Висновки

Розроблений пакет нормативних документів [1–5] був першим в системі НД ТЗІ, що регламентує проведення в замкненій системі ТЗІ випробувань РВ і забезпечує єдині умови для класифікації, приймальних випробувань, періодичних повірок і сертифікації РВ діапазону частот 10 кГц – 18 ГГц на відповідність показників призначення.

Література: 1. НД ТЗІ 1.5-001-2000 "Радіовиявлювачі. Класифікація. Загальні технічні вимоги", затверджений наказом ДСТСЗІ СБУ від 13. 06. 2000 р. № 29. 2. НД ТЗІ 2.3-004-2001 "Радіовиявлювачі індикаторні. Методи та засоби випробувань", затверджений наказом ДСТСЗІ СБУ від 09. 04. 2001 р. № 12. 3. НД ТЗІ 2.3-001-2001 "Радіовиявлювачі вимірювальні. Методи та засоби випробувань", затверджений наказом ДСТСЗІ СБУ від 27. 02. 2001 р. № 5. 4. НД ТЗІ 2.3-005-2001 "Радіовиявлювачі панорамні. Методи та засоби випробувань", затверджений наказом ДСТСЗІ СБУ від 11. 09. 2001 р. № 54. 5. НД ТЗІ 2.3-006-2001 "Радіовиявлювачі аналізувальні. Методи та засоби випробувань", затверджений наказом ДСТСЗІ СБУ від 06. 11. 2001 р. № 64. 6. Ван Трис Г. Теория обнаружения, оценок и модуляции. Том I. / Пер. с англ. под ред. проф. В. Т. Горяинова.– М.: Сов. радио, 1975. 7. Обнаружение радиосигналов. / П. С. Акимов, Ф. Ф. Евстратов и др.; Под ред. А. А. Колосова.– М.: Радио и связь, 1989. 8. Левин Б. Р. Теоретические основы статистической радиотехники. Книга первая.– М.: Сов. радио, 1969. 9. Ли У. Техника подвижных систем связи. / Пер. с англ. – М.: Радио и связь, 1985. 10. ДСТУ 2427-94 Приймачі радіомовні. Класифікація. Основні параметри. Загальні технічні вимоги.

УДК 638.235.231

МЕТОДЫ И СРЕДСТВА СЕРТИФИКАЦИИ СЛОЖНЫХ ЭЛЕКТРОННЫХ СИСТЕМ НА СООТВЕТСТВИЕ СПЕЦИФИЦИРОВАННЫМ ФУНКЦИЯМ

Валерий Горбачев, Владимир Степаненко, Сергей Саранча
Харьковский национальный университет радиоэлектроники

Анотація: **Розглядаються питання, пов'язані з розробкою методів та засобів сертифікації складних електронних систем на відповідність специфікованим функціям.**
Summary: **In the given work the questions connected with development of methods and means of certification of complex electronic systems for conformity to the specified functions are considered.**
Ключові слова: **Інформація, апаратні засоби, закладний пристрій, інформаційна безпека.**

I Введение

Развитие и широкое применение электронной вычислительной техники в промышленности, управлении, связи, научных исследованиях, образовании, сфере услуг, коммерческой, финансовой и других сферах человеческой деятельности являются в настоящее время приоритетным направлением научно-технического прогресса. Масштабы и сферы применения этой техники стали таковы, что на сегодняшний день, наряду с проблемами надёжности и устойчивости её функционирования возникает проблема обеспечения безопасности циркулирующей в ней информации.

Решение этой проблемы, несмотря на большой объём проведенных исследований, усложняется ещё и тем, что до настоящего времени в Украине и за рубежом отсутствуют единые и общепринятые теория и концепция обеспечения безопасности информации в автоматизированных системах её обработки.

На данном этапе во всем мире активно разрабатываются всевозможные программные средства защиты информации от несанкционированного доступа и разрушения. В то же время проблема поиска цифровых закладных устройств в вычислительной технике и любой цифровой технике вообще является практически не исследованной. Поскольку уровень аппаратных средств является самым низким уровнем доступа к информации, то контроль над доступом, осуществляемым при помощи аппаратных средств, невозможно осуществлять на программном уровне. Таким образом, поиск аппаратных закладных устройств, а также контроль за функционированием аппаратных ресурсов вычислительной техники, возможно, осуществлять только с использованием специализированного диагностического оборудования, а также программного обеспечения, входящего в его состав. Ниже *аппаратной закладкой (АЗ)* считается некоторое функционально-

структурное изменение электронного устройства, приводящее к тому, что данное устройство становится активным источником угрозы безопасности информации.

Поскольку закладные устройства, введенные в структуру серийных устройств, могут иметь полный доступ ко всем ресурсам, доступным данному устройству, то эффект от использования таких закладных устройств и вред, наносимый с их помощью, может быть значительно большим, нежели от программных закладок. Это связано с тем, что при этом наряду с возможностью несанкционированного доступа к информации (копирование, модификация, разрушение), появляется возможность разрушения аппаратных средств, что ведёт к выходу из строя всего вычислительного комплекса.

В данной работе в качестве объекта защиты информации (ЗИ) рассматривается персональная ЭВМ с полным набором возможных периферийных устройств. Следует отметить, что в работе в качестве объектов ЗИ рассматриваются аппаратные ресурсы ПЭВМ и не рассматриваются аспекты ЗИ, связанные со всевозможными видами излучений либо криптографическими способами ЗИ.

В ходе анализа литературы было рассмотрено достаточно большое количество публикаций на темы, связанные с защитой информации. При этом были просмотрены публикации зарубежных авторов и разработчиков стран СНГ. На основе просмотренной литературы можно сделать вывод, что на сегодняшний день основное внимание в области ЗИ уделяется вопросам контроля доступа к информации и средствам её обработки, а также всевозможным методам шифрования и кодирования информации, циркулирующей как внутри отдельно взятой вычислительной системы, так и предаваемой посредством локальных или глобальных сетей.

В то же время, поскольку современные компьютерные системы строятся на базе комплектующих, произведенных за рубежом, необходимо учитывать возможность внедрения в их структуру аппаратных закладок, позволяющих самой ЭВМ производить несанкционированные накопление, модификацию, а также передачу информации.

II Особенности сертификации электронных систем

В работе проблема обнаружения аппаратных закладок в электронных системах рассматривается как сертификация изделий компьютерной техники. Переходя к сертификации электронных систем, прежде всего, необходимо определить значение самого понятия «сертификация».

Согласно определениям, имеющимся в отечественной литературе, сертификация – это действие, удостоверяющее посредством знака или сертификата соответствие изделия требованиям определенных стандартов или технических условий [2].

Это определение является очень обобщённым и в рамках рассматриваемых вопросов необходима более чёткая формулировка, с учётом специфики темы.

Под *сертификацией* сложных электронных систем на соответствие специфицированным функциям предлагается понимать *совокупность действий, позволяющих произвести анализ структуры и тестирование электронных систем с целью определения степени соответствия специфицированным функциям, а также выявления наличия не специфицированных функций, с последующей выдачей сертификата соответствия*.

Таким образом, обнаружение в ходе сертификации электронных устройств функций, не заявленных производителем, позволяет утверждать, что данное оборудование кроме действий, непосредственно необходимых для его функционирования, выполняет ещё некоторые действия, о функциях которых пользователю этого оборудования ничего не известно. В случае рассмотрения в качестве сертифицируемой системы оборудования, используемого для обработки, передачи либо накопления информации, наличие не специфицированных функций оказывается однозначно связанным с вопросом защиты информации. Таким образом, обнаружение не специфицированных функций позволяет утверждать, что данные технические средства не соответствуют заявленным функциям и, следовательно, не могут использоваться в системах, требующих высокого уровня безопасности и защиты информации.

Методы сертификации электронных систем на наличие АЗ можно разбить на две группы: методы разрушающего контроля и методы неразрушающего контроля. Методы разрушающего контроля, такие как радиационный анализ, рентгеноскопия, физическое разрушение, основывающиеся на изучении топологии электронных компонентов, практически не могут быть использованы в силу сложности современной цифровой техники. Обнаружение АЗ методами неразрушающего контроля является достаточно новым направлением, в рамках которого требуется разработать:

- теоретическую базу сертификации электронных систем на соответствие специфицированным и неспецифицированным функциям;
- методику сертификации электронных систем на соответствие специфицированным функциям, а также её правовую основу;

- инструментальные средства сертификации;
- формальные и физические модели АЗ, располагающихся в компьютерных системах (КС).

Теперь коротко о каждой задаче.

Теоретические основы сертификации лежат в области системного анализа, имитационного моделирования и технической диагностики, основной функцией которых, как научных направлений, является оценка качества изделия на этапах проектирования, производства и эксплуатации.

Методика сертификации электронных систем, как метод защиты информации, должна соответствовать нормам и правилам Украинской государственной системы сертификации продукции. Для решения этой задачи потребуется разработка соответствующих нормативных документов.

В отличие от пользователя ПЭВМ для разработчика аппаратные средства являются полностью контролируемой средой. Поэтому он может реализовать закладку с практически неограниченными возможностями. Кроме того, если программная закладка, реализованная в рамках операционной системы (ОС), незаметна для пользователя, то она может быть обнаружена при помощи дополнительных программных или аппаратных средств. В случае же с аппаратными закладками их обнаружение при помощи программных средств невозможно, поскольку они работают на более низком уровне, контроль над которым невозможен при помощи программных средств.

Проводя анализ структуры современных КС с точки зрения защищённости от угроз, исходящих от интегральных схем (ИС), прежде всего надо ответить на вопрос: "какими возможностями может обладать аппаратная закладка?" Иными словами необходимо определить классы АЗ устройств, которые будут рассматриваться далее. Решение этих задач позволит существенно упростить поиск АЗ.

Рассмотрим несколько возможных классов аппаратных закладок:

- закладные устройства разрушающего (блокирующего) типа;
- закладные устройства накапливающего типа;
- закладные устройства, изменяющие протокол передачи данных;
- высокоуровневые закладные устройства.

Предлагается проводить анализ возможных мест размещения АЗ с учётом определённых выше классов, а также учитывая эффективность их функционирования.

В настоящее время в нашей стране широко используются персональные компьютеры нескольких поколений. Характерной особенностью всех последних поколений персональных компьютеров является наличие чипсетов. Обобщённая структура компьютеров на базе Pentium процесора показана на рисунке 1.

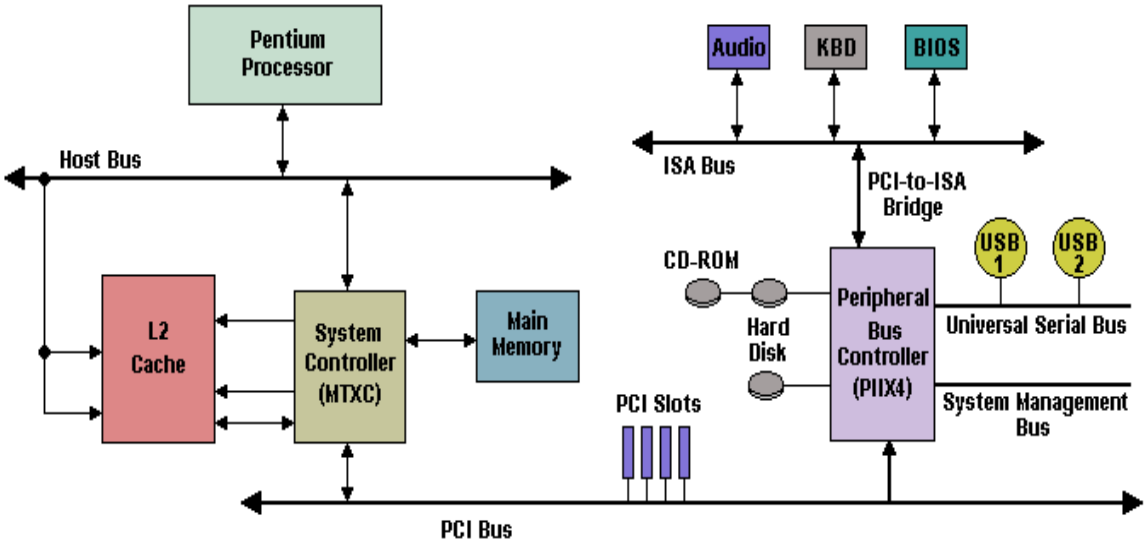

Рисунок 1 – Обобщённая структура компьютера на базе процессоров Pentium

Современный компьютер представляет собой электронное устройство с высокой степенью интеграции. Следовательно, в случае размещения АЗ в чипсете компьютера, можно получить полный доступ ко всем ресурсам ЭВМ.

Далее необходимо рассмотреть возможность внедрения АЗ вышеприведенных типов в чипсетах компьютеров и целесообразность использования каждого конкретного типа АЗ.

Очевидно, что АЗ разрушающего (блокирующего) типа могут размещаться в любых ИС. Не исключением являются и ИС чипсетов ПЭВМ. Введение подобной АЗ в структуру стандартной ИС не требует практически

никаких дополнительных ресурсов. Таким образом в случае активации подобной АЗ это приведёт к полной либо частичной функциональной непригодности ИС, а внешне это будет выглядеть как обычная неисправность.

Рассматривая возможность внедрения АЗ накапливающего типа в чипсеты ПЭВМ необходимо учитывать, что устройства этого типа целесообразно размещать в местах с циркуляцией явно выраженной информации. Таким образом, можно сделать вывод о том, что размещение подобных АЗ в чипсетах, а именно, непосредственно на PCI либо ISA шинах, в контроллерах IDE, USB, является нецелесообразным. Это связано с тем, что объёмы информации, циркулирующей по этим шинам очень велики, что делает мало возможным её накопление за большой промежуток времени, а практический смысл от её накопления в этом случае очень невелик. Исключение в этом случае составляет интегрированный контроллер клавиатуры, и этот вопрос будет рассмотрен более подробно далее.

Размещение АЗ, изменяющих протокол передачи данных, очевидно, должно осуществляться непосредственно в устройствах, осуществляющих передачу данных во внешнюю среду, например в модемах и сетевых картах. В связи с тем, что в настоящее время наблюдается тенденция интеграции сетевых карт, а вскоре возможно и модемов непосредственно на материнские платы (*Intel 815E, 820E chipset*), размещение АЗ данного типа непосредственно в чипсетах также вероятно.

Высокоуровневые закладные устройства предполагают возможность доступа ко всем ресурсам ПЭВМ и поэтому должны располагаться непосредственно в чипсетах. Однако при этом возникают трудности, связанные с тем, что АЗ не может обладать информацией обо всех возможных конфигурациях периферийного оборудования. Основной угрозой, исходящей от данных АЗ, является возможность несанкционированной передачи третьей стороне любой информации, хранящейся либо циркулирующей внутри ПЭВМ. В связи с этим АЗ должна обладать возможностью управления устройствами, осуществляющими обмен информацией с внешней средой, а именно модемами и сетевыми картами. На этом этапе и возникают трудности, связанные с тем, что на сегодняшний день количество комплектующих различных фирм производителей настолько велико, а их технические характеристики и функционирование так различно, что это делает возможность функционирования подобных АЗ практически невозможным. Это связанно с тем, что, как правило, все производители закладывают свои алгоритмы управления. В этом случае для корректного функционирования устройства необходимо помимо возможности физического доступа к управляемому устройству обладать полной информацией о его параметрах, хранящейся на уровне драйверов операционной системы. Таким образом, поскольку доступ к этой информации для АЗ невозможен (оно располагается на более низком уровне), то функционирование высокоуровневых АЗ в этом случае делается практически невозможным.

Останавливаясь более подробно на АЗ накапливающего типа, надо отметить, что наиболее вероятные места размещения подобных АЗ – это всевозможные периферийные устройства, объём циркулирующей информации в которых невелик и её накопление имеет явно выраженный практический смысл. Например, очень опасным для КС является размещение закладных устройств накапливающего типа в клавиатурах. При этом вся накапливаемая информация имеет явно выраженный характер и для её анализа не требуется много времени. Кроме того, поскольку, как правило, через клавиатуру вводится большое количество информации и, что самое главное, пароли доступа, то вопросу защиты клавиатуры надо уделять особое внимание.

Далее необходимо рассмотреть возможности внедрения АЗ накапливающего типа в принтеры и модемы, поскольку эти периферийные устройства также очень сильно распространены.

При внедрении АЗ накапливающего типа в принтеры необходимо учитывать, что информация, передаваемая на печать, имеет достаточно большие объемы. Её накопление при большой интенсивности работы за большой промежуток времени становится проблематичным в связи с тем, что накапливаемая информация должна храниться в энергонезависимой памяти, а ёмкость модулей Flash памяти не очень высока. К тому же их стоимость при размерах свыше 64 Мбайт становится довольно значительной. Однако, поскольку современные принтеры представляют собой достаточно сложные электронные устройства, обладающие достаточно мощными вычислительными ресурсами, то возможно применение всевозможных алгоритмов упаковки и сжатия информации, что существенно увеличивает объемы сохраняемой информации. Таким образом, возможность размещения подобных АЗ в принтерах ни в коем случае нельзя исключать и вопросам их выявления также необходимо уделять большое внимание.

Аналогичная ситуация складывается и при рассмотрении возможности внедрения АЗ накапливающего типа в модемы. Объемы циркулирующей здесь информации ещё более значительны по сравнению с клавиатурами и принтерами, но внедрение АЗ данного типа также нельзя исключать. При этом в модемах наиболее целесообразно использовать АЗ комбинированного типа, обладающие возможностью накопления информации с последующей её несанкционированной передачей третей стороне. При этом нельзя не учитывать, что в случае применения криптографических методов закрытия информации, эффективность от

использования данных АЗ сильно снижается.

Закладные устройства, изменяющие протокол передачи данных, очевидно, целесообразно использовать в таких устройствах, как модемы и сетевые карты. При этом данные АЗ могут осуществлять трансляцию передаваемой информации третьей стороне. Как уже отмечалось выше, в случае использования алгоритмов закрытия передаваемой информации эффективность от использования данных АЗ резко падает.

Говоря о сертификации сложных электронных систем на соответствие специфицированным функциям необходимо отметить, что для осуществления сертификации необходимы аппаратно-программные средства.

Структура инструментальных средств представляет собой аппаратно-программный комплекс, в состав которого входят прикладное программное обеспечение и аппаратные средства сертификации. Программное обеспечение должно включать в себя среду моделирования, позволяющую создавать программные модели сертифицируемых устройств, а также получать тестирующие последовательности для осуществления диагностики. Прикладное программное обеспечение должно выполнять следующие функции: инициализация комплекса; задание режимов работы; программная имитация внешней среды для исследуемого объекта; запись в аппаратную часть комплекса тестирующих последовательностей для исследуемого объекта; анализ результатов (обработка и анализ временных диаграмм, полученных от исследуемого объекта). Аппаратная часть комплекса предназначена для выполнения следующих функций: обеспечение аппаратной поддержки прикладного программного комплекса; реализация взаимодействия с исследуемым объектом в режиме реального времени; регистрация состояния и физическая эмуляция внешней среды исследуемой электронной системы.

III Выводы

В заключение хотелось бы отметить, что в данной работе исследуется проблема защиты информации от угроз, исходящих от аппаратных ресурсов КС. Рассматриваются источники угроз, размещение которых возможно как непосредственно в интегральных схемах ЭВМ, так и в периферийном оборудовании. Понятие «закладное устройство», определённое в ДСТУ [5], в работе без изменения сути трактуется как аппаратная закладка. Угроза информации осуществляется за счёт не специфицированных функций электронных систем. Приведём несколько важных характеристик АЗ: установить источник угроз невозможно без специальных инструментальных средств; контроль за угрозами аппаратного уровня невозможно осуществлять на программном уровне.

Эти и другие характеристики делают АЗ очень перспективным компонентом компьютерных диверсий, в том числе, в форме нарушения работы важных государственных и коммерческих систем.

Литература: 1. Анин Борис. Защита компьютерной информации. – СПб.: BHV Санкт-Петербург, 2000. VIII. – 368 с.: ил. 2. Попов М. И. Основы сертификации электронной техники. – М.: Издательство стандартов, 1988. – 277 с. 3. Проскурин В. Г. и др. Программно-аппаратные средства обеспечения информационной безопасности. Защита в ОС. – М.: Радио и связь, 2000. – 166 с.: ил. 4. Защита информации: Сборник научных трудов / Киев, Международный университет гражданской авиации.– К: КНИГА, 1999.– 188 с. 5. ДСТУ 2226-93. Автоматизированные системы. Термины и определения.

УДК 681. 324

МЕТОДИКА СИСТЕМАТИЗАЦИИ ХАРАКТЕРИСТИК ТИПОВЫХ КОМПЬЮТЕРНЫХ СИСТЕМ, ВЛИЯЮЩИХ НА ЗАЩИТУ ИНФОРМАЦИИ

Игорь Яковив, Александр Черноног*, Павел Алексийчук*

*Национальная академия СБУ, *ВИТИ НТУУ «КПИ»*

Анотація: **Комп'ютерні системи для формування документів (типові комп'ютерні системи) знайшли широке поширення. Пропонується методика, що дозволяє систематизувати їх характеристики, найбільш важливі для захисту інформації від несанкціонованого доступу.**

Summary: **Computer systems for creation of the documents (the standard computer systems) have found a wide circulation. The technique permitting to systematize their performances, which is most significant for the protection of the information from unauthorized access is offered.**

Ключові слова: **Інформація, інформаційна безпека, комп'ютерна система, захист інформації.**