И.А. СТЕПИН
(ОАО «ВТИ», г. Москва, Россия)

ИСПОЛЬЗОВАНИЕ OPENSSL-ПРОТОКОЛА ШИФРОВАНИЯ В SCADA-СИСТЕМАХ

На сегодняшний момент на рынке SCADA-системы (Supervisory Control and Data Acquisition) – системы диспетчерского управления и сбора данных – представлены как системы с открытым исходным кодом (open-source), так и закрытые системы. На современном этапе развития АСУТП для полноценной работы необходимо построение распределенных промышленных сетей с использованием различных протоколов передачи данных.

Одним из таких протоколов, обеспечивающих более безопасное использование при удаленных соединениях в SCADA-системах, является протокол шифрования SSL (Secure Socket Layers). Если рассмотреть всю классификацию сетевых протоколов – теоретическую модель OSI (Open Systems Interconnection Basic Reference Model) – базовая эталонная модель взаимодействия открытых систем, то использование SSL-протокола осуществляется на сеансовом уровне, который отвечает за создание и закрытие сеанса связи между различными точками.

Наиболее распространенной реализацией протокола SSL является криптографический пакет с открытым исходным кодом OpenSSL. Ввиду последних событий, связанных с обнаруженной в одной из последних версий OpenSSL ошибкой[1], позволяющей получить доступ к внутренней информации, возникает вопрос целесообразности использования данного протокола.

Рассмотрим преимущества и недостатки SCADA-систем.

ПРЕИМУЩЕСТВА

Системы с открытым исходным кодом:

1) открытый код системы позволяет разработчику более гибко настраивать систему, добавлять свои части кода, находить недочеты в уже написанном коде;

2) совместимость с большим количеством технических средств. Это также связано с открытостью кода системы. Разработчик может сам написать для своего проекта дополнительный модуль.

Закрытые системы:

1) широкий выбор. Большинство компаний, разрабатывающих SCADA-системы, предпочитают закрытость своих проектов ввиду интеллектуальной собственности.

2) техническая поддержка. В сложных ситуациях покупатель может обратиться к разработчику системы за помощью.

[1] http://ru.wikipedia.org/wiki/Heartbleed.

НЕДОСТАТКИ

Системы с открытым исходным кодом:

1) ограниченный выбор. Обычно используются для более простых технических решений;

2) сложность настройки. Обычно используют компании, имеющие собственного программиста.

Закрытые системы:

1) полностью закрытый код не дает гибкости настройки и не позволяет самостоятельно устранить возможные ошибки;

2) отдельно стоит рассмотреть стоимость данных систем. Закрытые системы требуют бо́льших затрат, ввиду, с одной стороны, необходимости технической поддержки, а с другой – наличия определенных гарантии от разработчика.

Преимущества и недостатки систем сведены в таблицу, приведенную ниже.

Тип SCADA	Преимущества	Недостатки
Системы с открытым исходным кодом	Открытый код системы. Совместимость с большим количеством технических средств	Сложность в настройке. Ограниченный выбор
Закрытые системы	Широкий выбор. Наличие технической поддержки	Полностью закрытый код

Таким образом, у каждой системы есть свои плюсы и минусы. Но одним из главных критериев при выборе системы должна быть безопасность использования. Отсюда можно сделать вывод, что системы с открытым исходным кодом не гарантируют безопасность, но позволяют ее проверить сообществом пользователей, а разработчики закрытых систем предоставляют определенные гарантии безопасности.