УДК 004 **Информационные технологии**

Акимин Олег Викторович, *студент,*
Студент ФГБОУ ВО Донской государственный технический университет

ПРОТОКОЛЫ ЗАЩИЩЕННОЙ СВЯЗИ

Аннотация: В современном взаимосвязанном мире передача данных по различным каналам связи имеет важное значение для бизнеса, правительств и частных лиц. Однако по мере того, как данные передаются по сетям и Интернету, они становятся уязвимыми для перехвата и несанкционированного доступа. Протоколы защищенной связи играют жизненно важную роль в защите данных во время передачи, обеспечивая конфиденциальность, целостность и подлинность. В статье описывается исследуется значение протоколов защищенной связи, их принципы, преимущества и их роль в защите данных при их передаче по сетям.

Ключевые слова: информационная безопасность, протоколы, передача данных, канал связи.

Annotation: In today's interconnected world, the transmission of data across multiple communication channels is essential for businesses, governments and individuals. However, as data travels across networks and the Internet, it becomes vulnerable to interception and unauthorized access. Secure communication protocols play a vital role in protecting data in transit by ensuring confidentiality, integrity, and authenticity. The article describes the importance of secure communication protocols, their principles, advantages and their role in protecting data during its transmission over networks.

Keywords: information security, protocols, data transfer, communication channel.

Протоколы защищенной связи - это наборы правил и алгоритмов, разработанных для установления защищенных соединений между взаимодействующими сторонами. Они шифруют данные во время передачи, делая их нечитаемыми для неавторизованных пользователей. Двумя распространенными протоколами защищенной связи являются Secure Sockets Layer (SSL) и Transport Layer Security (TLS), которые используются для безопасного обмена данными через Интернет, особенно для просмотра веб-страниц и служб электронной почты [1].

Принципы защищенных протоколов связи

1. Шифрование данных: Одним из основных принципов защищенных коммуникационных протоколов является шифрование данных. Перед передачей данные шифруются с использованием сложных криптографических алгоритмов, что делает их неразборчивыми для подслушивающих устройств.

2. Целостность данных: Защищенные протоколы связи обеспечивают целостность данных, обнаруживая любые несанкционированные изменения или подделку во время передачи. Любые изменения, внесенные в данные, обнаруживаются и отклоняются принимающей стороной.

3. Аутентификация: механизмы аутентификации проверяют личность взаимодействующих сторон, гарантируя, что обмен данными осуществляется только между законными и доверенными субъектами.

4. Прямая секретность: Прямая секретность является важнейшим принципом, который гарантирует, что даже в случае компрометации закрытого ключа в будущем ранее переданные данные останутся защищенными и недоступными [2].

Преимущества защищенных коммуникационных протоколов

1. Конфиденциальность данных: Протоколы защищенной связи шифруют данные во время передачи, защищая их от перехвата и несанкционированного доступа, тем самым обеспечивая конфиденциальность данных.

2. Защита от подслушивания: Защищенные протоколы связи не позволяют злоумышленникам отслеживать и перехватывать конфиденциальную

информацию по мере ее передачи по каналам связи.

3. Целостность данных: Обеспечивая целостность данных, протоколы защищенной связи защищают от подделки данных и несанкционированных модификаций, гарантируя, что полученные данные не отличаются от оригинала.

4. Доверие и уверенность пользователей: Внедрение защищенных протоколов связи вселяет доверие и уверенностьпользователям, гарантируя им, что их данные защищены и безопасны во время передачи [3].

Роль протоколов защищенной связи в защите данных во время передачи [4]

1. Безопасные онлайн-транзакции: Защищенные коммуникационные протоколы, такие как SSL и TLS, жизненно важны для обеспечения безопасности онлайн-транзакций, таких как покупки в электронной коммерции и онлайн-банкинг, путем шифрования конфиденциальной платежной информации.

2. Защищенная переписка по электронной почте: Протоколы защищенной связи используются для защиты переписки по электронной почте, гарантируя, что конфиденциальная информация остается конфиденциальной во время передачи.

3. Защита просмотра веб-страниц: протоколы SSL/TLS обеспечивают безопасность сеансов просмотра веб-страниц, защищая личные данные пользователей, учетные данные для входа в систему и другую конфиденциальную информацию от потенциальных хакеров.

4. VPN и удаленный доступ: Виртуальные частные сети (VPN) используют защищенные протоколы связи для создания зашифрованных туннелей, позволяющих удаленным пользователям безопасно получать доступ к корпоративным сетям.

5. Обмен данными в IoT: Защищенные коммуникационные протоколы необходимы в экосистеме Интернета вещей (IoT) для защиты данных, которыми обмениваются подключенные устройства, и обеспечения конфиденциальности и безопасности [5].

Вывод

В заключение следует отметить, что протоколы защищенной связи играют важнейшую роль в защите данных во время передачи. Придерживаясь таких принципов, как шифрование данных, целостность данных, аутентификация и прямая секретность, эти протоколы гарантируют, что конфиденциальная информация остается конфиденциальной, аутентичной и защищенной от несанкционированного доступа при ее передаче по каналам связи. Использование защищенных коммуникационных протоколов жизненно важно для обеспечения безопасности онлайн-транзакций, общения по электронной почте, просмотра веб-страниц, VPN и обмена данными в IoT. Внедрение защищенных протоколов связи имеет важное значение для предприятий, организаций и частных лиц, стремящихся защитить свои ценные данные и сохранить доверие пользователей во взаимосвязанном и управляемом информацией мире.

Библиографический список:

1. Петренко С. Защищенная виртуальная частная сеть: современный взгляд на защиту конфиденциальных данных // Мир Internet. М. 2001. № 2.

2. Файльнер М. Виртуальные частные сети нового поколения LAN // Журнал сетевых решений. М. 2005. № 11.

3. Фратто М. Секреты виртуальных частных сетей. Сети и системы связи // Emergent Actors in World Politics: How States and Nations Develop and Dissolv. Princeton University Press. 1997. № 3.

4. Иванов М. А. Криптографические методы защиты информации в компьютерных системах и сетях. М. КУДИЦ-Образ. 2001.

5. Колесников О. Linux: создание виртуальных частных сетей (VPN): пер. с англ. / О. Колесников, Б. Хетч. М. КУДИЦ-Образ. 2004. 459 с.