ОСНОВЫ БЕЗОПАСНОСТИ ИНДУСТРИАЛЬНЫХ СИСТЕМ УПРАВЛЕНИЯ

СУНИЛ ДОДДИ (SUNIL DODDI)
ПЕРЕВОД: ВЛАДИМИР РЕНТЮК

Для защиты от кибератак используемых в промышленности систем управления (ICS) крайне важно разработать и реализовать комплексный план по обеспечению кибербезопасности. При этом необходимо не только определить угрозы и уязвимости, но и удовлетворить требования соответствующих стандартов и регламентирующих документов.

Промышленная система управления (Industrial Control System, ICS) — это общее понятие, которое используется для обозначения нескольких типов систем управления, включая системы диспетчерского управления и сбора данных (Supervisory Control And Data Acquisition, SCADA), распределенные системы управления (Distributed Control System, DCS), системы на базе программируемых логических контроллеров и др. Все они применяются в промышленных средах и содержат критические инфраструктуры[1]. Обеспечение безопасности ICS подразумевает в первую очередь их защиту от любых преднамеренных или непреднамеренных помех, воздействие которых может привести к нарушениям функционирования системы.

БЕЗОПАСНОСТЬ ICS

Безопасность промышленных систем управления в широком смысле может быть классифицирована как кибербезопасность. Хотя само слово «кибербезопасность» у нас скорее ассоциируется с непосредственным воздействием через Интернет-соединение, но это не совсем так, когда дело касается среды использования ICS.

Потребность в безопасности для таких систем постоянно возрастает, поскольку увеличивается и число угроз. В связи с этим уже вступили в силу и действуют правила, регламентирующие требования безопасности, а компании имеют юридическое, моральное и финансовое обязательство ограничить потенциальные риски. Как следствие, основополагающий стандарт IEC 61511:2016 «Functional safety — Safety instrumented systems for the process industry sector» («Функциональная безопасность — Системы безопасности приборные для промышленных процессов»)[2], разработанный для индустриального сектора, также требует оценки приборной системы безопасности (Safety Instrumented System, SIS) в системах управления.

Из-за проблем, связанных с нарастающими кибератаками, и справедливого возмущения этими наглыми выходками, в области безопасности

[1] Полное определение ICS дано Национальным институтом стандартов и технологий США (NIST) в стандарте SP 800-82 Rev. 2 «Guide to Industrial Control Systems». — Прим. пер.

[2] Стандарт IEC 61511:2016 состоит из трех частей. В РФ его аналогами являются стандарты, аутентичные редакции соответствующих частей: ГОСТ Р МЭК 61511-1-2011 «Безопасность функциональная. Системы безопасности приборные для промышленных процессов. Часть 1. Термины, определения и технические требования»; ГОСТ Р МЭК 61511-2-2011 «Безопасность функциональная. Системы безопасности приборные для промышленных процессов. Часть 2. Руководство по применению МЭК 61511-1»; ГОСТ Р МЭК 61511-3-2011 «Безопасность функциональная. Системы безопасности приборные для промышленных процессов. Часть 3. Руководство по определению требуемых уровней полноты безопасности». — Прим. пер.

ICS необходимо уделять больше внимания уменьшению рисков ее уязвимости от действий внешних хакеров. Однако кибербезопасность является лишь одной из сторон защиты индустриальных систем управления. Угрозы для современных ICS проявляются в самых разных формах.

ИДЕНТИФИКАЦИЯ УГРОЗ

Угрозы для систем управления могут быть как внешними, так и внутренними. Также они могут быть классифицированы как преднамеренные, т. е. заранее нацеленные на нанесение того или иного ущерба, в том числе максимального, или же как случайные. Типичными внешними угрозами являются действия хакеров, соперников по бизнесу или конкурирующих организаций/государств. Внутренние угрозы чаще всего приобретают вид ошибочных действий, ненадлежащей реакции на какое-либо текущее событие, мести недовольных сотрудников и т. д.

Для защиты от внешних угроз необходимо предпринять нечто большее, чем просто повысить безопасность самой сети. В свою очередь, путем одного лишь усиления внутренних процедур или политик избежать всех внутренних угроз тоже не удастся. Оптимальная безопасность промышленной системы управления достигается за счет подходов, направленных одновременно и на укрепление сетевой безопасности, и на внедрение и поддержку правильных политик и процедур.

ОПРЕДЕЛЕНИЕ УЯЗВИМОСТЕЙ ICS

Ранее системы управления предприятием были автономными, но теперь это уже не так. ICS стали уязвимыми для внешних угроз главным образом из-за использования стандартных и коммерчески доступных (так называемых commercial off-the-shelf, или COTS) технологий и широкого подключения к сети. Причем по самым разным причинам. А вот внутренние угрозы возникают, как и изначально, в первую очередь из-за неправильных действий персонала или ошибок в организации системы управления.

Кроме того, ключевыми уязвимостями системы управления являются:

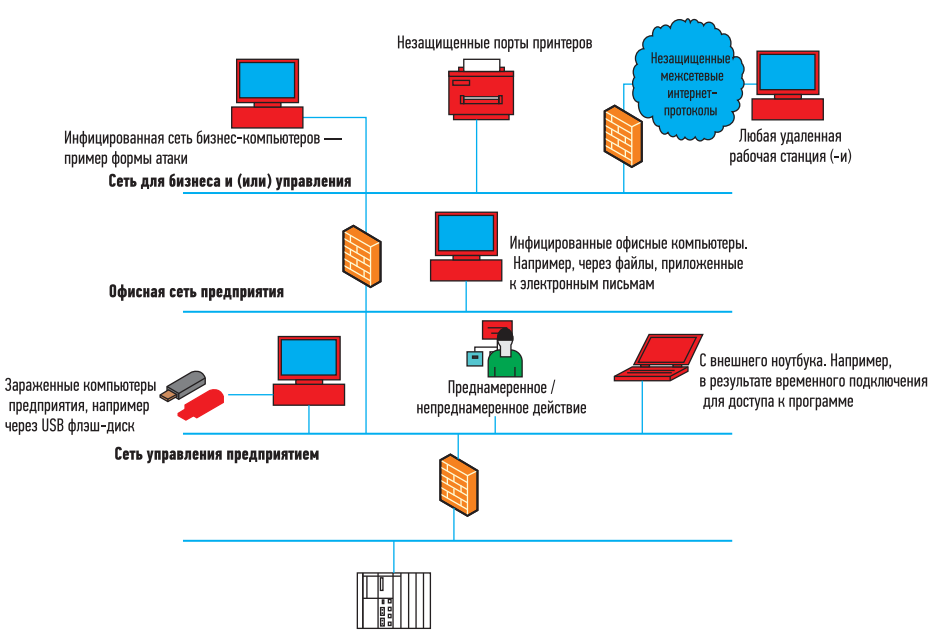
- неадекватные политики и процедуры;
- отсутствие концепции глубокоэшелонированной защиты (или, как ее иногда называют, «защита в глубину», от англ. «defense-in-depth»);
- несоответствующие элементы управления с удаленным доступом;
- ненадлежащее обслуживание программного обеспечения (ПО);
- неадекватная с точки зрения управления беспроводная связь;
- использование выделенной полосы пропускания ICS для целей, не связанных непосредственно с управлением;
- несоблюдение мер по пресечению ненадлежащей активности в системе;
- отсутствие валидации (подтверждения целостности и достоверности) сетевых данных управления;
- неадекватная поддержка критически важных компонентов и систем.

При этом для проникновения в сеть управления угрозы могут использовать множество самых разнообразных путей на различных уровнях системы (рис. 1).

Заблокировать путь угрозы в систему и справиться с ней может программный или программно-аппаратный элемент в виде межсетевого экрана, который часто называют брандмауэром, или файрволом. Установить брандмауэр просто, но программировать довольно трудно, а правильно программировать — очень сложно. При этом неверно настроенный брандмауэр эквивалентен его полному отсутствию.

Приборные системы безопасности (SIS) в системах управления подвержены угрозам, если в них используется неспециализированная общедоступная технология (COTS). Особенно в том случае, если они интегрированы как часть сети управления и обмениваются информацией по небезопасному открытому протоколу. Компрометация SIS может привести не только к временным проблемам, но и к полной потери управления предприятием или какой-либо единицей его инфраструктуры.

РИС. 1. ▼ Возможные пути взлома промышленной системы управления



СТАНДАРТЫ БЕЗОПАСНОСТИ ДЛЯ ICS

Правительства ведущих мировых держав и ряд отраслевых организаций, обеспокоенных текущей ситуацией в вопросах безопасности систем управления, разрабатывают и вводят в действие соответствующие стандарты безопасности. Они стремятся обеспечить должное руководство, предложить передовой опыт в решении данной проблемы и в результате повысить устойчивость систем к воздействию потенциальных угроз. Некоторые

из основных стандартов подобного типа приведены ниже:

- серия стандартов ISA99 — Industrial Automation and Control Systems Security (Безопасность промышленной автоматизации и систем управления) /IEC 62443[3];
- стандарт Национального института технологий стандартов США (National Institute for Standards Technology, NIST) SP 800-82 — Guide to Industrial Control Systems Security standard (Руководство по безопасности промышленных систем управления);
- серия стандартов безопасности CIP Совета североамериканских штатов по надежному обеспечению электроэнергией (North American Electric Reliability Council, NERC).

Как и у функциональной безопасности, жизненный цикл непосредственно той ее части, которую мы называем кибербезопасностью, зависит от трех основных компонентов: анализа, реализации и обслуживания. Под термином «жизненный цикл» в данном случае подразумевается непрерывный процесс функционирования системы безопасности, и решающее значение здесь имеет обратная связь (рис. 2).

Однако при этом могут возникнуть некоторые объективные и субъективные проблемы. Так, многим компаниям трудно согласиться на включение в бюджет внедрения и поддержания жизненного цикла кибербезопасности. Без продвижения этих действий руководителями компании жизненный цикл кибербезопасности тоже, скорее всего, потерпит неудачу. Чтобы этого не случилось, специалистам необходимо представить бизнес-план, в котором излагаются потенциальные угрозы, последствия, а также прямые и косвенные выгоды для конкретной компании.

Кроме того, должна быть проведена надлежащая оценка риска еще и в соответствии с потребностями организации. Она может включать план, тестовую среду, показатели и всю необходимую для подтверждения документацию.

Для оценки риска доступны различные инструменты и подходы. При этом для анализа воздействия цикла безопасности качественный или количественный подход может быть реализован уже на основе конкретных требований организации. При количественной оценке используются полученные ранее данные, а при качественной требуются определенные параметры для надлежащего получения результата.

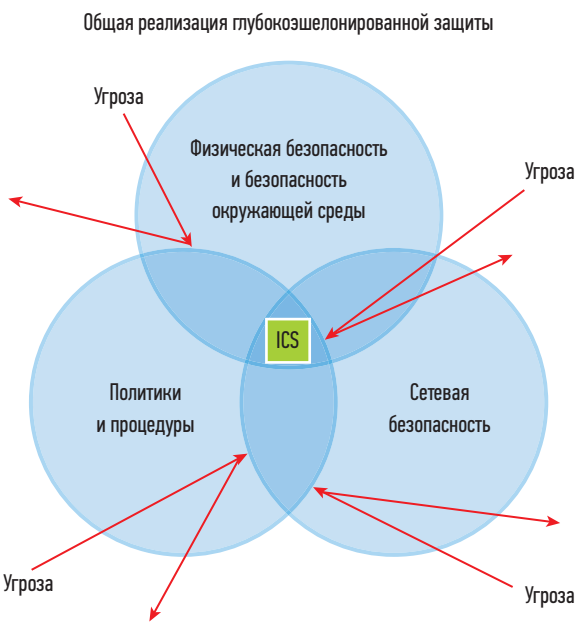


РИС. 2. ◀ Глубокоэшелонированная защита может быть организована путем комплексного укрепления мер безопасности. Так, например, если сетевая безопасность нарушена, то для нейтрализации угрозы могут быть противопоставлены правильные политики и процедуры

В тестовых средах соответствующую оценку уязвимости может выполнить специальная программа или детальный анализ, которые сыграют роль своеобразного сканера безопасности. Однако такого похода, как показано на рис. 1, все еще будет недостаточно. Безопасность самих ICS не защищает от кибератак, для этого необходимо также обеспечить личную, физическую безопасность и безопасность окружающей среды.

Требования по физической безопасности могут включать контроль доступа к ограниченным зонам, системы видеонаблюдения, датчики движения, тепловизоры, а также другие средства и методы защиты. Обезопасить окружающую среду от пыли, высоких и низких температур и токсичных газов можно с помощью надлежащей системы вентиляции и кондиционирования воздуха и систем сигнализации (для идентификации отказа того или иного оборудования и возможных последствий).

Решающее значение для устранения случайных и внутренних угроз имеют их четкое осознание, а также соответствующие политики и процедуры. Контроль доступа и авторизации для выполнения конкретных действий необходимо обеспечить именно с помощью четко разработанных политик и процедур. Для отслеживания уровней доступа также могут использоваться традиционные логи (файловые журналы).

Безопасность системы управления предприятием необходимо обеспечить еще на стадии разработки ПО для функционирования данной компании. Кроме того, в системе управления должны использоваться исключительно сертифицированные по кибербезопасности компоненты. Нужно твердо усвоить, что для защиты ICS и минимизации риска необходима глубокая и развитая техника защиты.

Поскольку киберугрозы быстро меняются, управление рисками безопасности также должно быть непрерывным процессом. Для поддержания ее работоспособности необходимы периодический аудит и проверка всего жизненного цикла кибербезопасности. Это включает управление внесением исправлений (патч-менеджмент), обновления антивирусных программ и баз, а также осведомленность о тенденциях и рисках в области безопасности для конкретной отрасли. ⬣

[3] Стандарт IEC 62443 — это серия стандартов. В РФ ее аналогами являются стандарты серии ГОСТ Р МЭК 62443... «Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы». — Прим. пер.