

«Технологический колледж № 34»

**ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
на тему:**

**«Организация защиты информации от
преднамеренных угроз в ЛВС под управлением
Windows в ООО «Художественная керамика»»**

Выполнил:

Научный руководитель:

Цель и задачи

Цель - разработка защищенной локальной сети, для повышения уровня сетевой безопасности сети, а также увеличение защищенности имеющихся сегментов сети.

Задачи:

1. провести анализ текущего состояния локальной сети;
2. описать защитные меры;
3. изучить политику безопасности;
4. разработать модели нарушителя и актуальных угроз;
5. разработать проект локальной сети;
6. осуществить выбор продукта для разработки защищённой сети;
7. разработать проект защищённой локальной сети на базе программного
8. комплекса VipNet.

Состав технических средств и программного обеспечения

№	Наименование
1	Технические средства
1.1	ПЭВМ (системный блок, монитор, клавиатура, мышь)
2	Программное обеспечение:
2.1	Операционная система со всеми компонентами, необходимыми для работы
2.2	Антивирусное СЗИ «Kaspersky Endpoint Security»
2.3	СЗИ от НСД «Secret Net 7»
2.4	Пакет программ управления VipNet IDS
Дополнительные компоненты	
1	VipNet IDS, выполняющий роль межсетевого экрана (МЭ)
2	Сетевой коммутатор
3	Источник бесперебойного питания
4	Многофункциональное устройство (МФУ), выполняющее роль принтера
5	Съемные носители информации для хранения ключевой информации
6	Съемные носители информации для передачи данных
7	Съемные носители информации для резервного копирования
8	Линии передачи информации между компонентами локальной сети в границах контролируемой зоны
9	Линии передачи информации между компонентами локальной сети, выходящие за границы контролируемой зоны
10	Линии электропитания и заземления
11	Линии охранной и пожарной сигнализации

Защищаемая информация

№	Защищаемая информация	Форма фиксации	Обозначение
1	Ключи ЭП владельцев сертификатов ключей проверки ЭП	Области оперативной памяти ТС - в процессе генерации ключей ЭП	ЗИ1
		Файлы на съемном ключевом носителе	ЗИ2
2	Ключ ЭПФС	Области оперативной памяти ТС	ЗИ3
		Файлы на съемном ключевом носителе	ЗИ4
3	Персональная и корпоративная информация пользователей ИС, не подлежащая рассылке	Записи БД на жестких дисках ТС	ЗИ5
		Записи БД на съемных носителях резервного копирования	ЗИ6
		Данные в сетевых пакетах	ЗИ7
		Изображение на экране монитора	ЗИ8
4	Сертификаты ключей проверки ЭП пользователя и их статус	Файлы и записи БД на жестких дисках ТС	ЗИ9
		Записи БД на съемных носителях резервного копирования	ЗИ10
		Данные в сетевых пакетах	ЗИ11
		Бумажные документы	ЗИ12
		Изображение на экране монитора	ЗИ13
5	Запросы на получение, аннулирование (отзыв), приостановление и возобновление действия	Файлы и записи БД на жестких дисках ТС	ЗИ14
		Записи БД на съемных носителях резервного копирования	ЗИ15
		Данные в сетевых пакетах	ЗИ16

Объекты доступа

Защищаемая информация	Объект доступа	Объект доступа на аппаратном уровне
ЗИ1, ЗИ3, СИ3	Области ОЗУ	Модули оперативной памяти
ЗИ5, ЗИ9, ЗИ14, ЗИ18, СИ1, СИ4, СИ7, СИ11	Базы данных и отдельные файлы	Жесткие диски
СИ12		Жесткие диски
ЗИ2, ЗИ4, СИ2	Файлы	Съемные защищенные носители информации
ЗИ6, ЗИ10, ЗИ15	Базы данных	Съемные носители информации для целей резервирования информации
ЗИ17, ЗИ20, СИ13	Файлы	Съемные носители информации для целей переноса информации
ЗИ7, ЗИ11, ЗИ16, ЗИ19, СИ6, СИ8	Сетевые пакеты	Сетевые кабели
ЗИ8, ЗИ11, СИ5, СИ9	-	Монитор
СИ10	-	ТС, сетевые кабели
ЗИ12	-	Принтер

Характеристика безопасности программного обеспечения

№	Объект угроз	Характеристики безопасности		
		Конфиденциальность	Целостность	Доступность
1	П01	-	+	+
2	П02	-	+	+
3	П03	-	+	+
4	П04	-	+	+
5	П03	-	+	+
6	П06	-	+	+
7	П07	-	+	+
8	П08	-	+	+
9	П09	-	+	+

Характеристика безопасности ТС

№	Объект угроз	Характеристики безопасности		
		Конфиденциальность	Целостность	Доступность
1	ТС1	-	+	+
2	ТС2	-	+	+
3	ТС3	-	+	+
4	ТС4	-	+	+
5	ТС5	-	+	+
6	ТС6	-	+	+
7	ТС7	-	+	+
8	ТС8	-	+	+
9	ТС9	-	+	+
10	ТС10	-	+	+
11	ТС11	-	+	+
12	ТС12	-	+	+
13	ТС13	-	+	+
14	ТС14	-	+	+
15	ТС15	-	+	+
16	ТС16	-	+	+

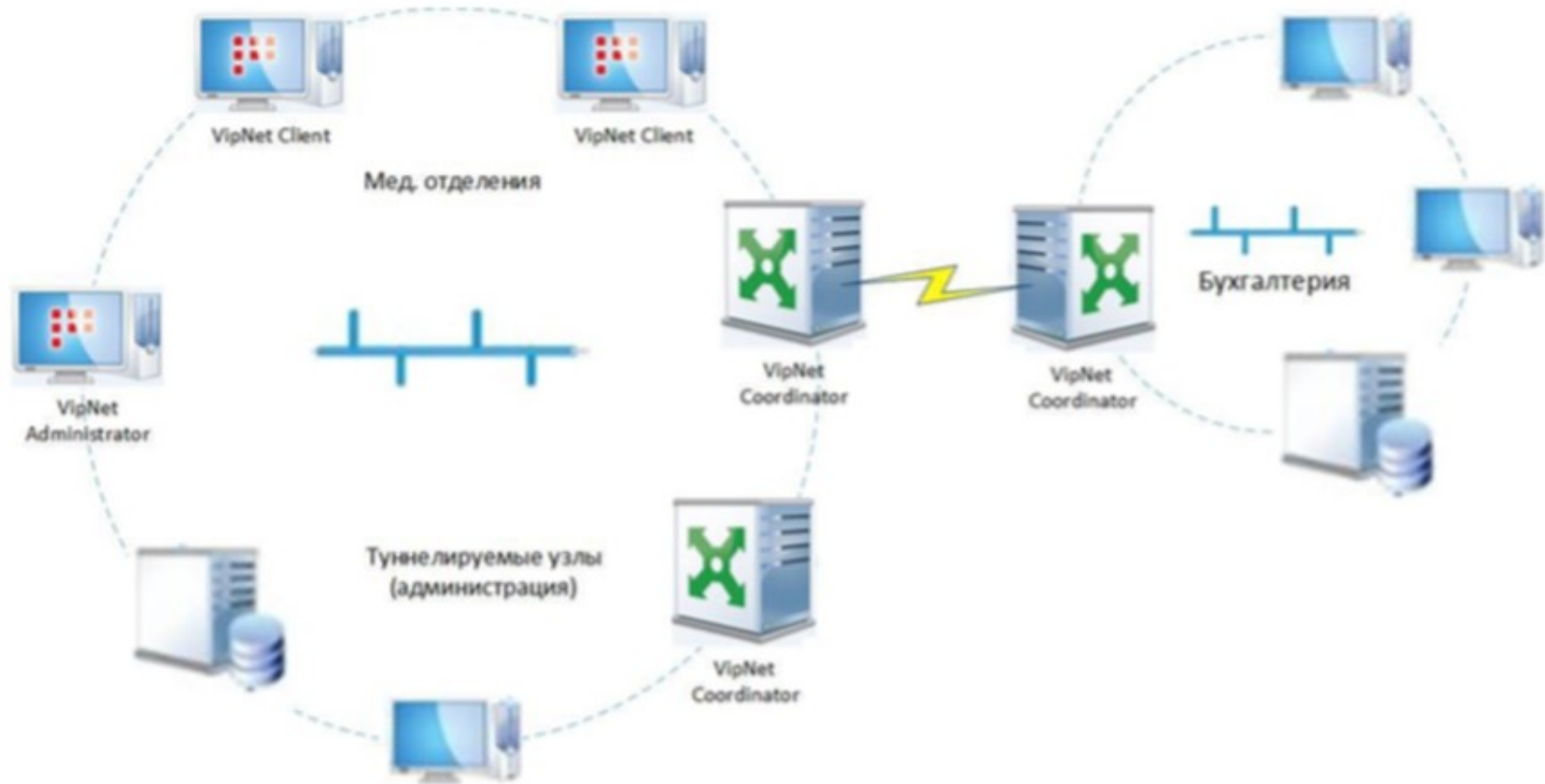
Соотношение ТС, ПО, ЗИ и СИ

Техническое средство	Функционирующее ПО	Обрабатываемая, хранящаяся, передаваемая информация	
		Защищаемая информация	Сопутствующая информация
ТС1	ПО1, ПО2, ПО3, ПО5, ПО7, ПО8	ЗИ9, ЗИ12, ЗИ18	СИ1, СИ4, СИ7, СИ10
ТС2	ПО1, ПО2, ПО3, ПО4, ПО3, ПО7, ПО8	ЗИ5, ЗИ9, ЗИ12, ЗИ18	СИ1, СИ4, СИ7, СИ10, СИ11, СИ12
ТС3	ПО1, ПО2, ПО3, ПО3, ПО6, ПО7, ПО8	ЗИ1, ЗИ3, ЗИ8, ЗИ9, ЗИ13, ЗИ12	СИ3, СИ4, СИ7, СИ10
ТС4	-	-	СИ4, СИ7
ТС5	ПО9	-	СИ4, СИ7, СИ10
ТС6	-	-	СИ5, СИ9, СИ10
ТС8	-	ЗИ7, ЗИ11, ЗИ16, ЗИ19	СИ6, СИ8, СИ10
ТС9	-	ЗИ7, ЗИ11, ЗИ16, ЗИ19	СИ6, СИ8, СИ10
ТС10	-	ЗИ11,ЗИ16, ЗИ19	-
ТС11	-	ЗИ11	-
ТС12	-	ЗИ6, ЗИ10, ЗИ15	-
ТС13	-	ЗИ9, ЗИ14	СИ9, СИ11

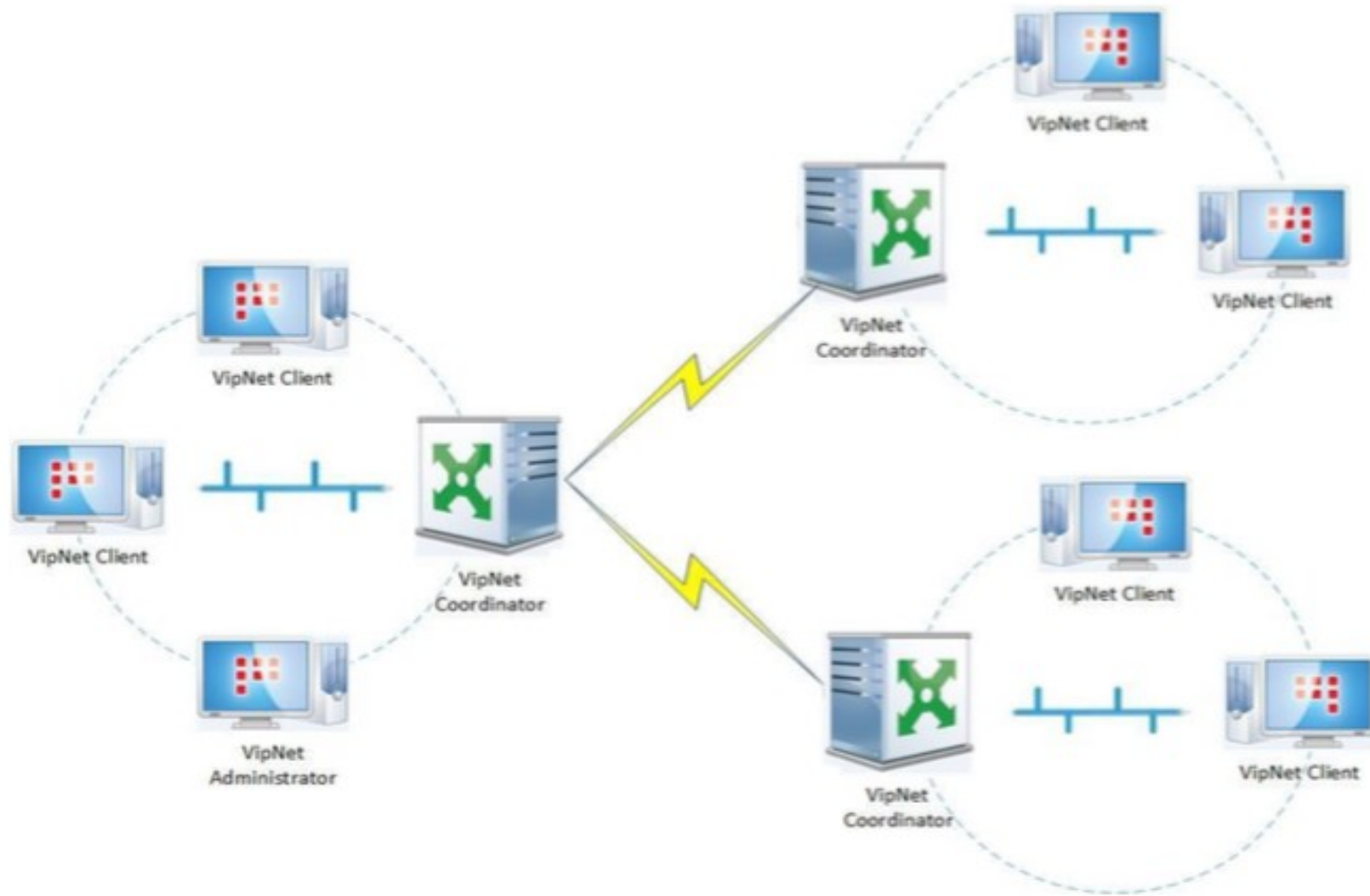
Сравнение VipNet и АПКШ «Континент»

Критерий	VipNet CUSTOM	АПКШТТ «Континент» 3.7
Сертификация СКЗИ	КС1 КС2 КС3	КС1 КС2 КС3
Сертификация МЭ	ФСБ 4-й ФСТЭК 3-й	ФСБ 4-й ФСТЭК 3-й
ИСПДн	К1	К1
Объединение двух и более сетей	ВОЗМОЖНО	Нет возможности
Возможность работы с пересекающейся IP адресацией	есть	нет
Возможные архитектуры	«клиент» - «клиент» «клиент» - «сервер» «сервер» - «сервер»	«клиент» - «сервер» «сервер» - «сервер»
Возможность работы с удаленными пользователями	есть	есть
Стоимость	7 790,00	6 600,00

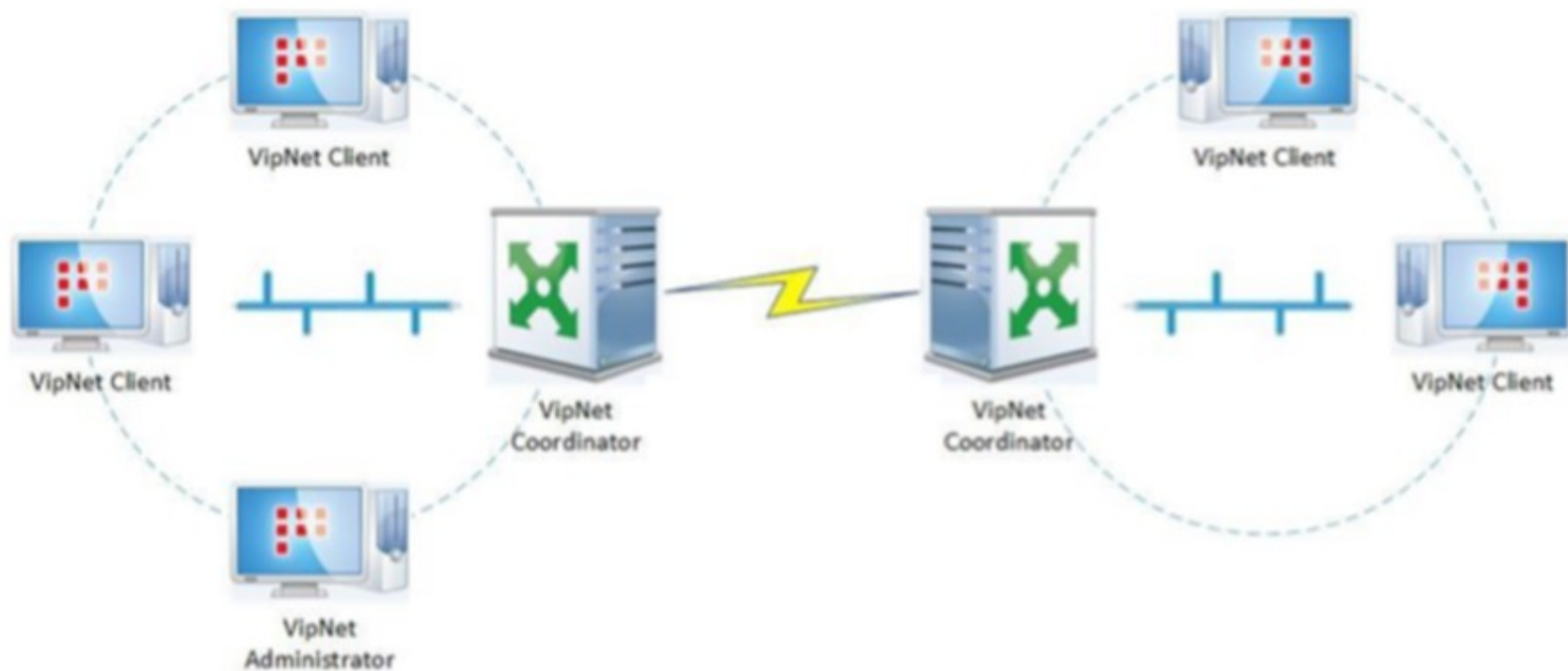
Первая сеть VipNet



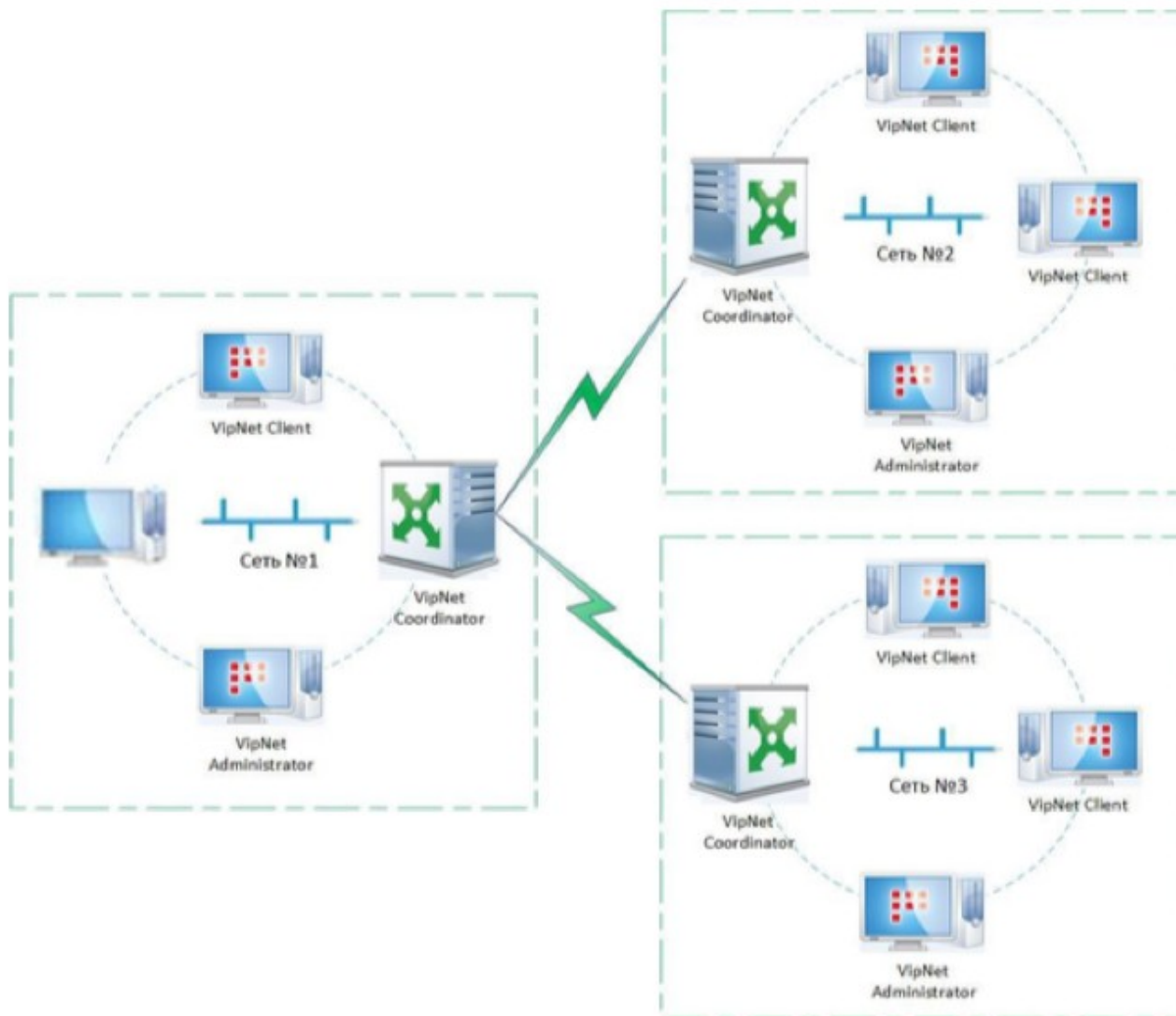
Вторая сеть VipNet



Третья сеть VipNet



Структура сети с организацией межсетевого взаимодействия



Рекомендации

- требуется защита информационного обмена при прохождении через открытый Интернет;
- требуется, чтобы защищенный туннель был прозрачен для пользователей, которые работают с ресурсами удаленных локальных сетей;
- требуется, чтобы пользователи локальной сети не имели доступа к ресурсам открытого Интернета, за исключением ресурсов других локальных сетей, определенных администратором, с которыми организуется защищенное взаимодействие и, возможно, ресурсов мобильных пользователей;
- требуется исключить необходимость установки ПО ViPNet [Координатор] на шлюзы локальной сети.

БЛАГОДАРЮ ЗА ВНИМАНИЕ!