Принципы и схемы работы системы видеонаблюдения с использованием средств комплексной защиты информации

Условные обозначения и сокращения

СКЗИ: Средства Комплексной Защиты Информации.

Камера: IP-камера BSP Security с устройством СКЗИ. IP-камера BSP Security с устройством, обеспечивающим шифрование отдаваемой камерой информации и дешифрование поступающих на камеру запросов.

Сервер СКЗИ: Программно-аппаратный комплекс (компьютер со специализированным программным обеспечением) обеспечивающий дешифрование видеопотока с камер и шифрование поступающих на камеры запросов.

Клиент: Клиентское устройство не оснащенный СКЗИ, с которого может идти управление камерами, или на котором ведется сбор или обработка поступающей с камер информации. Например, это может быть сервер с ПО BSP VMS или видеорегистратор.

АРМ Администратора: Компьютер со специализированным программным обеспечением, на котором производится инициализация (начальная настройка) камер.

Принципы работы и конфигурация элементов системы

СКЗИ перемещает весь трафик системы видеонаблюдения в виртуальную сеть, защищенную с использованием TLS-соединений, создаваемых с использованием сертифицированного СКЗИ. При этом все делается прозрачно для системы видеонаблюдения. Исключается чтение/подмена информации злоумышленником, получившим доступ к сетевой инфраструктуре системы видеонаблюдения.

На сервере СКЗИ ведётся syslog в формате НПО Гамма. Детекция кибератак осуществляется или Гаммой на основе анализа нашего syslog, или другой уполномоченной организацией. Сервер СКЗИ осуществляет дешифрование всей поступающей с камер информации для клиентов и шифрует все поступающие от клиентов камерам запросы.

В качестве протокола шифрования используется протокол TLS. Все криптографические алгоритмы, использующиеся для защиты данных, отечественные, принятые в качестве национальных стандартов:

- Ключи устройств (камер/серверов СКЗИ, используются для взаимной аутентификации устройств и выработки ключа согласования) - ГОСТ Р 34.10-2012 (поддерживаются "обычный" и "усиленный" варианты алгоритма);
- Алгоритм выработки ключа согласования: VKO_GOSTR3410_2012_512
- Алгоритм шифрования: ГОСТ 28147-89 на сессионном ключе.

Инициализация камер производится на специальном выделенном компьютере (АРМ Администратора). Для этого камера подключается к АРМ Администратора напрямую, или через

"удаленный" режим, предусматривающий передачу информации между АРМ и камерой с использованием отчуждаемых носителей информации (при разворачивании серверного ПО на полноразмерной ЭВМ-сервере). Ключи и запросы на сертификат генерируются на камере в процессе ее инициализации. Сертификаты на ключи выдаются либо на АРМ Администратора, либо могут выдаваться на стороннем сертифицированном Удостоверяющем Центре.

АРМ Администратора может быть поставлен заказчику для самостоятельной инициализации камер. Также сторонняя организация (дилер) может предоставлять услуги по содержанию и обслуживанию АРМ Администратора и ведения конфигурации камер, в этом случае заказчик получает камеры уже инициализированными и настроенными.

Вся схема в целом функционирует прозрачно для системы видеонаблюдения. Сервер системы видеонаблюдения (компьютер с BSP VMS или видеорегистратор) и камеры будут видеть друг друга используя IP-адресацию. Камера может получать закрепленный за ней адрес (задается при задании конфигурации системы на АРМ Администрирования) по DHCP, или должна быть настроена заранее на использование статического IP. На сервере системы видеонаблюдения должен быть прописан сервер СКЗИ в качестве шлюза по умолчанию, или прописан в качестве назначения для специфичных маршрутов для подсети, в которой находятся камеры.

Схемы подключения

Конфигурация камеры

Для конфигурации камеры ее подключают напрямую к АРМ Администратора, производят ее инициализацию (генерируется ключевая информация) и устанавливаются сетевые настройки (IP-адрес, маска и шлюз). После этого камера подключается по месту своего дальнейшего местонахождения в системе видеонаблюдения.

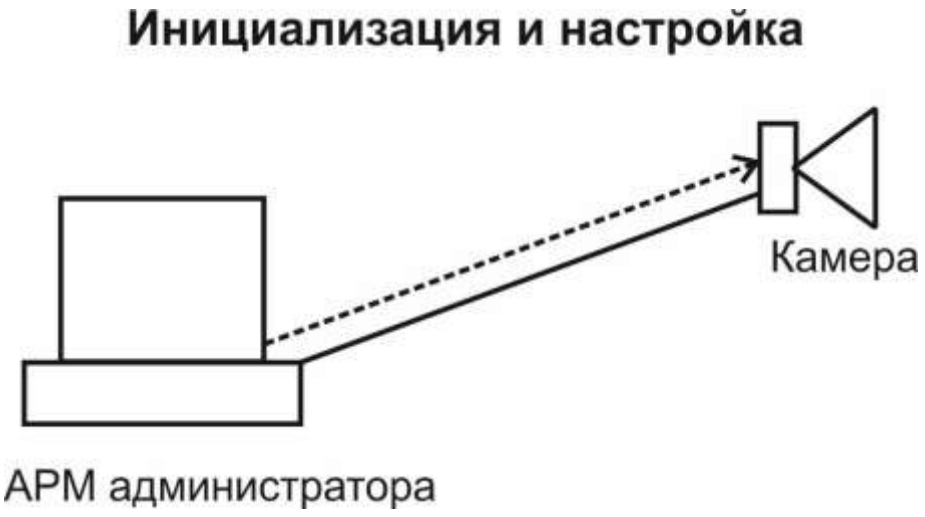

Схема подключения в ЛВС

Показана простейшая схема подключения, когда все сетевые устройства подключены к одному коммутатору. IP-адресация в такой системе может быть как «плоской» (все устройства находятся в одной IP-сети), так и сложнее (например, когда камеры находятся в одной сети, а компьютеры в другой). В любом случае, чтобы «достучаться» до камеры с компьютера или сервера BSP VMS необходимо добавить маршрут до камеры, указав в качестве маршрутизатора (шлюза) адрес сервера СКЗИ.

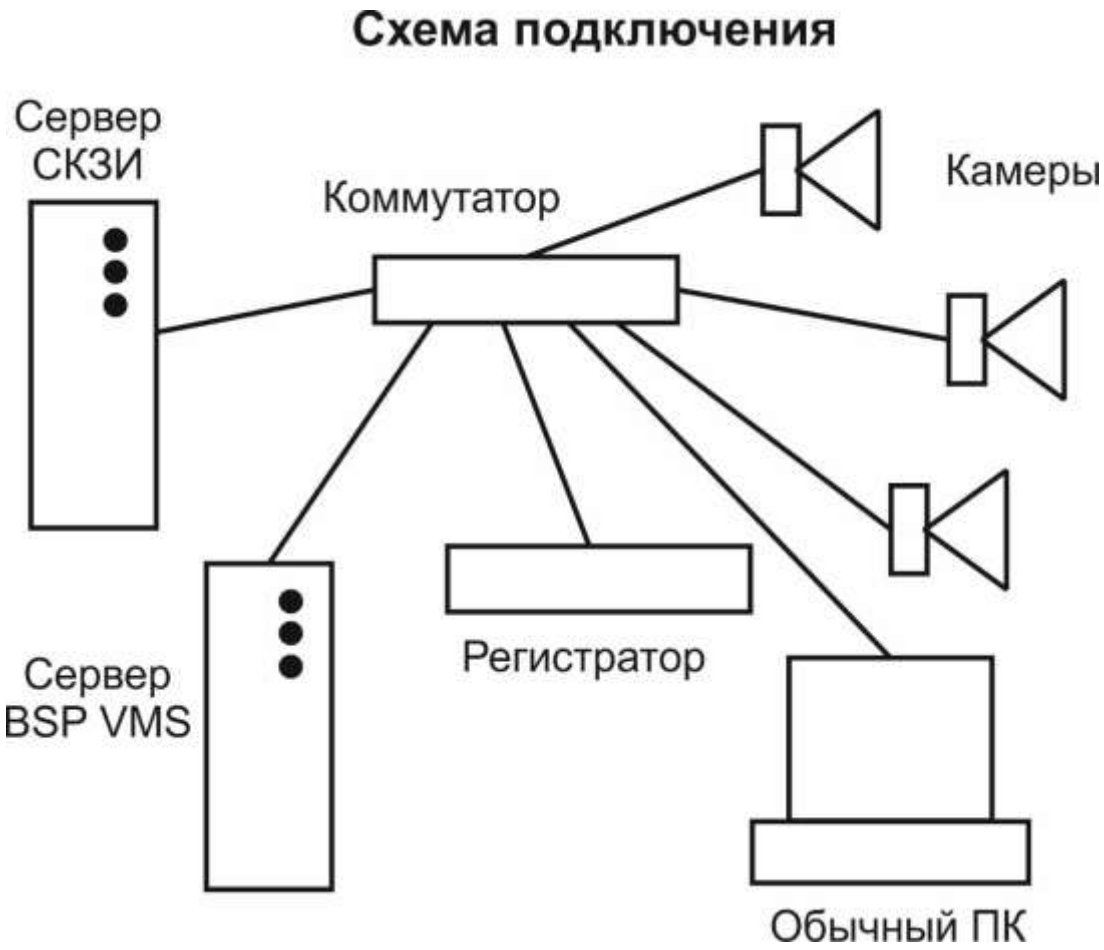

Схема передачи информации

При попытке доступа к камере напрямую, минуя сервер СКЗИ соединение установлено не будет. Чтобы получить видеопоток с камеры необходимо обращаться к ней через сервер СКЗИ.

Это можно сделать или добавив отдельные маршруты для каждой из камер, указав в них в качестве шлюза IP-адрес сервера СКЗИ, или, если камеры находятся в отдельной IP-сети, добавив один маршрут для сети камер, опять-таки указав в качестве шлюза адрес сервера СКЗИ.