



**Аппаратно-программный комплекс шифрования**

## **«Континент» 3.М**

**Защита корпоративных вычислительных сетей по классу КВ2**

Аппаратно-программный комплекс шифрования предназначенный для создания высокозащищенных виртуальных частных сетей (VPN) повышенной безопасности (соответствующих классу КВ2).

Обеспечивает криптографическую защиту информации класса КВ2, при передаче по общим сетям передачи данных в т.ч. сети Интернет (модель нарушителя H5).

### **Применение**

- Объединение локальных сетей территориально распределенной филиальной сети в единую сеть с применением технологии VPN
- Организация безопасной передачи конфиденциальной информации, с использованием сетей общего пользования (интернет)
- Защита корпоративной сети от вредоносного воздействия из внешних сетей
- Разделение доступа между информационными подсистемами организации (сегментация ЛВС)

### **Достоинства**

- Приведение АС в соответствие с требованиями ФСБ России, ФСТЭК России
- Интегрированные средства централизованного управления сетью криптошлюзов
- Централизованное автоматическое управление криптографическими ключами
- Устойчивость к сетевым атакам
- Высокая пропускная способность, до 1 Гбит/с
- Высокая надежность и отказоустойчивость



**Код безопасности**

ГК «Информзащита»

# АПКШ «КОНТИНЕНТ» 3.М

Аппаратно-программный комплекс шифрования предназначенный для создания высокозащищенных виртуальных частных сетей (VPN) повышенной безопасности (соответствующих классу КВ2).

Выполняет функции средства построения VPN сетей, межсетевого экрана и маршрутизатора (крипто-маршрутизатор).

## Сертификаты

- Сертификат ФСБ России подтверждающий соответствие требованиям предъявляемым к средствам криптографической защиты информации класса КВ2 и возможность применения для защиты информации не содержащей сведений составляющих гостайну.
- Сертификат ФСБ России подтверждающий соответствие требованиям предъявляемым к устройствам типа межсетевые экраны по 4 классу защищенности и возможность использования для защиты информации от несанкционированного доступа в информационно-телекоммуникационных системах органов государственной власти РФ.
- Сертификат ФСТЭК России подтверждающий соответствие руководящих документов по 4-му уровню контроля на отсутствие НДВ и 4-му классу защищенности по СВТ.

## Ключевые возможности

- Высокая криптографическая стойкость
- Возможность работы с оптическими каналами связи
- Централизованное, автоматическое управление криптографическими ключами
- Использование оптических каналов связи, упрощает защиту от ПЭМИН
- Прозрачность для любых прикладных протоколов и сетевых сервисов построенных на основе использования стека TCP/IP, включая IP-телефонию и видео-конференц связь
- Защита высокоприоритетного трафика (VoIP и видеоконференции) без потери качества связи
- Поддержка технологии NAT/PAT – обеспечивает сокрытие структуры защищаемых сетей
- Поддержка до независимых 8 зон безопасности
- Возможность организации до 6 зон DMZ
- Поддержка технологии VLAN (802.1Q) – простое встраивание в сетевую инфраструктуру
- Криптографическая защита передаваемых данных в соответствии с ГОСТ 28147-89

### Обслуживание и управление

- Интегрированные средства централизованного управления сетью криптошлюзов
- Возможность создания кластера высокой доступности («горячее» и «холодное» резервирование)
- Интегрированная системы журналирования событий, оповещение администратора о событиям, требующих оперативного вмешательства (НСД)

### «Континент» 3.М платформа IPC-1000F



Высокопроизводительное решение для защиты магистральных каналов крупных компаний

- Производительность МСЭ до 1 Гбит/с
- Производительность VPN до 800 Мбит/с
- Сетевые интерфейсы:  
2x 1000BASE-X оптические  
2x 1000BASE-T Ethernet 10/100/1000 RJ45
- Среднее время наработки на отказ 10 000 часов (MTBF)

### «Континент» 3.М платформа IPC-100



Решение для защиты сетей офисов средних и малых предприятий с территориально-распределенной структурой

- Производительность МСЭ до 400 Мбит/с
- Производительность VPN до 250 Мбит/с
- Сетевые интерфейсы:  
2x 1000BASE-X оптические SFP  
6x 1000BASE-T Ethernet 10/100/1000 RJ45
- Среднее время наработки на отказ 40 000 часов (MTBF)

### О компании «Код Безопасности»

Компания «Код Безопасности» – российский разработчик программных и аппаратных средств, обеспечивающих безопасность информационных систем, а также их соответствие требованиям международных и отраслевых стандартов. «Код Безопасности» входит в группу компаний «Информзащита» – признанного лидера в сфере информационной безопасности – и является преемником её многолетнего опыта в области создания средств защиты информации для государственных и коммерческих заказчиков.



**Код безопасности**  
ГК «Информзащита»

Тел.: +7 (495) 980-2345, E-mail: info@securitycode.ru  
www.securitycode.ru