УДК 351.864.1

Информационная безопасность систем управления производством

Ляхевич А.Г.
Белорусский национальный технический университет

В последнее время в мировой практике всё большую актуальность приобретает тема безопасности систем автоматизированного управления производством (АСУ ТП, SCADA-систем). Реальность современных телекоммуникационных сетей и информационных систем такова, что многие страны вынуждены создавать подразделения по противодействию киберугрозам, а также специальные подразделения для ведения военных действий в киберпространстве. Так, 17 января 2013 г. в Гааге состоялось открытие Европейского центра по борьбе с киберпреступностью (EC3), функционирующего на базе Европола. Израиль выделил 500 млн. долларов на программу по созданию «кибербоевых частей» (Intelligence Corps Unit 8200). Получил подтверждение факт, 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. В 2013 году ожидается рост активности хакеров по поиску уязвимостей в SCADA-системах и выпуску решений для их автоматической эксплуатации. Уже сейчас в свободном доступе появляются инструменты типа 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 АСУ ТП могли эксплуатироваться злоумышленниками удалённо, из любой точки сети Internet. В свете изложенного, безопасность SCADA-систем – это один из первоочередных вопросов, который должен решаться в ходе модернизации белорусских предприятий.