# Надо уметь жить
## в условиях киберопасности

**Владимир БЕТЕЛИН,**
*академик РАН*

Иностранная радиоэлектроника, созданная в условиях стратегии «двойного сокращения», зачастую содержит уязвимости, которые и провоцируют возникновение проблем при обеспечении информационной безопасности. Простое копирование технологий и их локализация в рамках стратегии импортозамещения не позволяют решить эти проблемы. Для создания надежных и безопасных вычислительных систем с критической миссией при их разработке необходимо учитывать требования по информационной безопасности.

### Плата за лидерство на глобальном мировом рынке радиоэлектроники – непреднамеренные уязвимости

**Непреднамеренно возникшие уязвимости и источники ненадежности массовых коммерческих аппаратных и программных продуктов компаний – лидеров мирового рынка**

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, создающих угрозу работоспособности информационных систем на их основе, свидетельствуют официальные документы этих компаний.

В качестве примера рассмотрим продукты Intel. В документе компании № 326767-004 от сентября 2012 г. декларируется: «…корпорация Intel снимает с себя всякую ответственность, которая может возникнуть при ненадлежащем функционировании продуктов корпорации в «системах с критической миссией». В документе № 324209-012 говорится: «Корпорация Intel официально заявляет, что продукты, описанные в документации, могут содержать дефекты или ошибки, которые могут вызвать отклонения реального поведения продуктов от поведения, описанного в опубликованных спецификациях…». По состоянию на май 2012 г. в процессорах Intel Xeon 5000 Series известно о 121 ошибке, десять из которых приводят к неустранимому зависанию процессора. По заявлению компании Intel, «пути обхода этих десяти ошибок неизвестны».

Другими словами, корпорация Intel официально уведомляет потребителей, что ее коммерческие продукты могут обладать недекларированными возможностями (НДВ), и приводит опубликованный на текущий момент их перечень для конкретного семейства микропроцессоров. Это фактически исключает какую-либо возможность обоснования технических и юридических гарантий того, что системы, построенные на основе таких продуктов, не будут обладать недекларированными возможностями, в том числе позволяющими получить несанкционированный доступ (НСД) к ресурсам системы.

Аналогичная ситуация с надежностью и безопасностью коммерческих периферийных (SATA, USB и др.) и коммуникационных контроллеров, драйверов для этих устройств, сетевых маршрутизаторов Cisco и т. д.

Недекларированные 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, 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 сколько-нибудь эффективно противодействовать наиболее опасным кибератакам целевых вирусов типа Staxnet. Вирусы этого типа имеют высокий уровень скрытности распространения, вторжения и воздействия, поскольку созданы на основе детальных знаний о возможностях и уязвимостях операционной системы Microsoft Windows.

**Преднамеренно созданные уязвимости**

До недавнего времени существование уязвимостей, преднамеренно созданных производителями аппаратных и программных средств, было лишь гипотетической возможностью. В последние годы, после разоблачений Эдварда Сноудена, стали появляться публикации материалов, косвенно подтверждающих связи производителей аппаратных и программных продуктов с федеральными агентствами США. Так, например, в начале 2015 г. российская компания «Лаборатория Касперского» опубликовала факты, косвенно свидетельствующие о том, что АНБ (Агентство национальной безопасности США) контактировало с производителями жестких дисков в целях получения информации, позволяющей преднамеренно создавать уязвимости. За последние пять лет количество стран, производящих жесткие диски, сократилось с трех (Корея, контролировавшая производство накопителей Samsung, Япония, производившая Hitachi и Toshiba, и Америка, контролировавшая производство Seagate и Western Digital), до одной (Америка). Корейские и японские производители жестких дисков были поглощены либо стали дочерними компаниями или ответвлениями американских производителей Seagate и WD. По сообщению «Лаборатории Касперского», АНБ использует централизацию производства жестких дисков в своих целях, заставляя Western Digital и Seagate встраивать шпионящие программы непосредственно в прошивку жестких дисков. Это обеспечивает 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.

«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.

## Отечественная сложнофункциональная элементная база на основе «отверточных технологий»

Сегодня в России использование заемных комплектующих, технологий и производств фактически никак не регламентировано, в том числе и в части требований к надежности и безопасности создаваемых на их основе продуктов.

По сообщению агентства CNews от 25.05.2015 г., созданная около трех лет назад компания «Байкал-Электроникс», являющаяся дочкой компании «Т-Платформы», выпустила «отечественный» процессор Baikal-T1, который собран из лицензионных IP-блоков 32-разрядного суперскалярного ядра микропроцессора Warrior P-Class P5600 компании Imagination Tecnologies и зарубежных лицензионных IP-блоков интерфейсов Ethernet, PCI, SATA, USB. Baikal-T1 планируется производить на заемном производстве компании TSMC (Тайвань) по технологии КМОП 28 нм.

По сообщению CNews от 08.07.2015 г., этот микропроцессор будут поставлять «Газпрому» для систем телеметрии и телемеханики, т. е. систем с безусловно критической миссией. Особо важным в связи с этим является сообщение из университета штата Мичиган о реализованном методе встраивания в микропроцессор на стадии его производства вредоносной модификации, которую практически невозможно обнаружить [1].

## 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 требования к ее безопасности. Действительно, годовые объемы производства микропроцессоров (универсальных и графических) и коммуникационных контроллеров составляют десятки и сотни миллионов штук, т. е. 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 ИТ-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 аппаратных и программных продуктов с дефектами защиты. О чем, собственно, и свидетельствуют приведенные выше материалы корпорации Intel.

Из вышеизложенного, в частности, следует, что, даже если пренебречь опасностью преднамеренных уязвимостей, создание отечественных микропроцессоров и коммуникационных контроллеров на основе лицензированных коммерческих IP-блоков и микропроцессорных ядер зарубежных производителей (POWER 7/8, ARM, MIPS-Imagination), разработанных на основе стратегии «двойного сокращения», позволит построить на этой базе информационные системы только с минимальным, экономически приемлемым уровнем безопасности. То есть в созданных с использованием импортных IP-блоков отечественных микросхемах были, есть и будут непреднамеренно созданные уязвимости, создающие реальную угрозу работоспособности разработанных на их основе аппаратных продуктов просто в силу того, что зарубежные коммерческие компании, создающие эти IP-блоки, включая Imagination Tecnologies, ведут свою работу также на основе стратегии «двойного сокращения». Поэтому даже наличие исходной документации на эти IP-блоки у отечественных компаний не является гарантией отсутствия таких уязвимостей, в том числе в микропроцессоре Baikal-T1.

> На программном уровне первоочередная задача – разработка и внедрение средств самоконтроля операционной системы типа Health Monitor стандарта ARINC 653.

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».

## О доверенной отечественной аппаратно-программной платформе

Требования гарантированного уровня безопасности и надежности должны закладываться как первичные на начальных этапах разработки аппаратуры и программного обеспечения.

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) 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.

Такую платформу нельзя создать на основе лицензионных микропроцессорных ядер и IP-блоков интерфейсов зарубежных компаний даже при предоставлении последними полной исходной документации. При огромной сложности и объеме этой документации (десятки миллионов строк исходного кода) даже непреднамеренные уязвимости могут быть обнаружены только в результате длительной и дорогостоящей работы большого коллектива специалистов, имеющих многолетний опыт разработки микропроцессоров такого же уровня сложности. Причем в течение длительного периода проведения работы по поиску уязвимостей импортных продуктов отечественными специалистами потенциальный киберпротивник может использовать уже известные ему уязвимости микропроцессорных ядер и IP-блоков интерфейсов для организации кибератак на информационные системы, созданные на основе микропроцессора, использующего импортные компоненты и технологии.

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

Нейтрализация угроз безопасности может быть обеспечена путем создания комплекса взаимосогласованных и взаимоувязанных аппаратных и программных средств анализа и самоконтроля корректности функционирования основных компонентов информационной системы и их самолечения (исправления ошибок), в том числе элементов самоконтроля и самокоррекции, встроенных:

- в элементную базу (микропроцессоры, коммуникационные, периферийные и графические контролеры, сложные СБИС);
- в операционную систему;
- в прикладные программы.

В микропроцессоре примерами таких средств являются аппаратное детектирование аномального поведения узлов всего микропроцессора, включая контроль динамического тока и температуры в большом количестве точек (порядка 40); контроль загруженности узлов микропроцессора и системного контроллера (до 100 счетчиков для 200 событий); контроль времени выполнения кода; контроль точек входа и выхода для системных вызовов.

В коммуникационных СБИС – это контроль входного и выходного импеданса физических линий связи для обнаружения несанкционированного подключения к линии связи; защита физического уровня каналов путем создания в интерфейсном контроллере контрольного символа с введением специального шифра для надежного отделения «своего» от «чужого» и предотвращения атаки через коммуникационный канал; шифрование данных внутри пакетов передач данных; неблокирующие режимы обмена пакетами вследствие замены приоритетов и т. д.

На программном уровне первоочередная задача – разработка и внедрение средств самоконтроля операционной системы типа Health Monitor стандарта ARINC 653. Этот очевидно избыточный с коммерческой точки зрения дополнительный комплекс аппаратных и программных средств должен обеспечить выполнение миссии информационной системы, несмотря на кибератаки, отказы аппаратных и программных компонентов и даже собственные ошибки реализации.

## О вирусах Stuxnet и Flame

Впервые вирус такого типа, который получил название Stuxnet, был обнаружен в июне 2011 г. Он способен выводить из строя физические устройства, которые управляются контроллерами фирмы Siemens, путем механического разрушения этих устройств. 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.

В мае 2012 г. был обнаружен вирус, получивший название Flame, активация которого происходит только в заданных географических зонах. Этот многофункциональный вирус способен перехватывать, изменять и уничтожать информацию в компьютерной сети, включая данные с клавиатуры, аудиофайлы и т. д. До настоящего времени функции этого самого большого из известных вирусов (более 600 тыс. строк кода) до конца не выяснены. По-видимому, с его помощью была собрана информация о компьютерах, топологии компьютерной сети, типах оконечных устройств (контроллеры центрифуг) иранской подземной фабрики. Эта информация была использована при создании вируса Stuxnet.

Автор одной из опубликованных в открытой печати статей подчеркивает, что и до 2012 г. было понятно, что США ведут разработку и распространение (в ждущем режиме) кибероружия, способного уничтожить промышленную инфраструктуру вероятных противников. Однако в 2012 г. возникла принципиально новая ситуация: США практически применили кибероружие в мирное время. ■

***Литература***

*2016 IEEE Symposium on Security and Privacy A2: Analog Malicious Hardware / Kaiyuan Yang, Matthew Hicks, Qing Dong, Todd Austin, Dennis Sylvester.*