ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 27033-5— 2021

Информационные технологии

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Безопасность сетей

Часть 5

Обеспечение безопасности межсетевого взаимодействия с помощью виртуальных частных сетей (ВЧС)

(ISO/IEC 27033-5:2013, IDT)

Издание официальное

Москва
Стандартинформ
2021

Предисловие

1 ПОДГОТОВЛЕН Федеральным государственным учреждением «Федеральный исследовательский центр «Информатика и управление» Российской академии наук» (ФИЦ ИУ РАН) и Обществом с ограниченной ответственностью «Информационно-аналитический вычислительный центр» (ООО ИАВЦ) на основе собственного перевода на русский язык англоязычной версии стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 022 «Информационные технологии»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 20 мая 2021 г. № 417-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 27033-5:2013 «Информационные технологии. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 5. Обеспечение безопасности межсетевого взаимодействия с помощью виртуальных частных сетей (ВЧС)» [ISO/IEC 27033-5:2013 «Information technology — Security techniques — Network security — Part 5: Securing communications across networks using Virtual Private Networks (VPNs)», IDT].

ИСО/МЭК 27033-5 разработан подкомитетом ПК 27 «Методы и средства обеспечения безопасности ИТ» Совместного технического комитета СТК 1 «Информационные технологии» Международной организации по стандартизации (ИСО) и Международной электротехнической комиссии (МЭК).

При применении настоящего стандарта рекомендуется использовать вместо ссылочных международных стандартов соответствующие им национальные стандарты, сведения о которых приведены в дополнительном приложении ДА.

Дополнительные сноски в тексте стандарта, выделенные курсивом, приведены для понимания текста оригинала

5 ВВЕДЕН ВПЕРВЫЕ

6 Некоторые положения международного стандарта, указанного в пункте 4, могут являться объектом патентных прав. Международная организация по стандартизации (ИСО) и Международная электротехническая комиссия (МЭК) не несут ответственности за идентификацию подобных патентных прав

Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (www.gost.ru)

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины и определения 1
4 Сокращения 2
5 Структура документа 2
6 Обзор 2
6.1 Введение 2
6.2 Типы ВЧС 3
7 Угрозы безопасности информации 4
8 Требования к обеспечению безопасности 4
8.1 Обзор 4
8.2 Конфиденциальность 5
8.3 Целостность 5
8.4 Аутентичность 6
8.5 Авторизация 6
8.6 Доступность 6
8.7 Безопасность конечных точек туннеля 6
9 Меры обеспечения информационной безопасности 6
9.1 Аспекты безопасности 6
9.2 Виртуальные цепи 6
10 Методы проектирования 7
10.1 Обзор 7
10.2 Нормативные и законодательные аспекты 8
10.3 Аспекты управления ВЧС 8
10.4 Архитектурные аспекты ВЧС 8
10.5 Технические аспекты ВЧС 11
11 Рекомендации по выбору продуктов 11
11.1 Выбор протокола передачи данных 11
11.2 Оборудование ВЧС 11
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов национальным стандартам 13
Библиография 14

Введение

Серия ИСО/МЭК 27033 состоит из следующих частей под одним общим заголовком «Информационные технологии. Методы и средства обеспечения безопасности. Безопасность сетей»:

часть 1. Обзор и понятия;

часть 2. Инструкции по проектированию и реализации безопасных сетей;

часть 3. Эталонные варианты реализации сетей. Угрозы, методы проектирования и вопросы управления;

часть 4. Обеспечение безопасного межсетевого взаимодействия между сетями с помощью шлюзов безопасности;

часть 5[1)]. Обеспечение безопасности межсетевого взаимодействия с помощью виртуальных частных сетей (ВЧС[2)]);

часть 6. Обеспечение безопасности беспроводного доступа к IP-сетям.

Примечание — Следует отметить, что могут появиться и другие части. В число возможных тем, которые могут быть в них освещены, входят локальные вычислительные сети, широкополосные сети, веб-хостинг, интернет-почта и маршрутизированный доступ к сторонним организациям. Основные разделы таких частей должны включать «Риски», «Методы проектирования» и «Вопросы управления».

---

1) *Положения настоящего стандарта должны рассматриваться с учетом требований национальных нормативных правовых актов и стандартов Российской Федерации в области защиты информации.*

2) *Далее по тексту используется сокращение ВЧС.*

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Безопасность сетей

Часть 5

Обеспечение безопасности межсетевого взаимодействия с помощью виртуальных частных сетей (ВЧС)

Information technology. Security techniques. Network security.
Part 5. Securing communications across networks using Virtual Private Networks (VPNs)

Дата введения — 2021—11—30

1 Область применения

Настоящий стандарт содержит рекомендации по выбору, реализации и мониторингу технических средств управления, необходимых для обеспечения сетевой безопасности посредством виртуальных частных сетей (ВЧС), используемых для установки сетевых соединений и подключения удаленных пользователей к сетям.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты. Для датированных ссылок применяют только указанное издание, для недатированных — последнее издание (включая все изменения к нему).

ISO/IEC 27001:2005, Information technology — Security techniques — Information security management systems — Requirements (Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования)

ISO/IEC 27002:2005, Information technology — Security techniques — Code of practice for information security controls (Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности)

ISO/IEC 27005:2011, Information technology — Security techniques — Information security risk management (Информационные технологии. Методы и средства обеспечения безопасности. Управление рисками информационной безопасности)

ISO/IEC 27033-1:2009, Information technology — Security techniques — Network security — Part 1: Overview and concepts (Информационные технологии. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и понятия)

3 Термины и определения

В настоящем стандарте применены термины по ИСО/МЭК 7498 (все части), ИСО/МЭК 27000, ИСО/МЭК 27001, ИСО/МЭК 27002, ИСО/МЭК 27005 и ИСО/МЭК 27033-1.

Издание официальное

4 Сокращения

В настоящем стандарте использованы сокращения по ИСО/МЭК 27033-1, а также следующие сокращения:

AH — заголовок аутентификации (authentication header);

ESP — безопасно инкапсулированная полезная нагрузка (encapsulating security payload);

IKE — схема обмена ключами через Интернет (internet key exchange);

IPsec — набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP (Internet Protocol Security);

ISAKMP — протокол ассоциаций безопасности и управления ключами в Интернете (internet security association and key management protocol);

L2F — переадресация на 2-м уровне (протокол) (layer two forwarding);

LDP — протокол распределения меток (label distribution protocol);

MPPE — протокол шифрования данных, используемый поверх соединений PPP (microsoft point-to-point encryption);

MPLS — многопротокольная коммутация по меткам (Multi-protocol Label Switching);

NAS — сетевое хранилище данных (network area storage);

OSI — взаимодействие открытых систем (open systems interconnection);

PPP — протокол двухточечного соединения (point-to-point protocol);

PPTP — туннельный протокол типа «точка-точка» (point-to-point tunneling protocol);

SSL — протокол безопасных соединений (secure sockets layer);

VPLS — сервис виртуальной частной локальной вычислительной сети (virtual private LAN service);

VPWS — сервис проводной частной сети (virtual private wire service);

WAN — глобальная вычислительная сеть (wide area network).

5 Структура документа

Настоящий стандарт содержит следующие разделы:

- обзор виртуальных частных сетей (ВЧС) (раздел 6);
- описание угроз безопасности информации, связанных с ВЧС (раздел 7);
- описание требований безопасности, определяемых на основе анализа угроз безопасности информации, связанных с ВЧС (раздел 8);
- описание мер обеспечения информационной безопасности (ИБ), относящихся к стандартным сетевым сценариям и областям сопряжения сетей и технологий, использующим ВЧС (раздел 9);
- описание методов проектирования ВЧС (раздел 10).

6 Обзор

6.1 Введение

ВЧС получили стремительное развитие как средство межсетевого взаимодействия и способ подключения удаленных пользователей к сетям.

Существует множество определений ВЧС. В самом простом варианте они обеспечивают механизм для создания безопасного канала или каналов передачи данных через существующую сеть либо через соединение типа «точка—точка». Эти каналы предоставляются исключительно ограниченному кругу пользователей и могут быть динамически установлены и удалены по мере необходимости. Хостинговая сеть бывает как частной, так и общедоступной.

На рисунке 1 представлен пример ВЧС с защищенным каналом данных, соединяющим конечного пользователя со шлюзом в общедоступной сети, и защищенным каналом данных, соединяющим два шлюза в общедоступной сети.

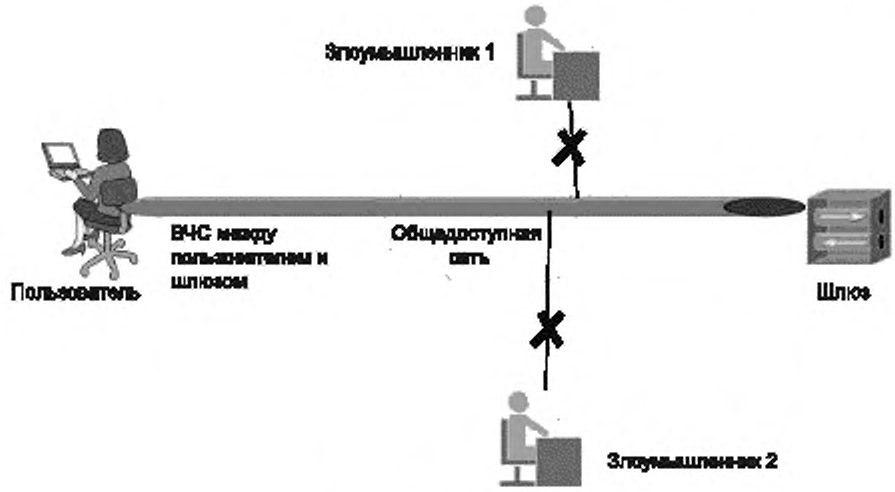

Рисунок 1 — Пример ВЧС

Удаленный доступ с помощью ВЧС реализуется поверх обычного соединения «точка—точка». В первую очередь устанавливается стандартное двухточечное соединение между локальным пользователем и удаленными узлами. Некоторые ВЧС предоставляются как управляемый сервис, в рамках которого в общедоступной инфраструктуре предоставляются защищенный и надежный канал передачи данных, а также средства управления и адресации, эквивалентные тем, что обеспечиваются в частной сети. Поэтому для усиления защиты ВЧС может потребоваться принять во внимание дополнительные меры обеспечения ИБ, как указано в настоящем стандарте.

Данные и код, передаваемые через ВЧС, должны предназначаться только организации, использующей ВЧС, и храниться отдельно от данных и кода других пользователей базовой сети. Данные и код, принадлежащие другим пользователям, не должны передаваться по одному и тому же каналу ВЧС. При оценке объема дополнительных мер обеспечения ИБ, которые могут потребоваться, следует учитывать уровень доверия к конфиденциальности и другие аспекты безопасности организации, владеющей ВЧС или предоставляющей ее.

6.2 Типы ВЧС

Как было сказано выше, существует множество способов описания типов ВЧС.

В архитектуру ВЧС входят:

- двухточечное соединение (например, клиентское устройство, получающее удаленный доступ к сети организации через шлюз сайта или шлюз сайта, подключающийся к другому шлюзу сайта); либо
- соединение типа «точка—облако» (например, реализованное с помощью технологии MPLS).

С точки зрения базовой модели OSI существует три основных типа ВЧС:

- ВЧС второго уровня предлагают смоделированный объект локальной вычислительной сети (ЛВС[1)]), используя подключения ВЧС, проходящие поверх хостинговой сети (например, сети поставщика), для связи сайтов организации или для обеспечения удаленного соединения с организацией. Типичные предложения поставщиков в этой области включают в себя сервис проводной частной сети (VPWS), которая обеспечивает моделируемое проводное соединение, или сервис виртуальной частной локальной вычислительной сети (VPLS), которая обеспечивает более полный моделируемый сервис ЛВС;

- ВЧС третьего уровня предлагают моделируемый объект глобальной вычислительной сети (WAN), вновь с помощью ВЧС, работающих поверх сетевой инфраструктуры. Эти предложения обеспечивают сайты с моделируемым подключением в контексте модели многоуровневой OSI-сети. Основным преимуществом в данном случае является возможность использования частных схем IP-адресации в

[1)] *Далее по тексту используется сокращение ЛВС.*

общедоступной инфраструктуре, что недопустимо в рамках обычного общедоступного IP-подключения. Частные адреса можно использовать поверх общедоступных сетей с помощью протокола преобразования сетевых адресов (NAT). Однако это может затруднить создание и использование соединений ВЧС на основе IPsec. Тем не менее существуют варианты решения этой проблемы;

- для обеспечения безопасности транзакций в общедоступных сетях используются ВЧС более высокого уровня. Как правило, такие сети обеспечивают безопасный канал между соединяющимися приложениями, тем самым гарантируя конфиденциальность и целостность информации во время транзакции. Подобный тип сетей также известен как ВЧС четвертого уровня, поскольку соединение ВЧС обычно устанавливается по протоколу управления передачей (TCP), являющемуся протоколом четвертого уровня.

7 Угрозы безопасности информации

В обозримом будущем организациям следует ожидать все более изощренных атак на свои системы. Попытки несанкционированного доступа могут быть злонамеренными и приводить, среди прочего, к атаке типа «отказ в обслуживании», неправомерному использованию ресурсов или доступу к ценной информации.

Обычно угрозы безопасности информации в отношении ВЧС принимают форму вторжений или атаки типа «отказ в обслуживании» (DoS).

Злоумышленные вторжения могут быть связаны с тем, что постороннее лицо или злоумышленник получает контроль над компонентом сети — компьютером или другим сетевым устройством (в том числе мобильным устройством).

Вторжения могут осуществляться из любой точки, имеющей подключение к (вашей) сети. В качестве источников таких атак могут выступать другие ВЧС, Интернет или базовая сеть самого поставщика услуг. В основе защиты от подобных атак лежит возможность фильтрации нежелательного трафика из нежелательных источников в точках входа в сеть. Один из типичных примеров вторжения — несанкционированный доступ к защищенному туннелю со стороны неавторизованного объекта.

Сложность может возникать в некоторых нецентрализованных модификациях ВЧС, поскольку все узлы соединяются между собой без контроля трафика.

Еще одним типом угроз безопасности информации для ВЧС являются угроза DoS-атаки. Источником DoS-атак и вторжений бывают другие ВЧС, Интернет или базовая сеть поставщика услуг. Основное различие между этими двумя типами атак заключается в том, что для проведения DoS-атак злоумышленнику необходим доступ к одному из сетевых устройств или контроль над ним.

DoS-атаки на устройства поставщиков услуг также могут привести к отказу в обслуживании некоторых компонентов ВЧС. В некоторых случаях будет сложно оградить сеть от DoS-атак, однако главный метод защиты от них заключается в грамотном проектировании ВЧС.

Вопросы обеспечения безопасности ВЧС охватывают:

- выделение адресного пространства и разделение маршрутизации между различными ВЧС посредством сети с коммутацией по меткам;
- обеспечение недоступности внутренней структуры ядра сети с коммутацией по меткам для внешних сетей (например, для ограничения доступа к информации со стороны потенциального злоумышленника);
- обеспечение устойчивости к атакам типа «отказ в обслуживании»;
- обеспечение устойчивости к атакам несанкционированного доступа;
- обеспечение защиты от подделки меток (однако, несмотря на возможность внедрения ложных меток в сеть с коммутацией по меткам извне домашней сети, за счет разделения адресов поддельный пакет может нанести вред только той ВЧС, в которой он был создан).

8 Требования к обеспечению безопасности

8.1 Обзор

Основной целью ВЧС является защита от несанкционированного доступа. В силу этого ВЧС могут использоваться для достижения более широких целей сетевой безопасности:

- для защиты информации в сетях, в системах, подключенных к сетям и используемых этими системами сервисах;

- для защиты поддерживающей сетевой инфраструктуры;
- для защиты систем управления сетью.

Для достижения изложенных выше целей ВЧС следует реализовать таким образом, чтобы обеспечить:

- конфиденциальность данных при передаче между конечными точками ВЧС;
- целостность информации при передаче между конечными точками ВЧС;
- аутентичность пользователей и администраторов ВЧС;
- авторизацию пользователей и администраторов ВЧС;
- доступность конечных точек ВЧС и сетевой инфраструктуры.

Это, в свою очередь, подразумевает необходимость такой реализации базовых туннелей, используемых для создания ВЧС, которая обеспечит достижение целей в сфере безопасности. Эти цели представлены на рисунке 2.

Рисунок 2 — Общие требования безопасности ВЧС, сопоставленные с базовым туннелем

Каждое из этих требований обсуждается более подробно далее.

В разделе 9 также рассматриваются типы мер обеспечения ИБ, используемых для реализации защищенных ВЧС.

8.2 Конфиденциальность

Передаваемые через туннель конфиденциальные данные и код не должны быть скомпрометированы. При использовании туннельных технологий передаваемые данные и код могут быть скрыты от других пользователей сети. Однако это не означает, что трафик остается конфиденциальным. В частности, передаваемые через туннели данные и код не защищены от анализаторов и перехватчиков данных, осуществляющих анализ трафика. Поэтому сохранение конфиденциальности данных и кода при передаче через туннели в решающей степени зависит от вероятности проведения такого анализа. Подобная вероятность служит показателем степени доверия к базовой сети, поддерживающей ВЧС; степень доверия варьируется в зависимости от владельца транзитной сети. Если транзитная сеть не находится в доверенном домене (более подробная информация о доверенных доменах приведена в ИСО/МЭК 27033-1) или если передаваемые данные и код считаются конфиденциальными, то для дальнейшей защиты конфиденциальных данных могут потребоваться дополнительные средства управления. В таких случаях используемые туннельные механизмы должны поддерживать шифрование, либо отправляемые элементы должны быть зашифрованы в автономном режиме перед передачей через ВЧС. Не следует также пренебрегать безопасностью конечных точек туннеля (см. 8.7).

8.3 Целостность

Целостность передаваемых через туннель данных и кода не должна быть нарушена. Механизмы, используемые для создания туннеля в ВЧС, должны поддерживать проверку целостности данных и кода в процессе передачи с помощью таких методов, как коды проверки сообщений, коды аутентификации сообщений и механизмы защиты от воспроизведения. Если такая защита недоступна при использовании туннеля или если передаваемые данные (код) являются особенно секретными, то в конечных системах следует реализовать средства управления защитой целостности и обеспечить подобную защиту сквозным образом, в каждой точке канала.

8.4 Аутентичность

Следует обеспечить аутентичность информации, передаваемой между участниками ВЧС через публичные IP-сети. Реализацию туннеля и процессы его функционирования необходимо поддерживать средствами контроля аутентификации. Эти средства должны гарантировать, что каждая конечная точка туннеля взаимодействует с конечной точкой авторизованного партнера (возможно, системой удаленного доступа), а также то, что полученные данные поступают из надлежащего авторизованного источника.

8.5 Авторизация

Создание туннеля и процесс его функционирования необходимо поддерживать средствами управления авторизацией, а также списками контроля доступа (ACL). Эти средства должны гарантировать, что каждая конечная точка туннеля взаимодействует с конечной точкой авторизованного партнера (возможно, системой удаленного доступа), а также то, что полученные данные поступают из надлежащего авторизованного источника.

8.6 Доступность

Доступность туннелей, а следовательно, и ВЧС зависит от доступности поддерживающей сетевой инфраструктуры и систем в конечных точках. Однако по мере возможности следует включать меры обеспечения ИБ для противодействия атакам типа «отказ в обслуживании», которые характерны для туннельных механизмов.

В случае конкретных соглашений об уровне обслуживания в качестве альтернативы следует рассмотреть вопрос о создании разнообразных и устойчивых туннелей.

8.7 Безопасность конечных точек туннеля

Кроме того, следует учитывать требования безопасности для конечных точек ВЧС. Как правило, каждая конечная точка ВЧС должна гарантировать наличие только контролируемого сетевого трафика между хостинговой сетью и ВЧС. Обычно это подразумевает отключение маршрутизации, а также использование по меньшей мере технологии пакетной фильтрации или межсетевой защиты. Более подробная информация приведена в 10.4.2 и 10.4.3.

9 Меры обеспечения информационной безопасности

9.1 Аспекты безопасности

Хотя туннели скрыты от обычных сетевых пользователей, они не являются невидимыми, а следовательно, не являются защищенными по своей природе. Процесс базового разделения (на виртуальные цепи или пути с коммутацией по меткам) и процесс инкапсуляции, используемый для создания туннеля, не защищены от злоумышленников, применяющих сетевые анализаторы и перехватчики для анализа трафика. Если передаваемые через туннель данные не защищены шифрованием, злоумышленник сможет получить доступ к трафику. Даже при условии применения шифрования будет известно о существовании туннеля и его конечных точек.

Кроме того, конечные точки туннеля не всегда можно защитить от несанкционированного логического и (или) физического доступа. Поэтому для безопасной реализации ВЧС необходимо применять меры обеспечения ИБ туннелей, в зависимости от политики безопасности организации и уровня приемлемости рисков. От политики безопасности организации будет зависеть, являются ли такие уязвимости приемлемыми или нет.

Примечание — Даже если данные зашифрованы, наличие потока данных может иметь не меньшую важность, чем сами передаваемые данные. Ведь если можно определить местоположение конечных точек ВЧС, значит, можно определить и местоположение пользователя. Это создает угрозу частной жизни человека, а в случае деятельности правоохранительных органов или вооруженных сил может поставить под угрозу выполнение ими своей миссии.

9.2 Виртуальные цепи

Меры обеспечения ИБ, устанавливающие базовые защищенные каналы, могут использовать виртуальные цепи в традиционных широкополосных телекоммуникационных системах, например арендованные линии на основе технологий типа Frame Relay или ATM. В этих технологиях базовые сети яв-

ляются, по сути, защищенными в той мере, в какой телекоммуникационные операторы поддерживают разделение между арендуемыми линиями связи для частных абонентов и предоставлением общедоступных интернет-сервисов. Технология, используемая в виртуальных цепях, подразумевает определенную степень конфиденциальности, но не абсолютную безопасность канала. ВЧС, построенная на основе традиционных виртуальных цепей, считается практически не подверженной компрометации, поскольку взломы или атаки обычно происходят в базовой сети поставщика.

10 Методы проектирования

10.1 Обзор

ВЧС проектируются на основе системных ресурсов физической сети, например с помощью технологий шифрования и (или) туннелирования каналов виртуальной сети через реальную сеть.

ВЧС можно реализовать полностью в частной сети под контролем организации-владельца, в общедоступных сетях или с использованием комбинации этих сетей. Существует вполне реальная возможность реализации ВЧС на основе существующих частных глобальных вычислительных сетей (WAN). Однако повсеместное наличие относительно недорогого доступа к Интернету сделало эту публичную сетевую среду экономически эффективным средством поддержки широкополосных ВЧС и ВЧС с удаленным доступом во многих сферах практического применения.

Кроме того, для реализации ВЧС можно использовать защищенные каналы, созданные с помощью туннелей, проходящих через сети поставщиков Интернет-услуг. В этом случае общедоступный Интернет фактически является базовой транспортной системой. Это подразумевает наличие огромной неопределенности в отношении конфиденциальности ВЧС. Туннель представляет собой канал передачи данных между сетевыми устройствами, который устанавливается поверх существующей сетевой инфраструктуры. Туннель обеспечивает прозрачность нормальной работы сети и, в большинстве вариантов практического применения, может использоваться аналогично обычным сетевым соединениям. Его можно с легкостью включать или отключать по мере необходимости без каких-либо изменений в базовой физической сетевой инфраструктуре. Благодаря этому ВЧС, созданная с помощью туннелей, является более гибкой, чем сеть на основе физических соединений.

Туннели могут быть созданы с помощью следующих технологий.

- виртуальных цепей;
- коммутации по меткам;
- инкапсуляции протоколов.

Туннели, создаваемые как виртуальные цепи, как правило, устанавливаются в обычных WAN-системах в качестве выделенных линий с помощью технологий пакетной коммутации (например, Frame Relay или ATM). Данные технологии обеспечивают разделение потоков данных между туннелями.

Коммутация по меткам представляет собой еще один способ создания туннелей. Всем пакетам данных, проходящим в одном туннеле, присваивается одна идентифицирующая метка. Это гарантирует, что пакеты с отличающимися от нее метками будут исключены из указанного сетевого пути.

Несмотря на то что эти методы туннелирования гарантируют правильное разделение данных, проходящих между туннелями и базовыми сетями, они не отвечают общим требованиям к обеспечению конфиденциальности. В целях обеспечения конфиденциальности необходимо использовать технологии шифрования для поддержки должного уровня безопасности.

Туннели ВЧС могут быть созданы на различных уровнях модели OSI. Виртуальные цепи образуют туннели на 2-м уровне. Методы коммутации по меткам позволяют создавать туннели на 2-м или 3-м уровнях. Метод инкапсуляции протокола пригоден для использования на всех уровнях, кроме физического (большинство реализаций расположены на 3-м уровне и выше). Шифрование обеспечивает дополнительный уровень безопасности туннелей, создаваемых на основе технологий виртуальных цепей, коммутации по меткам и инкапсуляции протокола.

Для создания туннелей также применяется метод инкапсуляции протоколов, при котором блок данных одного протокола упаковывается и переносится в другой протокол. Например, упаковка IP-пакета осуществляется посредством туннельного режима протокола IPsec ESP. Вставляется дополнительный IP-заголовок, после чего пакет передается по IP-сети.

10.2 Нормативные и законодательные аспекты

В странах, где будут использоваться ВЧС, следует рассмотреть любые нормативные и законодательные требования в сфере безопасности, касающиеся сетевых подключений и использования ВЧС, как это определено соответствующими регулирующими или законодательными органами (включая национальные правительственные учреждения).

Они охватывают нормативные и (или) законодательные акты, касающиеся:

- конфиденциальности/защиты данных;
- применения технологий шифрования;
- управления операционными рисками/руководства.

10.3 Аспекты управления ВЧС

Изучая вопрос о развертывании ВЧС, все лица, обязанности которых так или иначе связаны с ВЧС, должны четко представлять себе бизнес-требования и преимущества использования ВЧС. Кроме того, эти лица, равно как и остальные пользователи ВЧС, должны быть осведомлены о рисках безопасности и сферах контроля таких соединений. Бизнес-требования и преимущества, скорее всего, повлияют на многие решения и действия, предпринимаемые в процессе анализа возможности использования ВЧС, определения потенциальных сфер контроля, а затем, в конечном счете, при выборе, проектировании, реализации и поддержке мер обеспечения ИБ. Таким образом, эти бизнес-требования и преимущества необходимо учитывать на протяжении всего процесса отбора.

10.4 Архитектурные аспекты ВЧС

10.4.1 Обзор

При выборе ВЧС нужно учитывать следующие архитектурные аспекты:

- безопасность конечной точки;
- безопасность завершения соединения;
- защита от вредоносных программ;
- аутентификация;
- система обнаружения и предотвращения вторжений;
- шлюзы безопасности (межсетевые экраны);
- проектирование сети;
- другие подключения;
- раздельное туннелирование;
- ведение журналов аудита и мониторинг сети;
- управление техническими уязвимостями;
- шифрование маршрутов общедоступной сети.

Каждый из этих аспектов кратко изложен ниже.

10.4.2 Безопасность конечной точки

Функция ВЧС заключается в обеспечении безопасного канала связи в определенной сетевой среде. Пока установлена ВЧС, невозможно контролировать содержимое потока данных. Если одна из конечных точек взломана, то может быть скомпрометирован весь сеанс связи по ВЧС. Безопасность конечных точек применяется не только к самим устройствам, но и к установленным на них приложениям, а также к процедурным/физическим аспектам, связанным с их использованием.

Для того чтобы обеспечить бесперебойную работу системы безопасности конечных точек, следует свести к минимуму количество агрегирующих конечных точек.

Некоторые устройства конечных пользователей (например, мобильное/рабочее вычислительное оборудование), используемые для удаленного доступа, могут лежать вне зоны действия средств управления ВЧС. В разные моменты времени эти устройства могут подключаться к различным сетям, например для получения доступа к Интернету и частной сети организации. Эти сети несут дополнительные риски, поэтому следует рассмотреть вопрос о применении соответствующих средств управления. Изучая вопрос о безопасности таких конечных устройств, следует принимать во внимание меры обеспечения ИБ, предусмотренные ИСО/МЭК 27002, включая те из них, что связаны:

- с безопасностью оборудования;
- защитой от вредоносного и мобильного кода;
- информированием, повышением осведомленности и обучением персонала, использующего эти устройства, вопросам информационной безопасности;
- управлением техническими уязвимостями устройств и связанной с ними технологией ВЧС.

Следует принять во внимание другие средства управления, например фильтр пакетов или персональный межсетевой экран.

10.4.3 Безопасность завершения соединения

Одним из ключевых факторов, влияющих на безопасность ВЧС, является способ завершения соединения в каждой конечной точке. Если завершение соединения происходит непосредственно в ядре конечной точки (например, в безопасной зоне сети), то безопасность напрямую зависит от безопасности удаленного партнера. Если точка завершения соединения находится в незащищенной зоне, вполне вероятно, что злоумышленник сможет с легкостью осуществить подмену соединения.

Стандартный метод завершения соединения ВЧС — установка выделенных конечных точек ВЧС в периметровой сети. Это дает возможность дальнейшей обработки информации из ВЧС (например, если принято решение о предоставлении доступа к приложениям/системам в защищенной зоне). Потенциально завершение соединения в промежуточной зоне обеспечивает надежный контроль ВЧС и ее пользователей.

Примечание — Промежуточная зона будет описана в качестве периметровой сети или демилитаризованной зоны в ИСО/МЭК 27033-4.

В любом случае конечная точка ВЧС перед разрешением доступа должна аутентифицировать объект (например, пользователя или устройство). Это осуществляется в дополнение к аутентификации, выполняемой между конечными точками для установки соединения ВЧС. Например, для пользователей это обычно предполагает ввод имени пользователя и пароля. Также может потребоваться использование дополнительного метода аутентификации (так называемой строгой аутентификации), например токена, карты или системы биометрии.

10.4.4 Защита от вредоносных программ

Если информационные системы не содержат вредоносного программного обеспечения, то единственным способом внедрения такого кода являются данные, выполняемые получателем (например, код). Многие программы допускают возможность незаметного встраивания кода (скрипта) в данные. Конечные точки ВЧС предлагают надежные средства управления, позволяющие реализовать защиту от вредоносного программного обеспечения и контролировать передачу такого кода.

Дополнительная информация о защите от вредоносного кода, включая вирусы, червей и троянов, приведена в ИСО/МЭК 27002.

Примечание — Следует предусмотреть положение о кодах принуждения, чтобы обеспечить безопасность конечных точек, особенно в тех случаях, когда может быть задействована особо конфиденциальная информация. В целях защиты скомпрометированного конечного пользователя код принуждения, возможно, должен обеспечивать доступ. Однако его использование может повлечь за собой необходимость ведения дополнительных записей в журнале и отслеживания, а также оповещения соответствующих руководителей о ситуации.

10.4.5 Аутентификация

Аутентификация является одним из ключевых этапов создания ВЧС. При необходимости каждая сторона должна пройти аутентификацию у предполагаемого партнера сессии (т. е. необходима взаимная аутентификация). Такая аутентификация может быть выполнена несколькими способами:

- использование предварительных ключей. Это удобно, поскольку после установки соединения контроль больше не потребуется. Однако, если такие ключи будут скомпрометированы, они могут стать предметом злоупотреблений (например, в случае атаки методом посредника);
- использование сертификатов. Это повышает гибкость и масштабируемость развертывания, особенно при использовании PKI для более простого управления ключами, их отзыва и перевыпуска. Дополнительная информация об аутентификации и использовании для нее сервисов на основе технологий шифрования приведена в ИСО/МЭК 11770-1 и ИСО/МЭК 27002.

10.4.6 Система обнаружения и предотвращения вторжений (СОПВ)

Следует рассмотреть необходимость использования системы обнаружения и предотвращения вторжений (СОПВ). СОПВ может быть внедрена на обеих конечных точках ВЧС для обнаружения возможных вторжений. Можно использовать любой подходящий механизм для создания оповещений системы обнаружения вторжений (СОВ), их фиксации в журнале и управления ими как частью аудиторского следа. Следует отметить, что даже некоторые персональные межсетевые экраны могут играть роль простой системы предотвращения вторжений (СПВ), запрещающей сетевой доступ к неавторизованным приложениям.

Дополнительная информация о СОВ приведена в ИСО/МЭК 27039.

10.4.7 Шлюзы безопасности

Следует внимательно рассмотреть вопрос о выборе подходящего шлюза безопасности (включая межсетевой экран) для поддержки развертывания ВЧС.

Информация о шлюзах безопасности (включая межсетевые экраны) содержится в ИСО/МЭК 27033-4.

10.4.8 Проектирование сети

При проектировании сети в обеих конечных точках ВЧС необходимо обеспечить безопасное завершение соединения, о котором говорилось выше. В частности, соединение ВЧС следует завершать либо на внешнем межсетевом экране (например, в периметровой сети), либо в пределах собственной демилитаризованной зоны.

10.4.9 Другие возможности подключения

Следует рассмотреть дополнительные возможности подключения конечной точки ВЧС. Если на одной из конечных точек ВЧС имеется другое подключение, возможно, посредством его взлома могут быть атакованы как локальные, так и — через ВЧС — удаленные системы. Эту возможность атаки можно минимизировать путем правильного проектирования сети и использования межсетевых экранов. Однако наиболее эффективным средством управления является исключение ненужных подключений. Это особенно важно при наличии модемов на удаленных/домашних системах.

Особое внимание следует уделять подключению сетей внутри организации и сторонних компаний, предоставляющих, в частности, услуги технической поддержки и устранения неполадок. В соглашениях с поставщиками услуг необходимо предусмотреть меры обеспечения ИБ среды, в которой он работает. Такие средства должны обеспечить физическое и логическое разделение среды от других операций поставщика услуг и клиентской среды.

10.4.10 Раздельное туннелирование

По возможности следует избегать раздельного туннелирования. Под раздельным туннелированием понимается способность одного соединения (обычно через Интернет) поддерживать ВЧС и другое соединение (например, ВЧС или иное). В этой ситуации возникает риск того, что произойдет взлом удаленной сети посредством атак, выполняемых через другой туннель, по аналогии с персональным компьютером с двумя сетевыми картами, осуществляющими маршрутизацию между двумя сетями. В большинстве случаев раздельного туннелирования можно избежать, если за сетевое подключение будут отвечать системы ВЧС.

10.4.11 Ведение журналов аудита и мониторинг сети

Как и другие технологии безопасности, выбранное ВЧС-решение должно обеспечивать ведение журналов аудита для анализа всех действий на конечном устройстве. Как и другие журналы аудита, генерируемые сетью, они должны быть проверены на наличие признаков инцидентов ИБ.

Следует позаботиться о том, чтобы журналы аудита сами по себе были защищены от злоупотреблений и повреждений, насколько это соответствует оцениваемому риску. В случаях, когда журналы аудита будут использоваться в судебных разбирательствах, их целостность должна быть доказана при отсутствии разумных сомнений.

10.4.12 Управление вопросами технической уязвимости

Сетевые среды, как и другие сложные системы, не защищены от сбоев. Технические уязвимости присутствуют и создаются в стандартных компонентах, используемых в сетях типа ВЧС. Использование этих технических уязвимостей может иметь серьезные последствия для безопасности ВЧС, что чаще всего сказывается на доступности и конфиденциальности. Таким образом, управление техническими уязвимостями должно осуществляться на всех устройствах ВЧС.

10.4.13 Шифрование маршрутов общедоступной сети

Маршрутизация через ненадежную сеть третьей стороны по статическому туннелю делает ВЧС уязвимыми к сетевому анализу. Как упоминалось в 9.1, даже если используется шифрование данных, все равно можно обнаружить существование туннеля и его конечных точек.

В архитектурах ВЧС, где требуется маскировка конечных точек, необходимы средства управления для маскировки исходных и конечных точек пользователей ВЧС. Реализация этих средств управления — изначально непростая задача, поскольку оператор ВЧС не контролирует ненадежную сеть третьей стороны. Существуют технологии, которые обеспечивают маскировку IP-адреса источника и получателя в сети третьей стороны, например виртуальные прокси и многослойный маршрутизатор. Прежде чем внедрять такие инструменты, необходимо обсудить и согласовать юридические аспекты их использования с провайдерами сетей третьей стороны.

10.5 Технические аспекты ВЧС

10.5.1 Вводная информация

Безопасная реализация ВЧС требует систематического рассмотрения элементов, определенных в целях. В частности, следует проанализировать следующие аспекты:

- выбор протокола передачи данных;
- аппаратное и программное обеспечение;
- управление устройствами ВЧС;
- мониторинг безопасности ВЧС.

Каждый из этих аспектов изложен ниже.

10.5.2 Управление устройствами ВЧС

Следует обеспечивать надлежащее управление устройствами ВЧС. Управление устройствами ВЧС — это общий термин для процессов, необходимых для настройки и мониторинга устройств ВЧС. Как и для любого другого сетевого устройства, настройка устройства ВЧС состоит из задания его параметров в соответствии с конфигурацией сети и требуемым уровнем доступа к порту/приложению, установки сертификатов (например, для ВЧС более высокого уровня), а также непрерывного мониторинга сети устройства ВЧС. Развертывание ВЧС с использованием переносных носителей, таких как компакт-диски, дискеты и т. д., следует в обязательном порядке контролировать (например, необходимо создавать журнал (журналы) отправки и получения, вводить ограничения на повторное использование носителей, например контролировать дату/время истечения их срока действия или лимитировать число операций, выполняемых с ними).

10.5.3 Мониторинг безопасности ВЧС

ВЧС, особенно при использовании в качестве каналов удаленного доступа к корпоративным сетям, могут порождать специфические проблемы в сфере сетевой безопасности, если организация не будет должным образом контролировать их работу и управлять ею. Следует уделять внимание самому туннелю, его конечным точкам, а также данным и коду, проходящим через туннель, с тем чтобы исключить возможность легкого доступа в сеть для злоумышленников.

Для сохранения эффективности мер обеспечения сетевой безопасности следует проводить систематический мониторинг средств защиты, включая ВЧС, а также предоставлять менеджерам или администраторам сетей возможность выявлять и фактические или предполагаемые инциденты ИБ и реагировать на них.

Кроме того, должно быть реализовано одно или несколько из указанных ниже решений:

- система обнаружения вторжений;
- предупреждение об инцидентах ИБ;
- журналы безопасности/аудита;
- регулярные проверки;
- обучение пользователей методам выявления и информирования об инцидентах ИБ.

Важно также осознавать динамический характер концепции сетевой безопасности. Поэтому очень важно, чтобы специалисты по ИБ были в курсе актуальных событий в этой области, а ВЧС и поддерживающие технологии работали с новейшими исправлениями и обновлениями в области безопасности, предлагаемыми поставщиками.

11 Рекомендации по выбору продуктов

11.1 Выбор протокола передачи данных

Необходимо выбрать подходящий безопасный протокол передачи данных с учетом следующего:

- потребности деятельности организации;
- совместимости (официальный стандарт или собственный проприетарный стандарт);
- восприятие рынка;
- известные уязвимости;
- надежность.

11.2 Оборудование ВЧС

Следует рассмотреть возможность использования ВЧС-оборудования. В небольших ВЧС (например, при подключении одного пользователя к центральной системе) функциональность ВЧС можно

реализовать программными средствами — этого будет вполне достаточно. Однако во многих ситуациях использование специального ВЧС-оборудования может дать огромные преимущества, например позволит упростить управление или обеспечить работу на более защищенной платформе. Кроме того, может потребоваться определенная платформа аутентификации (например, каталог, PKI или RADIUS), которая позволит, например, подключаться к центральному узлу только авторизованным пользователям.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ISO/IEC 27001:2005	IDT	ГОСТ Р ИСО/МЭК 27001—2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»
ISO/IEC 27002:2005	IDT	ГОСТ Р ИСО/МЭК 27002—2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности»
ISO/IEC 27005:2011	—	*
ISO/IEC 27033-1:2009	IDT	ГОСТ Р ИСО/МЭК 27033-1—2011 «Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции»

* Соответствующий национальный стандарт отсутствует. До его принятия рекомендуется использовать перевод на русский язык данного международного стандарта.

Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов:

- IDT — идентичный стандарт.

Библиография

[1] ISO/IEC 11770-1, Information technology. Security techniques. Key management. Part 1: Framework

[2] ISO/IEC 27039, Information technology. Security techniques. Selection, deployment and operations of intrusion detection systems (IDPS)

[3] ISO/IEC 27033-2, Information technology. Security techniques. Network security. Part 2: Guidelines for the design and implementation of network security

[4] ISO/IEC 27033-3, Information technology. Security techniques. Network security. Part 3: Reference networking scenarios. Threats, design techniques and control issues

[5] ISO/IEC 27033-4, Information technology. Security techniques. Network security. Part 4: Securing communications between networks using security gateways

УДК 006.354:004.056.5 ОКС 35.040

Ключевые слова: методы и средства обеспечения безопасности, безопасность сетей, межсетевое взаимодействие, виртуальные частные серверы

Технический редактор *И.Е. Черепкова*
Корректор *И.А. Королева*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 24.05.2021. Подписано в печать 31.05.2021. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 2,32. Уч.-изд. л 1,90.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении во ФГУП «СТАНДАРТИНФОРМ»
для комплектования Федерального информационного фонда стандартов
117418 Москва, Нахимовский пр-т, д. 31, к. 2.
www.gostinfo.ru info@gostinfo.ru