Выпускная квалификационная работа

	PPTP	SSTP	L2TP/IPsec	IKEv2/IPsec	OpenVPN	WireGuard
Компания-разработчик	Microsoft	Microsoft	L2TP — совместная разработка Cisco и Microsoft, IPsec — The Internet Engineering Task Force	IKEv2 — совместная разработка Cisco и Microsoft, IPsec — The Internet Engineering Task Force	OpenVPN Technologies	Jason A. Donenfeld
Лицензия	Proprietary	Proprietary	Proprietary	Proprietary, но существуют реализации протокола с открытым исходным кодом	GNU GPL	GNU GPL
Развертывание	Windows, macOS, iOS, некоторое время GNU/Linux. Работает "из коробки", не требуя установки дополнительного ПО	Windows. Работает "из коробки", не требуя установки дополнительного ПО	Windows,Mac OS X, Linux, iOS, Android. Многие ОС (включая Windows 2000/XP + Mac OS 10.3+) имеют встроенную поддержку, нет необходимости ставить дополнительное ПО	Windows 7+, macOS 10.11+ и большинство мобильных ОС имеют встроенную поддержку	Windows, Mac OS, GNU/Linux, Apple iOS, Android и маршрутизаторы. Необходима установка специализированного ПО, поддерживающего работу с данным протоколом	Windows, Mac OS, GNU/Linux, Apple iOS, Android. Установить сам WireGuard, а затем настроить по руководству
Шифрование	Использует Microsoft Point-to-Point Encryption (MPPE), который реализует RSA RC4 с максимум 128-битными сеансовыми ключами	SSL (шифруются все части, кроме TCP- и SSL-заголовков)	3DES или AES	Реализует большое количество криптографических алгоритмов, включая AES, Blowfish, Camellia	Использует библиотеку OpenSSL (реализует большинство популярных криптографических стандартов)	Обмен ключами по 1-RTT, Curve25519 для ECDH, RFC7539 для ChaCha20 и Poly1305 для аутентификационного шифрования, и BLAKE2s для хеширования
Порты	TCP-порт 1723	TCP-порт 443	UDP-порт 500 для первонач. обмена ключами и UDP-порт 1701 для начальной конфигурации L2TP, UDP-порт 5500 для обхода NAT	UDP-порт 500 для первоначального обмена ключами, а UDP-порт 4500 — для обхода NAT	Любой UDP- или TCP-порт	Любой UDP-порт
Недостатки безопасности	Обладает серьезными уязвимостями. MSCHAP-v2 уязвим для атаки по словарю, а алгоритм RC4 подвергается атаке Bit-flipping	Серьезных недостатков безопасности не было выявлено	3DES уязвим для Meet-in-the-middle и Sweet32, но AES не имеет известных уязвимостей. Однако есть мнение, что стандарт IPsec скомпрометирован АНБ США	Не удалось найти информации об имеющихся недостатках безопасности, кроме инцидента с утечкой докладов АНБ касательно IPsec	Серьезных недостатков безопасности не было выявлено	Серьезных недостатков безопасности не было выявлено

Изм.	Лист	№ докум.	Подп.	Дата
Разраб.		Чернов А.Г.		
Пров.		Сафина М.Р.		
Т. Контр.				
Н. Контр.		Гайсафина Е.Р.		
Утв.				

Сравнение протоколов туннелирования

Лит.	Масса	Масштаб

Лист | Листов 8

МГТУ им Н.Э. Баумана
Кафедра ИУ5
Группа ИУ3-81Б

Инв. № подл. | Подп. и дата | Взам. инв. № | Инв. № дубл. | Подп. и дата