Специализированные межсетевые экраны для АСУ ТП: нюансы применения

Интерес к теме обеспечения информационной безопасности промышленных объектов в целом и автоматизированных систем управления технологическими процессами (АСУ ТП) в частности не угасает уже несколько лет, скорее, даже нарастая со временем. В России актуальность темы признается на высоком государственном уровне, доказательством чему могут служить принимаемые нормативные документы и ведущиеся общественные дискуссии.

Алексей Комаров, *региональный представитель в Москве*
Уральский центр систем безопасности
akomarov@ussc.ru

Широкое обсуждение и освещение темы безопасности промышленных объектов в нашей стране, к сожалению, не приводит к появлению большого количества реальных апробированных на практике подходов к обеспечению ИБ для АСУ ТП: на данный момент их не так много. Помимо явно недостаточной экспертизы свою роль в этом играет и малое разнообразие имеющихся специализированных продуктов для защиты промышленных сетей от информационных угроз, что зачастую приводит к идее (необходимости) использовать стандартные решения, широко распространенные в классических офисных сетях. Вместе с хорошим пониманием принципов работы таких решений неизбежно в мир технологических процессов разработчиками систем обеспечения информационной безопасности вносятся классические же подходы, никак не учитывающие реальные особенности промышленных объектов. Первые технико-коммерческие предложения по теме обеспечения безопасности ключевых систем информационной инфраструктуры от некоторых интеграторов несколько лет назад в части описания предлагаемых технических решений и вовсе походили, например, на предложения по обеспечению безопасности персональных данных с замененными титульными листами.

С течением времени ситуация, безусловно, меняется к лучшему: появляются действительно работающие подходы к обеспечению информационной безопасности АСУ ТП, находящие признание как в среде автоматизаторов, так и у специалистов по информационной безопасности на предприятиях. Расширяется и спектр доступных специализированных решений, в том числе, к слову, и отечественного производства.

Одним из наиболее богатых с точки зрения разнообразия среди средств обеспечения безопасности для промышленных сетей, пожалуй, является сегмент специализированных межсетевых экранов для АСУ ТП. Действительно, международные стандарты и лучшие практики рекомендуют выполнять сегментирование сети, обеспечивая предотвращение сетевых штормов (например, при выходе оборудования из строя) и защиту критических сегментов сети от распространения вредоносного программного обеспечения и несанкционированного доступа внутренних или внешних злоумышленников.

С точки зрения специализации, то есть ориентированности именно на промышленное применение, в качестве основных отличий таких межсетевых экранов от офисных решений выделяют конструктивные особенности и функциональные возможности. Некоторые из них представлены в таблице. На практике ни одно из решений не обладает сразу всеми перечисленными особенностями, и выбор конкретной модели

в любом случае всегда будет представлять собой компромисс между желаемым и возможным.

Промышленное исполнение безусловно важно, ведь на производственных объектах действительно могут быть сложные климатические условия, но в таком исполнении доступны и отдельные модели обычных межсетевых экранов широкого профиля применения. Часто они получают обозначения Military, Rugged или схожие – так называемые SCADA Editions.

С другой стороны, промышленное исполнение удорожает конечный продукт, и в каких-то случаях более экономически оправданным вполне может оказаться использование климатических шкафов или такое проектирование топологии, при котором не потребуется устанавливать дорогостоящее оборудование в помещениях с тяжелыми условиями эксплуатации.

Важнейшим же с точки зрения именно информационной безопасности функциональным отличием обычно считают поддержку промышленных протоколов с дополнительной глубокой инспекцией трафика (Deep Packet Inspection – DPI). Поддержка DPI означает контроль не только IP-адресов отправителя и получателя, портов, MAC-адресов объектов, но и возможность установки углубленных проверок полезной нагрузки пакетов вплоть до задания правил для каждой возможной пары «отправитель – получатель».

В теории такой подход позволяет очень гибко настроить правила фильтрации пакетов вплоть до запрета конкретных команд управления в случае поступления их, например, не из заданного сегмента сети или с несанкционированного рабочего места. На практике же существует целый ряд ограничений.

Во-первых, универсальных решений с одновременной поддержкой множества протоколов не существует, поэтому каждая ситуация будет уникальной в своем роде, требуя подбора под конкретный объект отдельного решения. В случае же применения в промышленной сети нескольких протоколов и вовсе может потребоваться набор продуктов, каждый из которых обладает своими особенностями подключения, настройки, управления и, что немаловажно, своим прайс-листом и политикой лицензирования.

Таблица. ***Некоторые указываемые производителями отличия специализированных промышленных межсетевых экранов от офисных решений***

Конструктивные особенности	● пыле-/влагозащищенность ● безвентиляторное исполнение ● работа в условиях повышенной влажности ● расширенный температурный диапазон ● устойчивость к электромагнитным наводкам ● питание от постоянного тока (9 В–48 В) ● специализированное крепление (DIN-рейка) ● наличие специализированных разъемов (RS232/485)
Конструктивно-функциональные особенности	● быстрое восстановление конфигураций с физических носителей (карты памяти или USB) ● физическая кнопка отключения/изменения режимов работы
Функциональные особенности	● упрощенный интерфейс управления ● длительное время безобслуживаемой работы ● корректная работа со специфическим трафиком (значительное число пакетов в секунду при небольшом их размере) ● глубокая поддержка промышленных протоколов

Вторым важным обстоятельством является высокая сложность настройки выбранного специализированного межсетевого экрана под конкретный технологический процесс. Для корректной настройки такого класса решений потребуется тесное взаимодействие со специалистами, хорошо понимающими суть технологических процессов, но не в представлении интерфейса системы управления или на уровне показаний конкретных датчиков и технологических параметров установок, а с точки зрения сетевого трафика и передаваемых пакетов с командами управления. При достаточно сложном технологическом процессе потребуется очень тонкая и длительная настройка межсетевого экрана, учитывающая нюансы всех возможных штатных и нештатных режимов работы.

Безусловно, такая работа может быть проведена, но с учетом имеющегося на сегодняшний день инструментария она будет достаточно затратной по ресурсам (человеческим и временным) и крайне слабо масштабируемой из-за различий, присущих в реальности даже двум типовым объектам в рамках одного сложного промышленно-технологического комплекса.

В заключение стоит отметить, что даже позиционирующиеся как специализированные для АСУ ТП межсетевые экраны на самом деле могут иметь целый ряд ограничений по области своего применения, поэтому в силу отсутствия универсального решения каждый конкретный случай сегментирования сети промышленного объекта с применением межсетевых экранов должен рассматриваться отдельно.

Иногда, например, применительно к особо критическим объектам, число которых не слишком велико, использование специализированных межсетевых экранов с глубокой поддержкой промышленных протоколов является оправданным и даже необходимым, но в других случаях такой функционал может оказаться избыточным.

Индустриальное исполнение действительно способно упростить и удешевить строительно-монтажные работы, но его итоговое влияние на общую стоимость проекта следует оценивать только в комплексе. Например, более целесообразным может оказаться применение, скажем, программного межсетевого экрана, установленного на компьютер, собранный в промышленном исполнении. ■