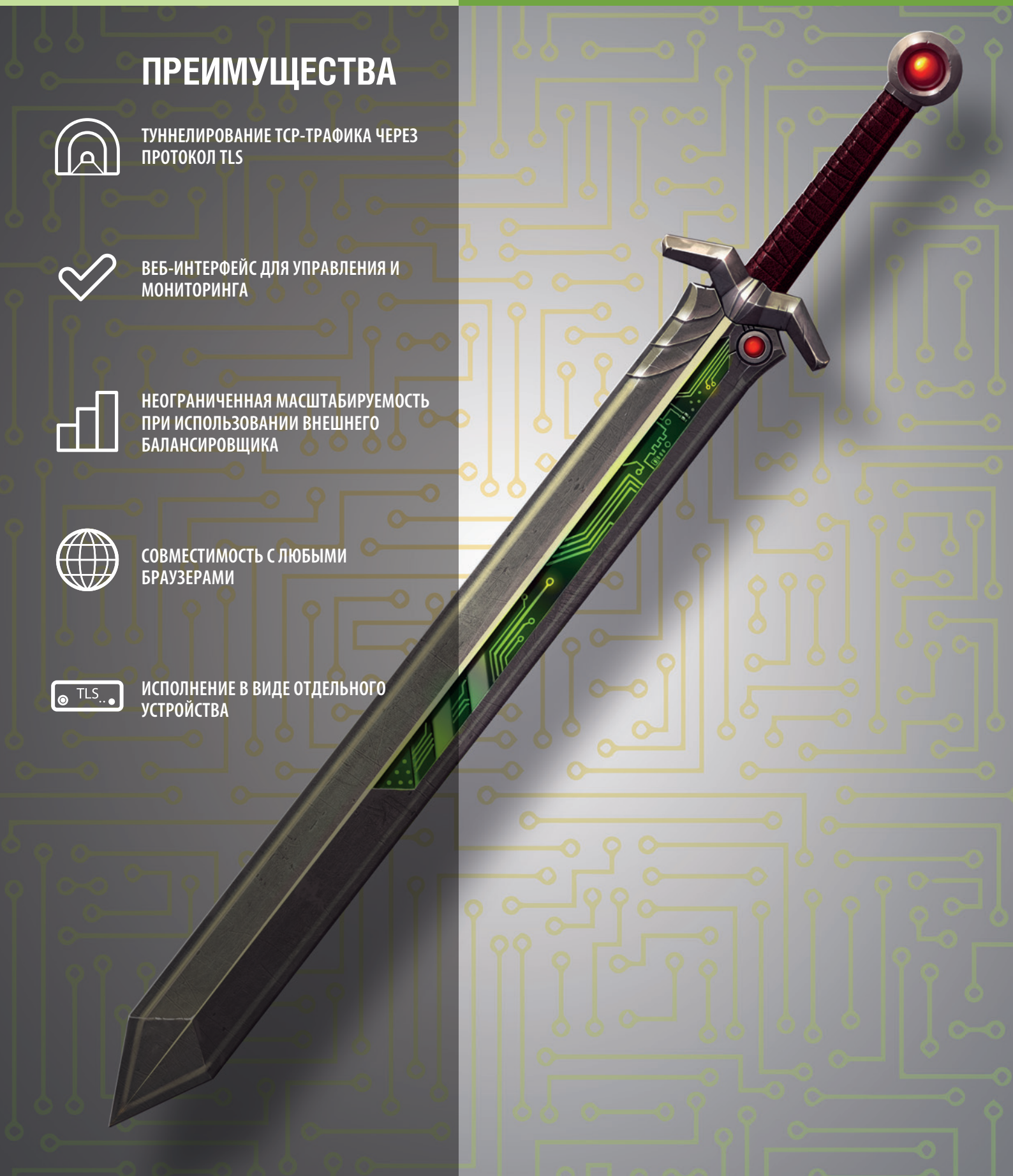
КОД БЕЗОПАСНОСТИ

КОНТИНЕНТ TLS VPN

Сертифицированная система
защищенного удаленного доступа к веб-ресурсам

ПРЕИМУЩЕСТВА

- ТУННЕЛИРОВАНИЕ TCP-ТРАФИКА ЧЕРЕЗ ПРОТОКОЛ TLS
- ВЕБ-ИНТЕРФЕЙС ДЛЯ УПРАВЛЕНИЯ И МОНИТОРИНГА
- НЕОГРАНИЧЕННАЯ МАСШТАБИРУЕМОСТЬ ПРИ ИСПОЛЬЗОВАНИИ ВНЕШНЕГО БАЛАНСИРОВЩИКА
- СОВМЕСТИМОСТЬ С ЛЮБЫМИ БРАУЗЕРАМИ
- ИСПОЛНЕНИЕ В ВИДЕ ОТДЕЛЬНОГО УСТРОЙСТВА



ВОЗМОЖНОСТИ

ШИФРОВАНИЕ

- Криптографическая защита HTTPS-трафика по протоколу TLS
- Поддерживаемые криптоалгоритмы:
  - Шифрование информации производится по алгоритму ГОСТ 28147–89
  - Расчет хэш-функции по алгоритму ГОСТ Р 34.11–94, ГОСТ Р 34.11–2012
  - Формирование и проверка электронной подписи осуществляются в соответствии с алгоритмом ГОСТ Р 34.10–2001, ГОСТ Р 34.10–2012
- Поддерживаемые протоколы:
  - TLS v1.0
  - TLS v1.2
- Возможность работы с различным клиентским ПО:
  - «Континент TLS VPN Клиент»
    - Поддержка туннелирования TCP-трафика через протокол TLS
    - Поддержка работы пользователя в любом браузере
  - «КриптоПро CSP» 3.9/4.0
    - Работа пользователя в браузере Internet Explorer

СЕТЕВЫЕ ВОЗМОЖНОСТИ

- Сокрытие защищаемых серверов (обратный прокси-сервер)
  - К каждой сессии пользователя может быть добавлен произвольный идентификатор
- Работа в режиме кластера с балансировкой нагрузки
  - Неограниченное линейное масштабирование производительности

УПРАВЛЕНИЕ И МОНИТОРИНГ

- Веб-интерфейс для управления и мониторинга
- Интеграция в SIEM-систему по протоколу syslog
- Регистрация событий информационной безопасности, связанных с работой «Континент TLS VPN Клиент»

ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ

- Идентификация и аутентификация пользователей по сертификатам открытых ключей стандарта x.509v3 (ГОСТ Р 31.11–94, 34.10–2001)
- Обоюдная аутентификация пользователя и сервера в процессе установки защищенного соединения
- Проверка сертификатов ключей по спискам отозванных сертификатов (CRL)
- Автоматическая загрузка и обновление Trust-service Status List (TSL)

РЕЖИМЫ РАБОТЫ

- Шифрование HTTP/HTTPS-трафика
- Туннелирование произвольного TCP-трафика через протокол TLS

СЦЕНАРИИ ПРИМЕНЕНИЯ

ВЫСОКОНАГРУЖЕННЫЙ ПОРТАЛ ГОСУДАРСТВЕННЫХ УСЛУГ

Результат:

- Минимизированы затраты на построение и эксплуатацию комплексной системы защищенного доступа к порталу государственных услуг, которая включает в себя:
  - электронную подпись пользовательских транзакций
  - защиту данных при передаче по открытым каналам связи
  - проверку корректности электронной подписи пользователя

СИСТЕМА УДАЛЕННОГО ДОСТУПА К РЕСУРСАМ ПРЕДПРИЯТИЯ

Результат:

- Организован доступ удаленных пользователей к внутренним веб-приложениям
- Обеспечено разграничение доступа удаленных пользователей к различным веб-приложениям
- Обеспечен доступ пользователей к корпоративным ресурсам с помощью толстых программных клиентов (терминалов, клиентов ERP-систем и т.д.)

СООТВЕТСТВИЕ ТРЕБОВАНИЯМ РЕГУЛЯТОРОВ

Результат:

- Информационная система приведена в соответствие требованиям приказа ФСТЭК России № 17 (ГИС)
- Минимизированы затраты на встраивание сертифицированной криптографии в приложения, к которым осуществляется удаленный доступ
- Минимизированы риски, связанные с невыполнением требований регуляторов

МОДЕЛЬНЫЙ РЯД

МОДЕЛЬ	IPC-100	IPC-400	IPC-1000	IPC-1000F	IPC-3000F
					
Производительность в режиме HTTPS-прокси, мбит/с	до 200	до 700	до 900	до 900	до 3000
Количество одновременных подключений	до 500	до 5000	до 10000	до 10000	до 18000
Интерфейсы	6x Ethernet 10/100/1000 2x 1Gigabit Ethernet Fiber SFP	6x Ethernet 10/100/1000	10x Ethernet 10/100/1000	6x Ethernet 10/100/1000 4x 1Gigabit Ethernet Fiber SFP	10x Ethernet 10/100/1000 4x 10G Ethernet Fiber SFP+

СЕРТИФИКАТЫ

ФСТЭК России.

4 уровень контроля отсутствия НДВ.
Применяется для защиты ИСПДн до У31 включительно, ГИС до К1 включительно, АСУ ТП до К1 включительно, АС до класса 1Г включительно.

ФСБ России.

ПАК «Континент TLS VPN Сервер»: СКЗИ КС2
СКЗИ «Континент TLS VPN Клиент»: СКЗИ КС1/КС2

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Техническая поддержка продуктов линейки «Континент» может осуществляться как напрямую, силами специалистов «Код-Безопасности», так и через авторизованных партнеров.
В случае технической поддержки через партнера, партнер обеспечивает первую линию технической поддержки, а в случае сложных вопросов обращается в службу технической поддержки вендора.
Существует несколько пакетов технической поддержки:

Базовый

Стандартный

Расширенный

VIP

КАТАЛОГ УСЛУГ	ПАКЕТ ПОДДЕРЖКИ			
	БАЗОВЫЙ	СТАНДАРТНЫЙ	РАСШИРЕННЫЙ	VIP
Доступность услуги	8x5, e-mail, телефон		24x7, e-mail, телефон	
Приоритет	Низкий	Средний	Высокий	Первоочередной
Количество обращений	Не ограничено			
Консультирование по установке и использованию продукта	●	●	●	●
Доступ на форум по продукту и к базе знаний	●	●	●	●
Доступ к пакетам обновлений	●	●	●	●
Личный кабинет на веб-портале	●	●	●	●
Прием предложений по улучшению продукта	●	●	●	●
Регистрация обращений на веб-портале		●	●	●
Консультирование по дополнительному функционалу продукта			●	●
Выделенный инженер (для проведения работ)				●
Присутствие инженера на площадке заказчика				●

О КОМПАНИИ «КОД БЕЗОПАСНОСТИ»

Компания «Код Безопасности» – лидирующий российский разработчик сертифицированных программных и аппаратных средств, обеспечивающих безопасность информационных систем, а также их соответствие требованиям международных и отраслевых стандартов.

+7 (495) 982-30-20 (многоканальный) info@securitycode.ru www.securitycode.ru