Обеспечение информационной безопасности при эксплуатации АСУ ТП

En **Information security in the SCADA**

A. V. Komarov,
regional representative in Moscow
Ural Security Systems Center
akomarov@ussc.ru

The article highlights the importance of an information security analysis and monitoring system as a key element of comprehensive information security system SCADA in the operational phase. It also describes the composition and the functions of the SCADA system.

Keywords: information security, monitoring system, cybersecurity, SCADA

В статье рассматривается важность роли системы анализа и мониторинга состояния информационной безопасности (САМСИБ) в качестве ключевого элемента комплексной системы обеспечения информационной безопасности (СОИБ) автоматизированной системы управления технологическим процессом (АСУ ТП) на этапе эксплуатации, а также состав и функции такой системы.

Ключевые слова: информационная безопасность, системы мониторинга, кибербезопасность, АСУ ТП

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

Жизненный цикл АСУ ТП и ПОИБ

Процесс разработки мер обеспечения информационной безопасности (ИБ) промышленных систем автоматизации и управления (ПСАиУ) в целом и автоматизированных систем управления технологическим процессом (АСУ ТП) в частности для достижения максимальной их (мер) эффективности необходимо рассматривать применительно к жизненному циклу самих систем ПСАиУ/АСУ ТП.

Упрощенно жизненный цикл АСУ ТП (далее для определенности будем рассматривать именно эти системы) можно представить в виде четырех основных этапов: Проектирование, Создание (строительно-монтажные и пуско-наладочные работы), прием в эксплуатацию и последующая Эксплуатация, Вывод из эксплуатации. Отдельно нужно рассматривать этап модернизации, когда система фактически проходит упрощенный вариант подцикла Проектирование – Создание – Эксплуатация (см. рисунок).

На каждом из жизненных циклов АСУ ТП процесс обеспечения информационной безопасности имеет свои характерные особенности. Система обеспечения информационной безопасности (СОИБ) точно так же проходит соответствующие этапы жизненного цикла: Проектирование СОИБ – Создание СОИБ – Эксплуатация СОИБ – Вывод СОИБ из эксплуатации.

В идеальном случае этапы жизненного цикла СОИБ по времени совпадают с этапами жизненного

цикла самой АСУ ТП. На практике, даже при наличии строгих требований в нормативно-методических документах, ситуации могут быть различными.

Например, отдельно нужно рассматривать случаи, когда СОИБ проектируется и внедряется для уже действующей АСУ ТП, находящейся в эксплуатации. В таком варианте отсутствует возможность выбора архитектуры АСУ ТП, а ключевым требованием к СОИБ становится отсутствие влияния АСУ ТП, которое может, в свою очередь, привести к негативному влиянию непосредственно на технологические процессы.

Самая протяженная во времени стадия жизненного цикла АСУ ТП – это эксплуатация. Рассмотрим данную стадию с точки зрения особенностей обеспечения информационной безопасности более детально.

Особенности этапа эксплуатации

Прежде всего необходимо отметить: несмотря на распространенное мнение о стационарности и неизменности АСУ ТП, на практике изменения вносятся, при этом порядок их внесения, как правило, строго регламентирован, а сами изменения, в частности, могут включать: изменение конфигураций компонентов АСУ ТП, обновление программного обеспечения, замену компонентов, вышедших из строя и т. п.

При какой-либо модернизации АСУ ТП необходимо одновременно проводить и модернизацию СОИБ.

В силу длительности этапа эксплуатации за это время существенно может поменяться перечень актуальных угроз (например, по причине выявления в компонентах АСУ ТП новых уязвимостей), а также могут модифицироваться сами требования обеспечения ИБ в силу изменения законодательных или отраслевых требований либо из-за пересмотра корпоративной политики.

Таким образом, в отношении СОИБ АСУ ТП можно сформулировать следующий набор мероприятий, которые должны реализовываться в ходе эксплуатации АСУ ТП для нивелирования негативного эффекта от вновь возникающих факторов (табл. 1).

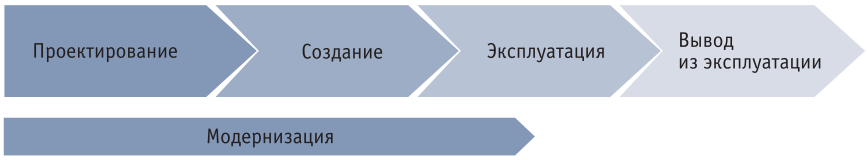

Рисунок. ***Жизненный цикл АСУ ТП***

Данные мероприятия в виде рекомендуемых присутствуют в документах Международной ассоциации автоматизации (ISA – *International Society of Automation*), в работах западных аналитических компаний (например, Langner Group), а также приведены в Приказе ФСТЭК России № 31 от 14.03.2014 «Об утверждении требований к обеспечению защиты информации в АСУ производственными объектами и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей среды».

Для автоматизации и выполнения мероприятий по обеспечению информационной безопасности АСУ ТП предназначены решения класса САМСИБ – системы анализа и мониторинга состояния информационной безопасности.

Подсистемы и функции САМСИБ

Для эффективной реализации приведенных выше мероприятий в состав системы анализа и мониторинга состояния информационной безопасности АСУ ТП должны входить следующие основные подсистемы:

- подсистема мониторинга состояния ИБ;
- подсистема анализа и корреляции событий ИБ;
- подсистема оценки соответствия требованиям по ИБ.

Такое функциональное разделение САМСИБ на несколько подсистем с четко ограниченным перечнем функций для каждой из них позволяет при проектировании использовать модульный подход, когда различные подсистемы и их функции могут быть реализованы на различных модулях одного решения либо на различных решениях, в том числе от разных производителей. Подробнее об этом мы поговорим немногим позднее, сейчас же рассмотрим детальнее функции, реализуемые каждой из перечисленных подсистем.

Подсистема мониторинга состояния ИБ

Данная подсистема является наиболее критичной с точки зрения степени ее непосредственного влияния на АСУ ТП, поэтому реализуемым ею функциям при проектировании должно быть уделено максимально пристальное внимание. Функции подсистемы мониторинга следующие:

- определение текущего состава компонентов АСУ ТП;
- выявление изменений в составе компонентов АСУ ТП;

Таблица 1. ***Факторы, возникающие в ходе эксплуатации АСУ ТП, и мероприятия ИБ, компенсирующие их негативное влияние***

Факторы	Мероприятия ИБ
Изменение компонентов АСУ ТП и/или их конфигураций	• Инвентаризация компонентов АСУ ТП • Контроль конфигураций компонентов АСУ ТП • Централизованный сбор, корреляция, систематизация и анализ значимости событий ИБ в АСУ ТП
Возникновение новых уязвимостей	• Контроль защищенности компонентов АСУ ТП • Обнаружение компьютерных атак
Изменение требований по обеспечению ИБ	• Контроль соответствия требованиям по обеспечению ИБ

Таблица 2. ***Соответствие мероприятий ИБ и функций подсистем САМСИБ, реализующих данные мероприятия ИБ***

Мероприятия ИБ	Подсистемы САМСИБ и их функции
Инвентаризация компонентов АСУ ТП	Подсистема мониторинга состояния ИБ: • определение текущего состава компонентов АСУ ТП • выявление изменений в составе компонентов АСУ ТП
Контроль конфигураций компонентов АСУ ТП	Подсистема мониторинга состояния ИБ: • сбор конфигураций компонентов АСУ ТП Подсистема анализа и корреляции событий ИБ: • выявление изменений конфигураций компонентов АСУ ТП
Централизованный сбор, корреляция, систематизация и анализ значимости событий ИБ в АСУ ТП	Подсистема мониторинга состояния ИБ: • сбор событий информационной безопасности с компонентов АСУ ТП Подсистема анализа и корреляции событий ИБ: • систематизация и анализ значимости событий ИБ Подсистема оценки соответствия требованиям по ИБ: • выявление инцидентов ИБ
Контроль защищенности компонентов АСУ ТП	Подсистема мониторинга состояния ИБ: • проверка компонентов АСУ ТП на наличие уязвимостей
Обнаружение компьютерных атак	Подсистема мониторинга состояния ИБ: • обнаружение компьютерных атак • выявление сетевых аномалий
Контроль соответствия требованиям по обеспечению ИБ	Подсистема оценки соответствия требованиям по ИБ: • оценка выполнения требований безопасной конфигурации • формирование отчетов • интеграция с комплексной автоматизированной системой управления информационной безопасностью (при ее наличии)

- сбор конфигураций компонентов АСУ ТП;
- проверка компонентов АСУ ТП на наличие уязвимостей;
- обнаружение компьютерных атак;
- выявление сетевых аномалий;
- сбор событий информационной безопасности с компонентов АСУ ТП.

Подсистема анализа и корреляции событий ИБ

Модули САМСИБ, реализующие данную подсистему, могут быть вынесены во внешние по отношению к сети АСУ ТП сегменты и с компонентами АСУ ТП не взаимодействовать. Ее основные функции – это систематизация и анализ значимости событий ИБ, а также выявление изменений конфигураций компонентов АСУ ТП.

Подсистема оценки соответствия требованиям по ИБ

Самая высокоуровневая подсистема, реализующая наиболее интеллектуальные функции САМСИБ. Основные функции подсистемы:

- выявление инцидентов информационной безопасности;
- оценка выполнения требований безопасной конфигурации;
- формирование отчетов;
- интеграция с комплексной автоматизированной системой управления информационной безопасностью (при ее наличии).

Итоговое соответствие мероприятий информационной безопасности и функций подсистем САМСИБ, реализующих данные мероприятия, приведены в табл. 2.

Особенности функционирования САМСИБ

Даже в случае первоначального проектирования системы обеспечения информационной безопасности (СОИБ) на этапе проектирования всей АСУ ТП ее функции являются дополнительными по отношению к основным функциям АСУ ТП, поэтому важно, чтобы функционирование СОИБ не оказывало влияние на непосредственные функции АСУ ТП, особенно, если речь идет об опасных либо критически важных объектах и инфраструктурах. Аналогичное требование накладывается и на САМСИБ как составную часть комплексной СОИБ.

В зависимости от текущего состояния АСУ ТП в ходе ее эксплуатации могут быть задействованы различные функции САМСИБ, функции также могут различаться для отдельных компонентов АСУ ТП в зависимости от их критичности с точки зрения способности повлиять на ход технологического процесса в результате внешнего воздействия.

Так, для подсистемы мониторинга состояния ИБ можно выделить три режима функционирования в зависимости от степени влияния на компоненты АСУ ТП: пассивный мониторинг, активный мониторинг и сканирование защищенности (табл. 3).

Режим пассивного мониторинга никакого воздействия на компоненты АСУ ТП не оказывает, но и набор доступных функций при этом минимален. На практике такой режим может быть реализован, например, путем анализа зеркалированного трафика (подключение к хабу, SPAN-порту либо TAP-устройству). Еще одним вариантом щадящего подключения модуля САМСИБ, реализующего функции мониторинга, является использование однонаправленного шлюза (сетевого диода).

При ***активном мониторинге*** осуществляется двусторонняя связь с компонентами АСУ ТП, предполагается их отклик на внешние запросы, но без каких-либо активных действий, способных привести к влиянию на АСУ ТП и, соответственно, непосредственно на сам технологический процесс.

Наиболее агрессивный режим – ***режим сканирования защищенности*** – реализует уже все заявленные функции подсистемы мониторинга состояния ИБ, но является наиболее критическим с точки зрения воздействия на компоненты АСУ ТП, а следовательно, – на технологический процесс.

Выбор конкретного режима работы подсистемы мониторинга состояния ИБ для различных компонентов АСУ ТП необходимо осуществлять на этапе проектирования. Общий подход предполагает наиболее щадящий режим функционирования для низкоуровневых компонентов АСУ ТП, непосредственно задействованных в самом технологическом процессе, и рост активности взаимодействия с более высоко расположенными в иерархии компонентами. Также при проектировании важно учитывать режимы функционирования самой АСУ ТП (штатный, режим обслуживания и т. п.), а выбор конкретных функций осуществлять исходя из степени возможного влияния конкретной функции на работу АСУ ТП.

Для модулей САМСИБ, реализующих подсистему анализа и корреляции событий ИБ и подсистему оценки соответствия требованиям по ИБ, непосредственного взаимодействия с компонентами АСУ ТП уже не требуется, и их подключение можно осуществлять только непосредственно к модулю подсистемы мониторинга состояния ИБ.

Таблица 3. ***Реализуемые функции подсистемы мониторинга состояния ИБ в различных режимах функционирования***

Функции подсистемы мониторинга состояния ИБ	Пассивный мониторинг	Активный мониторинг	Сканирование защищенности
Определение текущего состава компонентов АСУ ТП	Нет	Нет	Да
Выявление изменений в составе компонентов АСУ ТП	Да	Да	Да
Сбор конфигураций компонентов АСУ ТП	Нет	Да	Да
Проверка компонентов АСУ ТП на наличие уязвимостей	Нет	Нет	Да
Обнаружение компьютерных атак	Да	Да	Да
Выявление сетевых аномалий	Да	Да	Да
Сбор событий информационной безопасности с компонентов АСУ ТП	Да*	Да	Да

* *Сбор событий информационной безопасности с компонентов АСУ ТП в режиме пассивного мониторинга можно осуществить, настроив, например, отправку компонентами АСУ ТП информации о своем состоянии по протоколу, не требующему подтверждения о доставке непосредственно в САМСИБ или через промежуточный сервер логгирования. В случае невозможности реализации такой настройки, функция сбора событий ИБ с компонентов АСУ ТП может быть реализована только в режиме активного мониторинга, путем активного опроса.*

Варианты реализации САМСИБ

В зависимости от особенностей конкретной АСУ ТП, имеющихся решений по обеспечению информационной безопасности, если речь идет о построении СОИБ для уже действующей АСУ ТП, а также других факторов, в том числе экономических, возможны различные варианты реализации САМСИБ.

В качестве основных составных модулей САМСИБ могут выступать следующие классы решений:

- сканеры защищенности либо системы анализа защищенности;
- системы управления событиями информационной безопасности (SIEM – *Security information and event management*);
- системы обнаружения компьютерных атак (IDS – *Intrusion detection system*);
- системы анализа правил сетевого доступа;
- системы контроля конфинураций.

На рынке также присутствуют комплексные специализированные решения, в том числе отечественного производства, реализующие полный либо частичный набор перечисленных функций САМСИБ.

При выборе конкретного способа реализации САМСИБ в качестве основных критериев можно предложить следующий их набор:

- совокупная стоимость владения (цена, обслуживание и т. п.);
- производитель (наличие поддержки, локального офиса и пр.);
- реализуемые режимы работы (есть ли, например, режим полностью пассивного мониторинга либо требуется установка агентского программного обеспечения на какие-либо компоненты АСУ ТП);
- полнота поддерживаемого оборудования и специфических протоколов, используемых в конкретной АСУ ТП;
- дополнительная создаваемая нагрузка на каналы связи, требования к пропускной способности;
- наличие варианта аппаратной составляющей в промышленном исполнении (температурной диапазон, поддержка специфичных вариантов монтажа, требования к питанию и т. п.);
- простота и полнота интерфейса, его доступность для обслуживающего персонала.

Заключение

Система анализа и мониторинга состояния информационной безопасности, несмотря на ее широкие функциональные возможности и реализуемые с их помощью мероприятия информационной безопасности, является важной, но лишь одной из составных частей комплексной системы обеспечения ИБ. Полный набор средств для комплексной СОИБ может включать в себя в том числе межсетевые экраны, однонаправленные шлюзы, решения для защиты конечных узлов, средства управления доступом к сети, решения для контроля доступа привилегированных пользователей и др.

Корректный состав СОИБ определяется в каждом случае в зависимости от особенностей конкретной АСУ ТП, уже, возможно, имеющихся решений по обеспечению информационной безопасности у владельца АСУ ТП, а также из соображений экономической целесообразности и в зависимости от модели угроз для данной АСУ ТП. ■