С помощью вредоносных программ можно блокировать работу любого предприятия.

Фотобанк Лори

ОРУЖИЕ СТРАТЕГИЧЕСКОГО СБОЯ

Владимир ВОЛЧКОВ

Парализовать электронную технику, организовать массовую кибератаку и мимикрировать под взломщиков из третьих стран. Хакерам нашлось место в обновленной американской военной доктрине.

БОМБА ЗАМЕДЛЕННОГО ДЕЙСТВИЯ

Противостояние нашего времени будет решаться не на земле, в воздухе или воде. Ключевые события развернутся в невидимой сфере - кибернетической. И ее освоение США уже официально прописали в своей военной доктрине. Ряд документов есть в открытом доступе. Поэтому сомневаться в существовании кибероружия возможно только по наивности.

Член-корреспондент НАН Беларуси Анатолий Белоус, заместитель генерального директора по научно-техническим программам и научной работе «Интеграл», проблемами кибербезопасности занимается вплотную больше десяти лет. И с полной уверенностью заявляет: противостояние в киберпространстве не домыслы конспирологов, а реальность. И таковой она стала в том числе благодаря глобализации отрасли микроэлектроники.

Факт общеизвестный, что современные заводы по производству компонентной базы - крайне дорогие, окупаются только за счет больших объемов производства и выхода на глобальные рынки сбыта. Поэтому сегодня практически ни одна страна, даже США, не может обойтись полностью своими силами в производстве сложных электронных систем.

Американцы и китайцы закупают друг у друга микросхемы. Еще чаще используется механизм, когда в развитых странах проводится разработка микросхем, а их производство передается на заводы в третьи государства. В этом и кроется подвох. Анатолий Белоус объясняет:

- Микросхема может содержать больше миллиона транзисторов. И на фабрике-изготовителе могут появиться несколько десятков «лишних» транзисторов - так называемые скрытые трояны. Они ничем себя не проявляют, но только до поры до времени. Это бомба замедленного действия. В определенный момент - через несколько месяцев или даже лет - они «просыпаются». Могут передавать «хозяину» информацию или пагубно влиять на работу всей электронной системы. Вплоть до ее разрушения.

Опасно, когда такие «закладки» попадают в электронные системы.

БОЕВЫЕ ВИРУСЫ

Пожалуй, один из самых известных фактов применения «боевых вирусов» - атака на иранскую ядерную программу. Тогда около тысячи урановых центрифуг вдруг стали работать неадекватно и в итоге остановились. Скрытые трояны разрушили электронные системы управления аппаратами.

Надо отметить, что в этом направлении мировая индустрия значительно продвинулась за последние годы. И технологии внедрения разных вредоносных штучек стремительно совершенствуются. Каждая из стран, претендующих на роль великой державы, старается о своих оппонентах и партнерах знать как можно больше. А еще лучше - внедряться и в нужный момент управлять чужими электронными системами.

Именно поэтому вопрос гарантирования кибербезопасности является одним из ключевых на повестке дня в международных переговорах. В том числе между Россией и НАТО.

ВЫСОКИЙ УРОВЕНЬ

КЛЮЧЕВЫЕ ПАРТНЕРЫ

Успехи радиоэлектронной науки и технологий ставят РБ в один ряд с высокотехнологичными странами мира.

«Интеграл» находится под санкциями уже лет десять. Что в принципе только подтверждает его значимость для национальной безопасности.

Другой вопрос, что современные кибертехнологии развивать очень дорого. В той же Европе созданы по этой тематике кластеры, которые объединяют усилия сотен компаний.

В этом разрезе для Беларуси важно сотрудничество с Россией - ключевым партнером. Президенты РФ и РБ во время подписания союзных программ особое внимание уделяли сотрудничеству в области микроэлектроники.

Эта отрасль развиваться без государственной поддержки не может. Огромные дотации по разным каналам финансирования выделяются в США, Китае, Европейском союзе. В Беларуси и России вложения пока намного скромнее, хотя нельзя сказать, что отрасль полностью обделена вниманием.

Самое главное, что в Беларуси удалось сохранить не только производственную базу, но и научный потенциал, вузовскую школу в области электроники. И при соответствующем финансировании она сможет по уровню компетенций выйти на новую высоту.

КОММЕНТАРИЙ

Владимир АРЧАКОВ, заместитель Госсекретаря Совета Безопасности Беларуси:

- В последние два десятилетия за рубежом проработаны подходы к использованию кибертехнологий в военно-политических целях. Конечно, определяющее влияние на страны НАТО, ЕС оказывает лидирующая роль США в ведении соответствующих противоборств. В их стратегии говорится, что американские военные планируют проводить кибероперации для сбора разведданных и наращивания военного потенциала на случай полномасштабного кризиса. Минобороны США рассматривает операции в киберпространстве как достижение превосходства над потенциальным противником. Суть заключается в повседневном проведении кибероперации без их перерастания в вооруженную агрессию. Вместе с тем допускается возможность реагирования на враждебные кибератаки, которые причиняют ущерб людям либо объектам, как на вооруженную агрессию, что, на наш взгляд, неприемлемо.

НА ЧИСТУЮ ВОДУ

ТРОЯНСКИЙ КОНЬ МИКРОСХЕМУ НЕ ИСПОРТИТ

В республике есть мощная научная школа радиоэлектроники, способная в два счета поймать «засланного казачка».

- Выпустили двухтомник «Программные и аппаратные трояны: способы внедрения, методы защиты». Его уже перевели на английский, французский, испанский и другие языки, сегодня американские, европейские инженеры учатся по белорусским книгам. Мы подробно рассмотрели все возможные на сегодняшний день способы внедрения троянов. И доказали: если заказчик передает производство микросхем на аутсорсинг, существует минимум пять-шесть способов внедрить аппаратный троян, - продолжает Анатолий Белоус.

Как от них защититься? Первый вариант - электронную компонентную базу для стратегических отраслей производить собственными силами. Но в современных реалиях это очень дорого и практически невозможно осуществить, даже богатым странам.

Надо отметить, что в этом разрезе «Интеграл» является предприятием не столько коммерческим, сколько обеспечивающим белорусскую безопасность. И российскую тоже. Да, возможно, производственная база не самая мощная. Минимальная проектная величина изделий - 0,35 микрона. Кажется, что это очень много. Фабрики-лидеры в мировой полупроводниковой индустрии уже перешли на размерность четырнадцать нанометров.

По сравнению с этими крошками белорусские интегральные микросхемы выглядят великанами. Но все же больше половины элементной базы в мире сегодня производится в размерном ряде больше 0,25 микрона. Поэтому продукция «Интеграла» обеспечена спросом на ближайшие двадцать лет.

Но самый важный и принципиальный фактор - «Интеграл» является ключевым предприятием для формирования компетенций и развития научного потенциала в радиоэлектронике. По некоторым направлениям, например, вопросам воздействия различных излучений на электронные системы, белорусская школа является одной из лучших в мире.

Если невозможно отказаться от международной кооперации, то, обладая знаниями и опытом, есть возможность разработать системы защиты от тех же аппаратных троянов.

Анатолий Белоус объясняет: этими вопросами в США серьезно занимаются уже лет двадцать. Разработали большое количество стандартов, которые становятся барьером для несанкционированного внедрения в стратегические электронные системы. Огромную работу в этом направлении проводит Китай. В Беларуси этой проблематикой занялись вплотную лет десять назад. Разработали методику, сложную систему математических моделей, которые позволяют изготовленную за рубежом микросхему сравнить на соответствие с тем шаблоном, который передавали на фабрику разработчики для ее производства. Наши разработки позволяют среди миллионов транзисторов найти несколько десятков «лишних» и их блокировать.