



**ViPNet Coordinator (Linux)** — программный сервер защищенной сети ViPNet, устанавливаемый на ОС Linux с ядрами 2.6.x (до 2.6.39 включительно) или 3.x (до 3.6 включительно) (дистрибутивы RedHat, Suse и др.). В зависимости от настроек ViPNet Coordinator (Linux) может выполнять следующие функции:

- Сервера IP-адресов;
- Прокси-сервера защищенных соединений;
- Туннелирующего сервера (криптошлюза);
- Межсетевое экрана для открытых, защищенных ресурсов и туннелируемых ресурсов;
- Сервера защищенной почты;
- Отказоустойчивого сервера защищенной сети ViPNet в конфигурации ViPNet Failover.

**Поддерживаемые операционные системы:**

- ALT Linux 6.0 Server;
- ALT Linux 6.0 Desktop;
- CentOS 5.4;
- CentOS 5.7;
- CentOS 6.0;
- Mandriva Linux 2010 Powerpack;
- RedHat Enterprise Linux 5.4;
- RHEL 5.7; RHEL 6.0 AS;
- Slackware Linux 12.0 (только ядро 2.6.16.52 с FTP-сервера ftp://kernel.org); Slackware Linux 12.2; • SUSE Linux Enterprise Server 10; SUSE Linux Enterprise Server 10 SP1, SP2, SP3; SUSE Linux Enterprise Server 11;
- SLES 11 SP1;
- Ubuntu 10.04.

**Внимание! Все поддерживаемые дистрибутивы ОС Linux должны быть для 32-разрядной архитектуры.**

**ViPNet Coordinator (Windows)** - программный сервер защищенной сети ViPNet, функционирующий под управлением операционных систем MS Windows: Windows XP SP3 (32-разрядная) / Windows Server 2003 (32-разрядная) / Windows Vista SP2 (32/64-разрядная) / Windows Server 2008 (32/64-разрядная) / Windows 7 (32/64-разрядная)/Windows Server 2008 R2 (64-разрядная).

**В зависимости от настроек ViPNet Coordinator может выполнять следующие функции:**

- Сервера IP-адресов — обеспечивает регистрацию и доступ в реальном времени к информации о состоянии объектов защищенной сети и текущем значении их сетевых настроек (IP-адресов и т.п.).
- Проксирование защищенного трафика (организация безопасной связи между защищенными сетями через публичные сети).
- Оповещение узлов о параметрах доступа друг к другу (сервер IP-адресов).
- Организация защищенного взаимодействия с открытым узлом в локальной сети (туннелирование).
- Фильтрация открытого и туннелируемого трафика (межсетевой экран).
- Выполнение динамической и статической трансляции IP-адресов (NAT).
- Организация безопасного подключения компьютеров корпоративной сети к Интернету (сервер Открытого Интернета).

*Сертификат ФСБ № СФ/124-3091. Действителен до 31.12.2018. соответствует требованиям ГОСТ 28147-89, ГОСТ Р 34.11-94, Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, классов КС1 (для исполнения 1) и класса КС2 (для исполнения 2) и может использоваться для криптографической защиты (создание ключевой информации, шифрование файлов, данных, содержащихся в областях оперативной памяти, и IP-трафика, вычисление имитовставки для файлов, данных, содержащихся в областях оперативной памяти, и IP-трафика) информации, не содержащей сведений, составляющих государственную тайну*

**Наши контактные данные:**

*ул. Ленина, д.20, (четвертый этаж), каб. 422, 423. Остановка "Яблонька".  
e-mail: [info@ooo-skb.ru](mailto:info@ooo-skb.ru) (ссылка для отправки email)  
тел. 53-20-18*