**Руслан Амиров**, Директор USSC-SOC УЦСБ
**Алексей Комаров**, автор блога ZLONOV.com
11 января 2022 г.

Публикация: https://www.anti-malware.ru/analytics/Technology_Analysis/SOC-for-Industrial-Control-System

# Особенности применения SOC для мониторинга промышленных сетей АСУ ТП

## Как грамотно организовать мониторинг промышленных объектов (АСУ ТП) и оценить уровень их информационной безопасности? Как поможет и какую роль сыграет центр мониторинга и оперативного реагирования на инциденты в информационной безопасности (SOC — Security Operations Center)?

### Введение

Необходимость непрерывного мониторинга промышленных объектов с точки зрения оценки того, каков уровень их информационной безопасности, может быть вызвана как внешними факторами, так и внутренними. Среди основных внешних можно назвать возросшее число атак, увеличивающийся интерес к такого рода объектам со стороны злоумышленников или необходимость выполнения законодательных требований. Также потребность может быть продиктована желанием повысить общий уровень прозрачности инфраструктуры предприятия, снизить издержки или увеличить эффективность подразделения отвечающего за информационную безопасность.

## И стар, и млад

Длительный средний срок службы систем автоматизации, в разы превышающий время жизни корпоративных ИТ-сервисов, приводит к широкому разнообразию технологий, оборудования, программного обеспечения и сетевых протоколов, применяемых на промышленном предприятии одновременно.

При этом новые, недавно прошедшие модернизацию автоматизированные системы управления технологическими процессами (АСУ ТП) легко могут соседствовать с такими, которые не обновлялись годами или даже десятилетиями. Такой «зоопарк» систем и компонентов означает существенное разнообразие защищаемых активов, что требует от средств защиты информации (в том числе — средств мониторинга) большой гибкости в добавлении новых типов объектов. Как бы ни был широк спектр поддерживаемых «из коробки» программируемых логических контроллеров (ПЛК), протоколов и специального программного обеспечения, велика вероятность на практике встретить редкую их модификацию, а то и вовсе проприетарную заказную разработку.

Средство мониторинга для промышленных систем автоматизации, в которое производитель не заложил возможность расширять поддержку новых защищаемых активов без необходимости изменения исходного кода с привлечением разработчиков, в большинстве случаев будет уступать в скорости внедрения средству мониторинга, имеющему такую возможность.

Не стоит также забывать, что любые модернизации объекта мониторинга (АСУ ТП) неминуемо потребуют адаптации и самого средства мониторинга к этим изменениям, так что упомянутая выше гибкость важна и с точки зрения недопущения пропусков в мониторинге по причинам, например, отсутствия поддержки обновлённой версии прошивки ПЛК.

## Остановы не по требованию

Устаревшее оборудование и программное обеспечение АСУ ТП, в эпоху внедрения которого о вопросах информационной безопасности не было принято особо задумываться, постепенно заменяется на актуальное с одновременным переходом на унифицированные операционные системы и

протоколы, что приводит, как ни парадоксально, ко значительному росту риска. Причина этого проста: широкое распространение стандартных технологий означает, к сожалению, и повышенный интерес к ним злоумышленников, которым стратегически выгоднее искать уязвимости в повсеместно используемом программном обеспечении, чем изучать слабости какого-то редкого программного пакета.

Кроме того, атаки, целью которых изначально могли являться активы корпоративной сети, за счёт применения таких же уязвимых компонентов могут распространиться и на технологические сегменты.

При этом в АСУ ТП по объективным причинам нет возможности реализовать оперативную установку обновлений или внесение изменений в конфигурации. В силу приоритета непрерывности технологических процессов и существенного ущерба, который может быть нанесён из-за технических сбоев в программном обеспечении, любые изменения в технологических сегментах мало того что должны быть тщательно предварительно протестированы, но и реализованы могут быть в подавляющем большинстве случаев исключительно в рамках сервисных обслуживаний (технологических остановов).

Патч операционной системы, требующий обязательной перезагрузки узла АСУ ТП, может быть применён исключительно тогда, когда такая перезагрузка не приведёт ко сбою самого технологического процесса.

В то же время сам по себе технологический останов изначально проводится в первую очередь всё же для сервисного обслуживания компонентов АСУ ТП с целью повышения их производственной эффективности и продления срока службы, а на решение вопросов информационной безопасности может остаться ничтожно мало времени.

В связи с вышеизложенным важно использовать отведённое время максимально эффективно: нужно чётко понимать, какие именно уязвимости наиболее критически значимы и должны быть устранены в первую очередь, а общий подход к выполнению нужных изменений должен обязательно учитывать, что любые потенциальные технические сбои и проблемы вынудят откатиться к изначальным настройкам, рискуя свести на нет все приложенные до этого усилия по повышению уровня защищённости АСУ ТП.

Эффективная система мониторинга позволит выполнить такие работы оптимальным образом, заранее собрав всю нужную информацию о компонентах АСУ ТП и предоставив возможность отслеживать, фиксировать и контролировать даже ход самих работ по внесению изменений.

## Незазорные каналы

Трудно даже примерно оценить, какое количество презентаций решений по информационной безопасности для промышленных систем автоматизации на различных мероприятиях только за этот год начинались с «разрушения мифа о воздушном зазоре».

Тем не менее нельзя не признать тот факт, что так или иначе технологические сегменты в большинстве случаев всё-таки обособляются от корпоративных сетей, а при правильно реализованных подходах — ещё и имеют внутреннюю сегментацию.

Эффективно контролировать происходящее в различных изолированных сегментах, которые в масштабах предприятия могут дополнительно иметь значительную территориальную распределённость, можно либо с помощью соответствующего количества персонала «на местах», либо при помощи автоматизированных систем мониторинга, которые дополнительно должны в максимально щадящем режиме использовать существующие каналы связи. Средство мониторинга, «отъедающее» полезную полосу пропускания от продуктивной работы самой АСУ ТП (что особенно важно для удалённых площадок), вряд ли будет положительно воспринято подразделениями ответственными за технологический процесс.

Позитивным же аспектом более высокой сегментации является, например, возможность оперативной принудительной изоляции отдельных производств от остальной сети в случае выявления атаки. Изначальная ориентированность на плохую связь предполагает допустимость полного прерывания соединений за счёт более высокой автономности, когда АСУ ТП вполне может продолжить самостоятельно работать в течение нескольких часов или даже более длительного периода.

В то же время сетевая связанность с удалёнными площадками может быть важна для более высокоуровневых производственных / бизнес-

процессов, поэтому чем раньше будет обнаружена атака и применена мера реагирования в виде принудительной изоляции, тем быстрее удастся принять меры по остановке атаки и возвращению функционирования распределённой сети предприятия обратно в штатный режим.

Автоматизированная система мониторинга даёт неоспоримое преимущество по времени, не доводя, как пример, до ситуации, когда невозможно вовремя предоставить обязательную информацию отраслевым регуляторам.

## Хорошего мониторинга должно быть много

Резюмируя, можно перечислить основные задачи, которые позволяет решать мониторинг информационной безопасности АСУ ТП.

- Инвентаризация защищаемой системы: нельзя защищать то, чего ты не знаешь.
- Оценка состояния защищённости: комплексные системы мониторинга помогают понять, насколько безопасно настроены компоненты АСУ ТП (например, в части выполнения рекомендаций производителей оборудования и программного обеспечения).
- Выявление инцидентов на основании зарегистрированных событий в информационной безопасности: система мониторинга должна поддерживать функции нормализации и корреляции событий.
- Контроль соблюдения требований законодательства: всесторонний анализ сетевого трафика, конфигураций компонентов АСУ ТП и регистрируемых событий может дать интегральную, развёрнутую по шкале времени оценку степени соответствия текущего состояния защищаемой АСУ ТП (являющейся, например, объектом критической информационной инфраструктуры — КИИ) законодательным требованиям.

Не требует дополнительного пояснения тот факт, что для действительно эффективной работы система мониторинга должна собирать и обрабатывать существенный объём информации, причём весьма оперативно — как для снижения рисков серьёзного ущерба, так и, в отдельных случаях, для выполнения установленных предписаний: например, в случае обязательного информирования субъектом КИИ уполномоченного регулятора.

## Есть реакция!

Вернёмся к вопросу реагирования на инциденты в информационной безопасности: в конце концов, само по себе выявление инцидента полезно разве что с точки зрения последующего расследования и восстановления хронологии.

С учётом рассмотренных особенностей АСУ ТП как объекта защиты для своевременного и правильного выбора способа реагирования нужно одновременно собирать разнородную информацию (сетевой трафик, события от смежных средств защиты информации и на самих компонентах АСУ ТП, конфигурации и текущие состояния программного и аппаратного обеспечения) от существенного числа источников, а затем оперативно и адекватно их оценивать, принимая во внимание в том числе и информацию от внешних по отношению к объекту защиты источников — таких как индикаторы компрометации, различные базы данных угроз и уязвимостей, общий новостной поток и т. п.

Естественно, не представляется возможным возлагать такие высокоуровневые задачи на эксплуатирующий или обслуживающий АСУ ТП персонал; но и на специалистов по информационной безопасности, пусть даже специально выделенных в штате, полагаться в этих вопросах затруднительно по причине имеющихся у них других обязанностей — например, по обслуживанию средств защиты информации и контролю выполнения тех же законодательных мер.

Кроме того, для по-настоящему распределённых предприятий немаловажную роль начинает играть и фактор времени — ограниченное рабочее время и разница в часовых поясах.

## Выводы

Разумным представляется вынесение задач координации всех процессов — от непрерывного мониторинга до выявления, отработки и постанализа инцидентов — на выделенное внутреннее либо внешнее подразделение, реализующее функции оперативного управления информационной безопасностью: такие подразделения традиционно называют Security Operations Center (SOC).

Принимать же решение о том, самостоятельно ли создавать SOC либо воспользоваться аутсорсингом данной услуги, нужно уже исходя из практической ситуации с кадровым обеспечением, возможностями по капитальным вложениям в создание соответствующих технической и организационной структур. Впрочем, этот вопрос уже выходит за рамки статьи.

--- === @zlonov === ---