

## ПАК ViPNet Coordinator HW



### Общие сведения

Программно-аппаратный комплекс (ПАК) **ViPNet Coordinator HW** представляет собой линейку устройств с интегрированным программным обеспечением производства ОАО «ИнфоТеКС». ПАК ViPNet Coordinator HW является универсальным шлюзом безопасности и предоставляет возможность создать в любой телекоммуникационной инфраструктуре, включая сети связи общего пользования, распределенную виртуальную сеть (VPN), защищенную от сетевых атак и несанкционированного доступа к информации. ПАК ViPNet Coordinator HW легко устанавливается в существующую инфраструктуру и соответствует самым жестким требованиям по функциональности, удобству эксплуатации, надежности и отказоустойчивости.

ПАК ViPNet Coordinator HW входит в состав программного комплекса ViPNet VPN.

### Возможности

ПАК ViPNet Coordinator HW предоставляет широкий спектр сервисов.

### Функции безопасности

- VPN-шлюз — стандартная для классических VPN функция, реализующая создание защищенных каналов (туннелей) посредством шифрования трафика открытых узлов, размещенных за координатором, и передачи этого трафика на другие VPN-шлюзы или защищенные клиенты. VPN-шлюз интегрирован с межсетевым экраном для защищенных и открытых соединений, который осуществляет фильтрацию незашифрованного трафика, а также трафика внутри защищенного соединения.

- L2VPN-шлюз (технология L2OverIP) – функция, благодаря которой координатор выполняет защиту магистральных L2 каналов связи. Такая защита может потребоваться, например, для организации работы территориально распределенных ЦОДов (Центров обработки данных) как единого центра.

- Межсетевой экран — функция, благодаря которой координатор выполняет фильтрацию открытых транзитных и локальных сетевых соединений по IP-адресам, протоколам, портам, направлениям соединений и другим параметрам на основании заданных правил. Одновременно координатор может выполнять функции трансляции адресов для проходящего через него открытого трафика

- Сервер IP-адресов — функция, которая в автоматическом режиме обеспечивает взаимодействие защищенных узлов (клиентов и координаторов) как внутри данной виртуальной сети, так и при взаимодействии с другими виртуальными сетями ViPNet. Это возможно благодаря использованию специального протокола динамической маршрутизации VPN-трафика, реализующего обмен информацией о параметрах доступа узлов друг к другу. Данный протокол обеспечивает маршрутизацию VPN-трафика между узлами в сети ViPNet тем методом, который наиболее оптимален для используемого способа подключения узла к сети.

- Маршрутизатор VPN-пакетов — функция, обеспечивающая маршрутизацию транзитного VPN-трафика, проходящего через координатор, на другие защищенные узлы. Маршрутизация осуществляется на основании идентификаторов защищенных узлов, содержащихся в открытой части VPN-пакетов, которая защищена от подделки, и на основании защищенного протокола динамической маршрутизации VPN-трафика. Одновременно выполняется функция трансляции адресов для VPN-трафика, и все пакеты, поступающие на координатор, отправляются на другие узлы от имени IP-адреса координатора.

- Сервер-маршрутизатор — функция, которая обеспечивает доставку на сетевые узлы управляющих сообщений, обновлений ключей и программного обеспечения из программы ViPNet Центр управления сетью, а также обмен почтовых сообщений, передаваемых почтовыми клиентами корпоративной электронной почты ViPNet Деловая почта и Файловый обмен.

- Сервер Открытого Интернета — функция, которая позволяет обеспечить отдельный доступ защищенных узлов в Интернет и к ресурсам защищенной сети ViPNet, если этого требует политика безопасности организации. Защищенные узлы, которые имеют связь с сервером Открытого Интернета, могут работать в одном из двух режимов:

- Доступ к защищенной сети ViPNet при отсутствии подключения к Интернету.
- Доступ в Интернет при отсутствии соединения с защищенными узлами ViPNet.

### Сервисные функции

- DNS-сервер - может использоваться для разрешения (преобразования) символьных имен Интернет в IP-адреса в ответ на собственные запросы и на запросы других сетевых узлов (DNS-клиентов).

- NTP-сервер - может использоваться для синхронизации времени на самом ПАК и на других сетевых узлах (NTP-клиентах).

- DHCP-сервер – может использоваться для динамического назначения IP-адресов сетевым узлам (DHCP-клиентам). Одновременно с выделением IP-адресов DHCP-сервер может назначать дополнительные параметры настройки клиентов, например, IP-адреса шлюза по умолчанию и WINS-серверов.

- DHCP –Relay – может использоваться для перенаправления DHCP –запросов удаленным DHCP- серверам.

### **Сценарии использования**

Совместно с другими программными продуктами из состава комплекса ViPNet VPN, ViPNet Coordinator HW обеспечивает эффективную реализацию множества сценариев защиты информации:

- Построение защищённых каналов связи между офисами компании (Site-to-Site и Multi Site-to-Site).

- Защищенный доступ удаленных и мобильных пользователей.

- Межсетевые взаимодействия.

- Защита магистральных каналов соединяющих ЦОДы.

- Защита беспроводных сетей связи.

- Защита мультисервисных сетей (включая IP-телефонию и видеоконференцсвязь).

- Разграничение доступа к информации в локальных сетях.

- Защищенный контролируемый доступ в Интернет.

- А также любые комбинации перечисленных выше сценариев.

### **Преимущества**

- Количество одновременно установленных соединений через криптошлюз не ограничивается;

- Поддержка работы в современных мультисервисных сетях связи с серверами DHCP, WINS, DNS и преобразованием адресов (NAT, PAT);

- Использование в качестве центра генерации ключей шифрования сертифицированного ФСБ России ПО ViPNet Administrator;

- Низкая стоимость по сравнению с аналогичными по возможностям СЗИ других отечественных компаний.

### **Сертификаты:**

**Сертификат ФСТЭК № 2353** от 26.05.2011. Действителен до 26.05.2020. РД МЭ (3), РД НДВ (3), ТУ (ViPNet Coordinator HW)

**Сертификат ФСТЭК № 3692** от 26.01.2017. Действителен до 26.01.2020. Профиль защиты МЭ (А четвертого класса защиты. ИТ.МЭ.А4.ПЗ). (ViPNet Coordinator HW 4)

**Сертификат ФСБ № СФ/525-2667** от 23.07.2015. Действителен до 23.07.2018. Соответствует требованиям ФСБ России к устройствам типа межсетевые экраны 4 класса защищенности и может использоваться для защиты информации от несанкционированного доступа в информационных и телекоммуникационных системах органов государственной власти Российской Федерации. (ПАК ViPNet Coordinator HW 3)

### **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