3.3. О проблеме создания российского промышленного «интернета вещей»

БЕТЕЛИН В. Б., акад. РАН, д-р. физ.-мат. наук, проф.
(член Объединенного ученого совета ОАО «РЖД»,
научный руководитель Научно-исследовательского института системных исследований РАН)

1. «Интернет вещей» США – угроза, еще не осознанная российским обществом

Сенат США 24 марта 2015 года принял решение №110 о разработке стратегии развития «ИНТЕРНЕТА ВЕЩЕЙ» как катализатора роста экономики США и ускорении разработки и внедрения «ИНТЕРНЕТА ВЕЩЕЙ».

В 2016 г. Рабочей группой, включающей представителей промышленности, академических, правительственных и других структур США был подготовлен 30-страничный документ (далее Документ), содержащий стратегические политические рекомендации, принятие которых, по мнению авторов, должно обеспечить безусловное лидерство США в технологии «интернета вещей» [1].

На странице 12 Документа констатируется, что свободное перемещение цифровых данных через границы позволяет компаниям США способствовать инновациям, росту и созданию рабочих мест в Америке. Федеральное правительство должно энергично защищать свободу организации трансграничных потоков цифровых данных путем торговых соглашений и других механизмов принуждения торговых партнеров. То есть, обеспечить право компаниям США хранить, обрабатывать и манипулировать своими данными в пределах границ страны. Именно **эти зарубежные компании**, а не российский потребитель, и **будут реально управлять** функционированием **всем промышленным оборудованием**, цифровые системы управления которым (промышленные контроллеры) **приобретены по импорту** или собраны из **импортных комплектующих**.

Очевидно, что в существующих экономических и производственных условиях, внедрение в России «ИНТЕРНЕТА ВЕЩЕЙ» в варианте, реализуемом зарубежными лидерами глобальных рынков полупроводников и радиоэлектроники, приведет только к увеличению объемов закупаемой у этих компаний продукции и, как следствие, к еще большей импортозависимости России и существенному возрастанию вероятности кибератак прежде всего на импортные, или собранные на основе импортных комплектующих, промышленные контроллеры в энергетической, транспортной и нефтегазовой отраслях России.

Вирус Stuxnet, способный выводить из строя физические устройства, которые управляются контроллерами фирмы SIEMENS, путем механического разрушения этих устройств, был обнаружен в июне 2011 года. По данным открытых публикаций (Нью-Йорк Таймс, 24 июня 2012 г.) этими

целевыми физическими устройствами являлись центрифуги иранской подземной фабрики по обогащению урана, которые управлялись контроллерами фирмы SIEMENS [2].

Существует реальная угроза того, что на основе этой отработанной технологии будут созданы (или уже созданы) варианты Stuxnet для атаки на контроллеры зарубежных компаний, применяемые в российских транспортных и энергетических системах, о чем свидетельствуют недавние атаки на гидроэлектростанцию в Венесуэле, а также недавние сообщения газеты Нью-Йорк Таймс о планируемых МО США кибератаках на энергетическую инфраструктуру России.

2. Уровень безопасности и надежности «ИНТЕРНЕТА ВЕЩЕЙ» США – минимальный экономически приемлемый для производителя

Действительно, массовые коммерческие аппаратные и программные продукты зарубежных компаний INTEL, MICROSOFT, HP, CISCO, SIEMENS и т. д., обладают наилучшими показателями производительность/стоимость, но обеспечивают при этом только **экономически приемлемый для производителя, уровень безопасности и надежности**, недостаточный для использования в системах с критической миссией.

О непреднамеренно возникших уязвимостях аппаратных и программных продуктов этих компаний, создающих угрозу работоспособности информационных систем на их основе, свидетельствуют официальные документы, этих компаний.

Не декларированные возможности в коммерческой аппаратуре и драйверах относятся к категории уязвимостей, которые **не могут быть компенсированы** на более высоких программных уровнях информационно-управляющей системы и могут являться средством злоумышленного несанкционированного доступа к их критическим ресурсам. Об этом, собственно, и свидетельствует проникновение целевого вируса Stuxnet в компьютерную сеть иранской фабрики по обогащению урана через уязвимость коммерческого драйвера интерфейса USB.

Россия, имея, аналогичные по сути проблемы безопасности киберинфраструктуры, что и США, **принципиально ограничена** в части возможностей компенсирования непреднамеренно созданных уязвимостей. Прежде всего потому, что российским специалистам **недоступны детальные данные о перечнях** и особенностях проявления обнаруженных производителями **уязвимостей** элементной базы (INTEL, AMD, CISCO, и т. д.) и программного обеспечения (MICROSOFT). Это обстоятельство **не позволяет ни достоверно оценить реальный уровень безопасности** и надежности существующей в нашей стране киберинфраструктуры, ни сколь-нибудь эффективно противодействовать наиболее опасным кибератакам целевых вирусов типа Stuxnet. Вирусы этого типа имеют высокий уровень скрытности распространения,

вторжения и воздействия, поскольку созданы на основе **детальных знаний о возможностях и уязвимостях** MICROSOFT WINDOWS.

3. Непреднамеренные уязвимости – неизбежный результат стратегии «двойного сокращения»

Небезопасность аппаратного уровня, возникающая из-за появления непреднамеренных уязвимостей – это очевидное следствие **первичности рыночных требований** к аппаратуре и **вторичности требовании к ее безопасности**. Действительно, годовые объемы производства микропроцессоров (универсальных и графических), и коммуникационных контроллеров составляют десятки и сотни миллионов штук, то есть относятся к категории товаров массового спроса. В ту же категорию попадают и компьютеры (мобильные, моноблоки, микросерверы, серверы и т. д.), и коммуникационная аппаратура на их основе. Как и для любых других производителей товаров массового спроса, конкурентная борьба на этих рынках требует от производителей IT-продуктов следования стратегии **«двойного сокращения»**.

- сокращения времени жизни производимого продукта;
- сокращения сроков разработки **нового продукта с новыми функциональными свойствами**.

Очевидно, что сокращение сроков разработки нового продукта (микропроцессора, компьютера на его основе) и соответствующих новых информационных сервисов, ведет к снижению качества тестирования и **выпуску и аппаратных и программных продуктов с дефектами защиты**. О чем, например, и свидетельствуют материалы корпорации INTEL.

4. Преднамеренно созданные уязвимости

Согласно сообщению Лаборатории Касперского, Агентство Национальной Безопасности (АНБ, NSA) США использует централизацию производства жестких дисков в своих целях, заставляя Western Digital и Seagate встраивать шпионящие программы АНБ прямо в прошивку жестких дисков. Это дает агентству прямой доступ к данным, независимо от раздела, файловой системы, операционной системы и т. д. Лаборатория Касперского сообщает, что ПК с одной или двумя следящими программами были найдены в 30 странах. Самое большое количество заражений обнаружено в Иране. Далее идут Россия, Пакистан, Афганистан, Китай, Мали, Сирия, Йемен и Алжир.

О возрастании угрозы кибератак свидетельствуют также данные о том, что с 2008 года микропроцессоры и коммуникационные контролеры компаний INTEL, AMD и ARM включают от одного до трех микропроцессорных ядер, которые аппаратно защищены от доступа, как из операционной системы, так и из прикладной программы. Эти дополнительные ядра доступны из внешней

сети и имеют возможность контролировать весь сетевой поток на входе и выходе микропроцессора, до того, как к нему будут применены какие-либо механизмы шифрования, выполняемых «штатными» ядрами микропроцессоров. Отсюда следует, что никакую систему обработки данных на основе микропроцессоров INTEL, AMD и ARM выпуска 2008 года и позже принципиально невозможно защитить от внешних воздействий программным путем.

5. Основа российского промышленного «ИНТЕРНЕТА ВЕЩЕЙ» – модель производства долгоживущих, надежных, ремонтопригодных изделий

На основе этой модели в настоящее время и в России, и в других промышленно развитых странах, ведется разработка, серийное производство и сопровождение изделий стратегических отраслей – вооружения и военной и авиационно-космической техники, изделий тяжелого энергетического, транспортного и атомного машиностроения, судостроения, станкостроения и т. д. Требования к характеристикам цифровых систем управления этими изделиями, таким, как надежность, готовность, долговечность, ремонтопригодность должны соответствовать, в целом, аналогичным требованиям, предъявляемым к собственно этим изделиям. То есть, Россия, в принципе, могла бы полностью контролировать эту нишу своего внутреннего микроэлектронного и радиоэлектронного рынка, на котором в настоящее время доминирует продукция крупных зарубежных компаний. Таких, например, как компания SIEMENS, которая наряду с турбинами, электрогенераторами, скоростными поездами и. т. д. разрабатывает и производит цифровые системы управления для этих изделий. Заменить цифровые системы управления в этих изделиях компании SIEMENS какими-либо российскими аналогами, конечно невозможно, но заменить контроллеры компании SIEMENS российскими аналогами в системах управления отечественными турбинами, электрогенераторами и энергосистемами вполне возможно на основе имеющегося в России научно-технологического и производственного заделов. Более того, **критически важно**, поскольку **именно контроллеры** компании SIEMENS уже **были объектами атаки** вирусом Stuxnet. Потенциальными потребителями отечественных промышленных контроллеров такого класса, наряду с теплоэнергетической отраслью, является ГК РОСАТОМ, в части применения в системах управления атомными энергетическими установками, АО «РЖД», в части применения в системах управления локомотивами, стрелочными и сигнальными системами, нефтегазовые компании России, в части систем управления добычей, транспортировкой и переработкой нефти и газа.

6. Концепция доверенной аппаратно-программной платформы российского промышленного «ИНТЕРНЕТА ВЕЩЕЙ»

Безопасная и надежная аппаратно-программная платформа, для которой

требования безопасности и надежности (**«доверенность»/«стоимость»**) являются первичными, основополагающими, и которая, по сути, представляет собой **специальную систему**, не может и не должна создаваться на основе стратегии «**двойного сокращения**» и **первичности** показателя «**производительность/стоимость**». То есть, обеспечивать «**экономически неприемлемый**» для INTEL и MICROSOFT уровень безопасности.

Кибербезопасность нельзя обеспечить или оценить постфактум путем анализа исходных текстов программ и тестирования аппаратуры уже созданных систем или их компонент. Она закладывается на начальных этапах разработки и аппаратуры, и программного обеспечения систем автоматизированного управления, путем контролирования (сертификации) процесса разработки и реализации этих систем, что собственно гарантирует их безопасность.

Доверенная отечественная аппаратно-программная платформа должна **обеспечить выполнение миссии**, созданной на ее основе информационно-управляющей системы, **независимо от наличия** допущенных при разработке платформы **ошибок** и **уязвимостей** и попыток **злонамеренных** внешних **воздействий**, как то:

- ошибки в элементной базе, компьютере, операционной системе, прикладной программе;
- нештатное поведение окружения;
- целенаправленные деструктивные воздействия;

Необходимо отметить, что решить эту триединую задачу методом распознавания вредоносного программного обеспечения (антивирусы) очевидно невозможно, а в отношении целевых вирусов типа STUXNET использование этих методов просто не имеет смысла.

Доверенная отечественная аппаратно-программная платформа, включая коммуникационный сегмент (маршрутизаторы) должна основываться **на аппаратной и программной избыточности ее базовых составляющих**:

- сложно-функциональной элементной базы для средств вычислительной и коммуникационной техники;
- операционной системы и прикладных программ;

обладающих развитыми средствами самоконтроля их функционирования.

Нейтрализация угроз безопасности обеспечивается в таких системах путем создания комплекса взаимосогласованных и взаимоувязанных аппаратных и программных средств анализа и самоконтроля корректности функционирования основных компонент информационной системы и их самолечения (исправления ошибок).

7. ФГУ ФНЦ НИИСИ РАН и АО «КБ «КОРУНД-М» обладают научно-технологическим заделом, необходимым для создания аппаратно-программной платформы российского промышленного «ИНТЕРНЕТА ВЕЩЕЙ»

1. Ключевыми составляющими этого задела являются:

• технология проектирования и серийного производства долгоживущих, ремонтопригодных ЭВМ, электронных модулей семейства БАГЕТ высокой надежности и готовности;

• технология проектирования и серийного производства СБИС (32^x и 64^x разрядные микропроцессоры и сложные контроллеры) высокой надежности;

• технология создания и серийного производства долгоживущих ремонтопригодных аппаратно-программных комплексов высокой надежности и готовности на основе интеграции ЭВМ, электронных модулей семейства БАГЕТ, операционной системы ОС РВ БАГЕТ и прикладного программного обеспечения, функционирующих в рамках этой ОС.

Показатели долговечности, надежности, готовности и ремонтопригодности ЭВМ и электронных модулей семейства БАГЕТ, которые серийно производятся уже 25 лет, подтверждены результатами их эксплуатации у потребителей.

2. В ОС РВ БАГЕТ 3.0 реализованы средства самоконтроля в соответствии со стандартом ARINC 653 (монитор здоровья), обеспечивающие диагностику восьми классов ошибок: питания, аппаратуры, защиты памяти, стека и т. д. Реакции на эти ошибки определяет разработчик приложений.

3. Разработаны и серийно производятся 64х разрядные микропроцессоры 1890ВМ8Я и 1890ВМ108 по технологии 65 нм, функциональные возможности которых достаточны для реализации на их основе широкого класса промышленных контроллеров.

4. На основе микропроцессоров 1890ВМ8Я и 1890ВМ108 разработаны и производятся малыми партиями образцы промышленных контроллеров, планируемых к применению в системах управления насосами нефтяных скважин (БАГЕТ-ПК на базе модуля БТ74-201) и стрелочными механизмами на железнодорожных станциях.(на базе модуля ММ05Р). Контроллеры функционируют под управлением ОС РВ БАГЕТ.

СПИСОК ЛИТЕРАТУРЫ

1. Бетелин В. Б. О проблеме диверсификации производства на предприятиях оборонно-промышленного комплекса России // Инновации. 2018. № 7.
2. Бетелин В. Б. Надо уметь жить в условиях киберопасности // Connect. 2016. № 8.