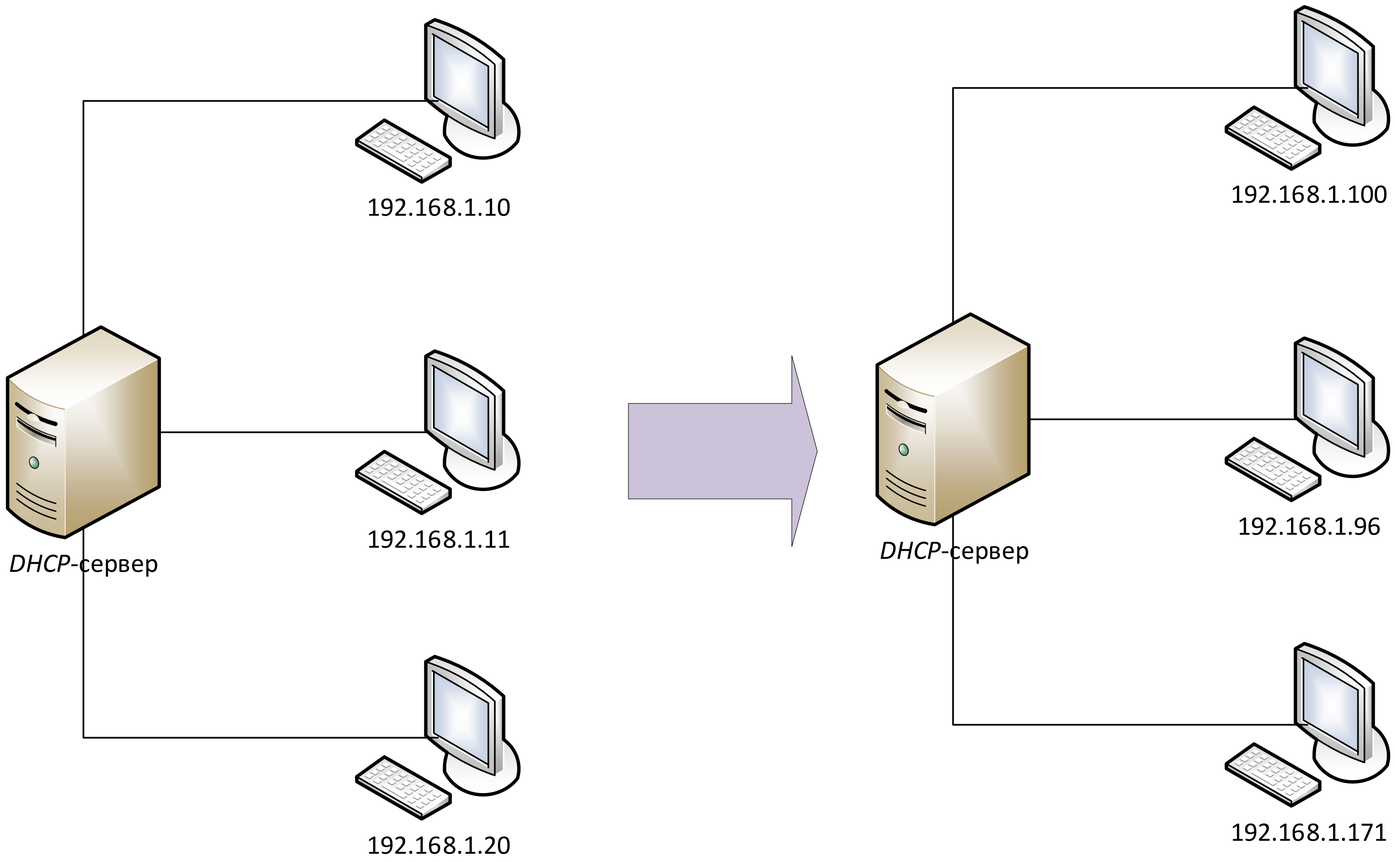


Схема процесса смены сетевых параметров клиентам сети DHCP-сервером

Применение ложных компонентов ИС