УДК 351.864.1

РИСКИ ВНЕДРЕНИЯ И ЭКСПЛУАТАЦИИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ПРОИЗВОДСТВОМ

Ляхевич А.Г.
Белорусский национальный технический университет
Минск, Республика Беларусь

Современные инновационно-ориентированные предприятия широко используют автоматизированные системы управления производством. Подобные системы, именуемые АСУП в отечественной традиции, в западной литературе получили название ICS-системы (Industrial Control System), или применительно к системам сбора данных и контроля за технологическим процессом - SCADA-системы (Supervisory Control And Data Acquisition). Существует сформировавшийся рынок программной продукции как для SCADA-систем, так и для автоматизированных систем планирования и управления производственной деятельностью.

Внедрение подобных систем существенно повышает эффективность бизнес-процессов и конкурентоспособность предприятия, однако в то же время несёт в себе и существенные риски. К числу факторов, порождающих эти риски, можно отнести как человеческий фактор, так и чисто технические проблемы. Так внедрение ICS-системы требует переобучения персонала, что, с одной стороны, потребует дополнительных финансовых затрат, отвлечения работников от выполнения своих прямых обязанностей или снижения эффективности выполнения работниками своих обязанностей на время обучения. С другой стороны, необходимость переобучения сама по себе может стать серьёзным психологическим стрессом, особенно для лиц старше среднего возраста, что способно ухудшить психологическую атмосферу в коллективе и даже привести к саботажу нововведений. Даже верхний уровень управления может быть не в полной мере заинтересован во внедрении автоматизированных систем управления, т.к. наличие подобных систем делает процесс управления более «прозрачным» и наблюдаемым, следовательно, ошибки управления также становятся более наглядными, как для подчинённых, так и для вышестоящего руководства. Кроме того, внедрение автоматизированных систем существенно ускоряет бизнес-процессы, следовательно, управленческие решения придётся принимать в более сжатые сроки и оперативно реагировать на все возникающие проблемы. Это следствие внедрения автоматизированных систем, безусловно положительное для предприятия в целом, негативным образом сказывается на интенсивности и психологической напряжённости содержания работы лиц, принимающих решение.

Работники предприятия и лица, принимающие решения, могут иметь устоявшиеся приёмы работы и опыт управления, трудно совместимые с внедряемой автоматизированной системой. В таких случаях автоматизированная система может существовать сама по себе, просто дублируя традиционную систему управления. В результате бизнес-процессы не ускоряются, а наоборот замедляются в связи с необходимостью функционирования сразу двух дублирующих систем. Возможен также вариант, когда ресурсы, высвободившиеся в результате внедрения автоматизированной системы управления, направляются на усложнение действующей схемы принятия решений, т.е. если раньше на учёт и документирование малозначительных (с точки зрения принятия решения) обстоятельств просто не хватало времени и ресурсов, то внедрение автоматизированной системы управления предоставляет такую возможность. В результате скорость бизнес-процессов сохраняется на прежнем уровне (до внедрения автоматизированной системы), что уже не требует столь интенсивной работы от лиц принимающих решение.

В последнее время в процессе внедрения и эксплуатации автоматизированных систем управления производством всё большее значение начинают приобретать информационные риски. Злоумышленник, воспользовавшийся той или иной уязвимостью в SCADA-системе, способен остановить производственный процесс, нанеся тем самым существенный экономический ущерб предприятию за время вынужденного простоя, а также ущерб для его деловой репутации, в результате срыва обязательств предприятия перед контрагентами. Злоумышленнику, к слову, совсем не обязательно полностью блокировать производственный процесс, он может ограничиться модификациями в SCADA-системе, приводящими к снижению уровня качества выпускаемой продукции, путём нарушения параметров технологического процесса. Такое воздействие может быть замечено предприятием далеко не сразу, а только по факту появления рекламаций от потребителей продукции. Не меньшую угрозу представляет собой и промышленный шпионаж, посредством хищения информации, циркулирующей в SCADA-системе. В случае реализации наиболее худшего сценария, действия злоумышленника могут привести к авариям на производстве и человеческим жертвам.

Указанные информационные риски отнюдь не являются чисто теоретической возможностью. В настоящий момент существуют легкодоступные широкому кругу лиц инструменты, позволяющие осуществлять атаки на SCADA-системы. В качестве примера, можно привести программный комплекс WinCC Harvester, позволяющий после взлома SCADA-системы WinCC получить доступ к дополнительной информации о пользователях и подключенных к системе промышленных контроллерах. Система WinCC относится к семейству продуктов Siemens SIMATIC (WinCC, Step 7, PCS 7), на долю которых только в России приходится более 52% всех АСУ ТП. Очевидно, что нахождение уязвимостей в SCADA-системах такого класса способно нанести серьёзный экономический ущерб большому числу предприятий. В то же время, такие уязвимости появляются регулярно. Так в ноябре 2012 года компания ReVuln обнаружила уязвимости в SCADA-системах, разрабатываемых фирмами Siemens, General Electric, Schneider Electric, ABB/Rockwell. Все обнаруженные бреши в SCADA-системе могли эксплуатироваться злоумышленниками удалённо, из любой точки сети Internet. На конференции Black Hat 2013 эксперты продемонстрировали, как путём эксплуатации уязвимости в SCADA-системе можно удаленно управлять насосами в нефтепроводах и нефтяных скважинах [1]. Экспертам удалось удаленно включать и выключать насосы, что в определённых условиях может привести к значительным повреждениям скважины. Специалисты также смогли подменить данные в человеко-машинном интерфейсе оператора системы. Впоследствии они переполняли нефтяную цистерну, а оператору выводили данные о том, что уровень жидкости наоборот падает. В этом случае оператор начинает закачивать в бак больше, что становится причиной аварии. В феврале 2013 года немецкие журналисты из издания Heise Security, обнаружили несколько сотен уязвимых SCADA-систем, подключенных к сети Интернет [2]. Выявленные бреши были охарактеризованы как «тривиальные», однако большая часть из них позволяла получить доступ и внести произвольные изменения в уязвимых системах. Так, например, не составило бы труда полностью остановить местную электростанцию, вмешаться в технологический процесс на пивоваренном заводе, и отключить отопление в одной из немецких тюрем. Особенно показателен тот факт, что и спустя месяц после извещения руководителей указанных учреждений о найденных уязвимостях, никаких мер принято не было.

Особую важность информационным рискам придаёт тот факт, что в последнее время атаки на SCADA-системы приняли организованный характер: атаки тщательно подготавливаются большими группами высококвалифицированных специалистов в самых разных областях знаний. Сейчас атаки на SCADA-системы – это не только противоправные действия конкурентов и технарей-одиночек, но и долгосрочная стратегия целого ряда промышленно-развитых стран. Достоверно установлено, что атака вируса Stuxnet на SCADA-системы предприятий Ирана была совместной операцией правительства США и армии Израиля. Операция с кодовым именем «Olympic Games» была начата ещё администрацией Джорджа Буша в 2006 году. В 2010 году вирус нанес огромный урон заводу по обогащению урана на иранском предприятии Natanz. С тех пор появилось уже несколько модификаций этого вируса - Duqu, Gauss и Flame. В настоящий момент ФБР преследует должностных лиц, причастных к утечке информации о причастности США к кибератаке. Важность предотвращения подобных кибератак для национальной безопасности прекрасно осознаётся во всём мире. Так 17 января 2013г. в Гааге состоялось открытие Европейского центра по борьбе с киберпреступностью (ЕС3), функционирующего на базе Европола. В 2013 году в Российской Федерации был внесён законопроект «О безопасности критической информационной инфраструктуры Российской Федерации». Однако было бы крайне не дальновидно ограничиваться защитой только критически-важных инфраструктурных объектов. Практика расследования инцидентов в сфере информационной безопасности показывает, что злоумышленники, стремящиеся нанести ущерб хорошо защищённой системе, чаще всего начинают с атаки менее защищённых второстепенных систем. Для предотвращения подобных сценариев, мероприятия по минимизации информационных рисков и обеспечению информационной безопасности должны прорабатываться в рамках единого системного и согласованного подхода на всех уровнях государственного управления, а также на уровне каждого конкретного предприятия. В свете изложенного, безопасность SCADA-систем – это один из первоочередных вопросов, который должен решаться в ходе модернизации белорусских предприятий.

1. Эксперты обнаружили уязвимость в SCADA-системе, управляющей нефтяными скважинами [Электрон. ресурс] // SecurityLab. 2013.- 02 августа. Режим доступа: http://www.securitylab.ru/news/442846.php
2. Немецкие журналисты сообщили об обнаружении уязвимости в SCADA-системе пивоваренного завода [Электрон. ресурс] // SecurityLab. 2013.- 07 мая. Режим доступа: http://www.securitylab.ru/news/440171.php