Лишнее звено в защите АСУ

Екатерина ГЕРЛИНГ,
доцент, к. т. н., ведущий инженер-аналитик лаборатории стратегического развития продуктов кибербезопасности, Аналитического центра кибербезопасности компании «Газинформсервис»

На фоне широкого внедрения автоматических систем управления (АСУ) в различные сферы деятельности вопросам безопасности уделяется недостаточное внимание, о чем свидетельствует ужесточение нормативных требований. Востребованность в защите АСУ без участия человека – закономерный этап эволюции, обусловленный развитием технологий, экономики, а также возрастающим количеством киберугроз для объектов с критической информационной инфраструктурой (КИИ). Что можно противопоставить существующим рискам в сфере кибербезопасности?

Культура безопасности

Автоматическая система управления технологическом процессом (АСУ ТП) – технологически сложное решение, включающее многочисленные конечные устройства, такие как датчики, сенсоры, контроллеры. Остановка АСУ ТП на современном предприятии грозит остановкой всего производства. Финансовые и репутационные потери от киберинцидента на современном предприятии многократно превышают стоимость внедрения и владения системой защиты информации.

Контроллеры также являются частью локальной сети, поскольку снабжены интерфейсом Ethernet, передают данные через локальную сеть в SCADA-системы. Датчики и сенсоры раньше не имели доступа в локальную сеть, но в последнее время активно развивается технологии IIoT (англ. Industrial Internet of Things) – Промышленный Интернет вещей.

IIoT – это концепция сети физических устройств (датчиков или сенсоров), подключенных к интернету (либо локальной сети) и обменивающихся данными для оптимизации производственных процессов и повышения эффективности технологического производства. Технология IIoT помогает повысить эффективность производства и увеличивает риск атаки на датчики, сенсоры и механизмы управления.

Активное развитие цифровизации, в том числе IIoT, АСУ ТП, связано, в частности, с высокими темпами технологического производства. Современные системы энергетики, транспорта, топливно-энергетического комплекса работают на скоростях, недоступных для человеческой реакции.

Раньше системы управления технологическими процессами были сосредоточены внутри предприятий. Постепенно сети АСУ ТП становятся менее изолированными. Повышается уровень их интеграции с корпоративными ИТ-сетями и облаками.

В отсутствие изолированности АСУ ТП и при внедрении IIoT расширяется поверхность атаки на промышленные системы. Сбой в работе системы может привести к катастрофическим последствиям за миллисекунды.

Заметим, что системы защиты информации без участия человека достаточно быстро реагируют на инциденты, при этом исключают ошибки, вызванные человеческим фактором. В этом они превосходят даже высококвалифицированных сотрудников, которые не застрахованы от выполнения неточных или неправильных действий. При этом на рынке труда острейший дефицит специалистов по кибербезопасности, особенно в узкоспециализированной области защиты АСУ ТП.

Наряду с этим повышаются сложность и скрытость кибератак. Все это способствует росту востребованности защиты информации АСУ ТП без участия человека.

Помимо АСУ ТП, систем, отвечающих за технологический процесс, в современном мире активно развиваются прочие АСУ, например системы управления инженерными службами жилых зданий.

Внедрение АСУ в повседневную жизнь повышает эффективность инженерных систем. Но стремительному проникновению АСУ во все сферы жизни не соответствует уровень внимания к их кибербезопасности, что создает серьезные риски для систем.

Последствиями уязвимостей в АСУ ТП могут стать не просто утечка данных, а прямые угрозы физическому миру, например:

- остановка производства на дни или недели, ведущая к колоссальным убыткам;
- техногенные и экологические катастрофы из-за сбоя в управлении критическими процессами;
- веерные отключения электроэнергии в городах;
- угроза жизни и здоровью людей.

Миру известны прецеденты: в частности, атака «червя» Stuxnet на иранский ядерный объект, паралич работы трубопровода в США.

В настоящее время необходимо менять культуру безопасности, внедряя ее на этапе проектирования систем (Security by Design). Критически важно сегментировать сети, изолируя АСУ от непроверенных подключений, использовать специализированные средства защиты информации, не полагаясь на стандартные ИТ-решения.

Ключевую роль играют государственное регулирование и разработка обязательных стандартов для защиты критической информационной инфраструктуры. Развитие цифровой экономики и рост киберугроз заставили государства разрабатывать строгие нормативные рамки. Ужесточаются требования к информационной безопасности. Подходы разных стран к решению подобных задач имеют общие черты и ключевые различия.

Общемировая тенденция в стандартах киберзащиты – сдвиг от рекомендаций к жестким обязательным требованиям. В фокусе находятся объекты с критической информационной инфраструктурой.

Регуляторные требования

Национальные стандарты России прямо предписывают внедрение средств автоматического контроля целостности, обнаружения вторжений и управления инцидентами в АСУ ТП.

В России основной нормативный документ в этой сфере – Федеральный закон от 26.07.2014 № 187-ФЗ «О безопасности критической информационной инфраструктуры». Законом предусмотрено обязательное категорирование всех объектов КИИ по уровню значимости и потенциального ущерба. Для каждой категории установлены строгие требования к используемым средствам защиты информации, проведению регулярных оценок, передаче информации об инцидентах в ГосСОПКА (единый централизованный, территориально распределенный комплекс, который включает силы и средства обнаружения, предупреждения и ликвидации последствий компьютерных атак). Система нужна для того, чтобы не допустить масштабных сбоев в работе объектов с КИИ.

Сведения, которые необходимо передавать в ГосСОПКА, указаны в Приказе ФСБ России № 367 «Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка представления информации в эту систему». Помимо информации об инцидентах и атаках объект с КИИ обязан передавать сведения о категории значимости объекта, защищенности информационных ресурсов, доступных из интернета, нарушениях требований по обеспечению безопасности и др.

В России нормативные документы в области информационной безопасности тесно связаны с политикой импортозамещения. Так, Федеральный закон от 07.04.2025 № 58-ФЗ «О внесении изменений в ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» закрепляет переход госсектора и объектов с КИИ на отечественное программное обеспечение, в частности, в области информационной безопасности.

> Общемировая тенденция в стандартах киберзащиты – сдвиг от рекомендаций к жестким обязательным требованиям, фокусируясь на критической информационной инфраструктуре.

Международный подход к кибербезопасности основывается на рамочных моделях (frameworks), которые обеспечивают структурированный и унифицированный подход к защите информационных систем. Один из наиболее ярких примеров такой модели – американский NIST Cybersecurity Framework, который предлагает гибкую систему построения защиты, основанную на пяти ключевых функциях: выявление, защита, обнаружение, реагирование и восстановление. Таким образом, ставка делается на гибкость и управление рисками.

Для бизнеса, функционирующего в глобальном масштабе, необходимо соответствовать одновременно двум системам требований. Кибербезопасность требует комплексного подхода, включающего в себя технические меры и организационные изменения. Необходимо разработать и внедрить внутренние политики и процедуры, направленные на предотвращение кибератак и минимизацию ущерба

в случае их возникновения. Для успешного ведения бизнеса в глобальном мире следует уделять особое внимание вопросам кибербезопасности. Это вопрос не только конкурентоспособности и финансовой устойчивости, но и национальной безопасности, требующий совместных усилий со стороны государства и частного сектора.

Специфика защиты

В России выполнение регуляторных требований усложняется особенностями АСУ. Промышленное оборудование рассчитано на 20–30 лет службы. Многие критически важные АСУ ТП были развернуты во времена, когда о кибератаках не задумывались. Системы проектировались для изолированных сетей. Сегодня, когда сети и АСУ ТП подключены к корпоративным сетям и интернету для удаленного контроля и постоянного сбора данных для последующего анализа, важно обеспечить эффективную киберзащиту, которую необходимо интегрировать в защищаемые системы. Заметим также, что в АСУ ТП не всегда можно внедрить продукты информационной безопасности. А инженеры-технологи могут не обладать достаточными знаниями в области кибербезопасности, что повышает риски, связанные с человеческим фактором.

Как показывает практика, внедрение средств защиты информации часто требует остановки технологического процесса или временного отключения сети. Это может оказывать негативное влияние на бизнес, для которого главное – бесперебойная работа. Кроме того, зачастую специалисты сталкиваются с непониманием рисков со стороны руководства, которое воспринимает кибербезопасность как статью расходов, а не как инвестиции в повышение устойчивости АСУ ТП.

Ландшафт угроз АСУ ТП эволюционировал от случайных заражений к целевым сложным атакам. Например, вымогатели все чаще стали целиться в промышленные объекты, пытаясь блокировать работу АСУ ТП. Появляется специализированное вредоносное программное обеспечение, созданное с учетом особенностей промышленных протоколов. Все чаще используются атаки на цепочку поставок, которые реализуются через обновление легального программного обеспечения или скомпрометированное оборудование и ПО от вендора. Атаки через легальные каналы крайне сложно обнаружить.

> Безопасность АСУ перестала быть техническим вопросом – сегодня это стратегическая необходимость для национальной и экономической безопасности.

Индустриальные тенденции

Вслед за атаками развивается индустрия промышленной кибербезопасности. Участившиеся атаки на цепочку поставок стимулировали широкое распространение принципа «Никому не доверяй, проверяй всё и всех». Такой подход реализуется через разделение сети на доверенную и недоверенную зоны, что позволяет изолировать инцидент и предотвратить его распространение внутри инфраструктуры. Появляются базы уязвимостей для ПО и оборудования АСУ ТП, которые позволяют приоритезировать риски. Разрабатываются и внедряются специальные алгоритмы устранения последствия атак без остановки оборудования. Важную роль играют мониторинг, контроль трафика и обнаружение аномалий. Для эффективного контроля алгоритмов и протоколов АСУ ТП разрабатываются специальные программные продукты.

Помогать специалистам в сфере кибербезопасности будет искусственный интеллект (ИИ). Системы научатся прогнозировать атаки, анализировать большие массивы телеметрии и выявлять едва заметные аномалии, что, в свою очередь, позволит организовать проактивную защиту. Повышения доверия к сторонним вендорам можно добиться, следуя принципу «безопасность по умолчанию». Производители оборудования будут вынуждены встраивать инструменты киберзащиты в свои продукты, а не предлагать их как опцию. В сторону ужесточения мер будут развиваться регуляторные документы и подход к контролю со стороны государства.

Стоит помнить и том, что с приходом квантовых вычислений возникнет риск взлома современных алгоритмов шифрования, что потребует заблаговременного перехода на квантово-устойчивую криптографию.

Безопасность АСУ перестала быть техническим вопросом – сегодня это стратегическая необходимость для национальной и экономической безопасности. Игнорирование проблемы сегодня может привести к катастрофе завтра. Для эффективной защиты требуется комплексный подход, включающий внедрение стандартов, использование специализированных технологий, постоянное обучение сотрудников и разработку детализированных планов реагирования на инциденты. Инвестирование в кибербезопасность АСУ ТП – основа стабильности и безопасности в будущем. ■