# МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

УДК 638.235.231

## ФОРМАЛЬНЫЕ ОСНОВЫ МЕТОДОВ БЛОКИРОВКИ АППАРАТНЫХ ЗАКЛАДНЫХ УСТРОЙСТВ

*В.А. ГОРБАЧЕВ*

Рассматривается классификация аппаратных закладных устройств, анализ современных методов их обнаружения и предлагается формальная основа методов проектирования сложных электронных систем, которые блокируют аппаратные закладные устройства.

*Ключевые слова:* модель аппаратной закладки, классификация аппаратных закладок, модель операции доступа, функции управления доступом, оператор сопряжении, оператор управления соединением элементов ЭС.

### ВВЕДЕНИЕ

Высокие экономические затраты вынуждают компании по производству электронной продукции использовать интеллектуальную собственность, средства и технологии сторонних разработчиков. Все это приводит к тому, что сложные ЭС разрабатываются и производятся в сравнительно ненадежной рабочей среде [1-3, 5] и могут быть инфицированы аппаратным вирусом (аппаратным закладным устройством). Аутсорсинг в сфере производства ЭС представляет собой серьезную угрозу, особенно для правительственных учреждений, для военной, финансовой, энергетической и политической сферы. ЭС, содержащие аппаратные закладные устройства или просто аппаратные закладки, показали, что они способны выключать центральный процессор, передавать конфиденциальную информацию и обходить программные механизмы аутентификации пользователя. Таким образом, методы для обнаружения аппаратных закладных устройств находятся в центре внимания исследования безопасности IT-систем.

В работе рассматривается подход, использовании которого при проектировании сложных ЭС, позволит ЭС самостоятельно, в реальном масштабе времени, блокировать воздействие аппаратной закладки. Формальная основа, предлагаемого подхода, использует объектно-субъектную модель аппаратной закладки и концепцию управления доступом к ресурсам с учетом критериев гарантированного выполнения политики безопасности.

Оставшаяся часть работы систематизирована, как изложено ниже. В разделе 1 предлагается классификация аппаратных закладок. Анализ существующих методов обнаружения аппаратных закладок приведен в разделе 2. В разделе 3 приводятся формальные основы концепции управления доступом к ресурсам ЭС. Предложенная функция управления доступом может быть использована при разработке методов, которые могут блокировать действие аппаратной закладки в реальном масштабе времени. Выводы по работе представлены в разделе 4.

### 1. КЛАССИФИКАЦИЯ АППАРАТНЫХ ЗАКЛАДНЫХ УСТРОЙСТВ

Введем определение АЗ. Государственный стандарт [4] определяет аппаратную закладку (АЗ), как скрытно установленное техническое устройство, которое создаёт угрозу безопасности информации.

Классификация аппаратных закладок могут быть выполнена на основании трех главных параметров [6, 7, 10]: физические характеристики, условия активации, функциональные характеристики.

**Физические характеристики**: Физические характеристики АЗ могут быть либо **функционального**, либо **параметрического** типа**.** Если АЗ изменяет функции системы, в этом случае тип АЗ является функциональным. Тип АЗ будет параметрическим, если ее действие приводит к уменьшению надежности функционирования за счет повышению температуры ЭС, снижению напряжения питания и т.д.

Еще одной физической характеристикой является **размер** АЗ. АЗ может быть большого размера, если она состоит из нескольких компонентов, которые в свою очередь распределены в пределах системы. Если АЗ соизмерима с несколькими транзисторами, в этом случае размер ее маленький.

**Характеристики активации**: Рассмотрим два типа активации. Внутренний тип активации предусматривает возможность запуска АЗ внутренними датчиками, внутренними состояниями некоторого процесса, определенным шаблоном ввода или внутренним счетчиком. Запуск АЗ извне предполагает использование антенны или других датчиков, доступных злоумышленнику.

**Функциональное назначение.** Проведем классификацию АЗ по их функциональному назначению [10]: накапливающего типа; разрушающего или блокирующего типа; модифицирующие протокол передачи данных. С точки зрения информационной безопасности, эти АЗ нарушают конфиденциальность, целостность и доступность информации.

## 2. АНАЛИЗ МЕТОДОВ ОБНАРУЖЕНИЯ АЗ

В этом разделе анализируются современные методы обнаружения АЗ. На рис. 1 приведена классификация методов обнаружения АЗ.

Методы обнаружения АЗ можно классифицировать по двум основным типам: разрушающие и неразрушающие исследуемую ЭС [8, 11].

Разрушающие методы, описанные в работах [12, 13, 14], используют эталон изготовленной ИС, который подлежит деметаллизации с использованием химико-механической полировки, а затем сканирующего электронного микроскопа, получая изображение для реконструкции и анализа. Однако, такой подход является чрезвычайно дорогостоящим и трудоемким, а также плохо переносим для случаев, когда увеличивается плотность интеграции ИС. Кроме того, результаты анализа образцов не могут распространяться на все изготавливаемое количество ЭС.

Неразрушающий метод может быть, в свою очередь, классифицирован на два основных типа: встроенный и невстроенный. Невстроенный метод оставляет оригинальный проект ЭС неизменным, когда при встроенном методе проект ЭС изменяется для внедрения дополнительных компонентов, направленных на обнаружение АЗ.

Встроенные методы обнаружения АЗ. Эти методы могут быть представлены тремя классами: профилактические методы, направлены, на то, чтобы не допустить установку АЗ во время проектирования или изготовления ИС; методы реального времени, устойчивые к воздействию АЗ; вспомогательные методы, облегчающие обнаружение и блокировку установленных АЗ на ЭС.

Встроенные профилактические методы. В работе [14] было отмечено, что внедрение АЗ зависит от наличия свободного «мертвого» пространства на макете ИС. Владея определенной информацией, злоумышленник способен, используя оптимизацию логики и более оптимальный метод размещения, освободить пространство для АЗ. Методики автоматизированного проектирования, предложенные в работе [15], необходимы для предотвращения успешной установки АЗ. Здесь сам оригинальный проект существенно усложняет для злоумышленника возможность расширения пространства для АЗ.

Настоящая работа посвящена новому подходу, который объединяет группу методов (устойчивые к АЗ рис. 1), которые реализует заданную политику безопасности, основанную на стратегии управления доступом к компонентам ЭС. Заданная политика безопасности обеспечивается на архитектурном уровне с помощью специальных методов проектирования ЭС.

Частным случаем предыдущего подхода является группа вспомогательных методов. Методы этой группы используют различные частные решения, зависящие от структуры конкретной ЭС. Например, в работе [16] изменение напряжения питания альтернативных логических уровней в ИС приводит к активности ранее запущенных АЗ. В работе [17] авторы предлагают метод изменения задержки распространения сигналов. В проверенную цепь ЭС вводится задержка, которая позволяет обнаружить присутствие АЗ по времени изменения распространения сигналов.

В невстроенных методах АЗ обнаруживается путем сравнения тестируемой ИС с оригинальной ИС или с ее функциональной моделью. Они могут быть разделены на два основных типа: оперативные и тестовые. В оперативном методе

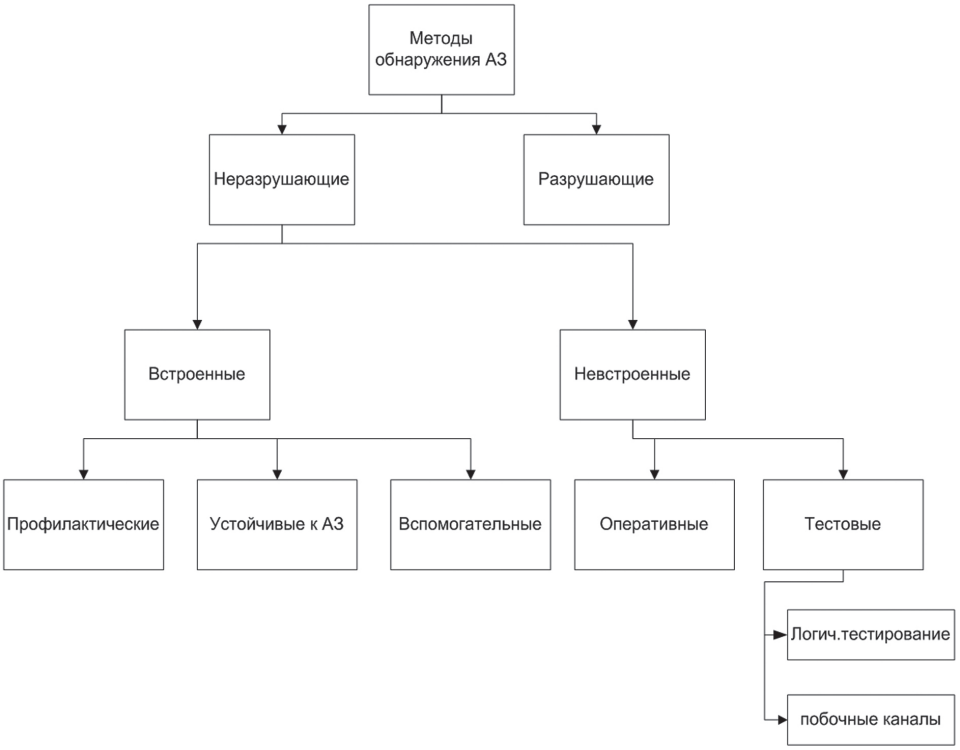


Рис. 1. Классификация методов обнаружения АЗ

используют систему наблюдения, которая пытается выявлять подозрительные действия при работе в реальных условиях, в то время как тестовые методы, направлены на обнаружение инфицированных чипов до их внедрения.

Невстроенные оперативные методы обнаружения АЗ. В работе [18] авторы предлагают включения в систему дополнительного перенастраиваемого устройства, логика которого включает наблюдение за ЭС в режиме реального времени. Проверки могут быть выполнены одновременно с работой схемы в реальных условиях с применением соответствующих мер, когда обнаруживается отклонение от нормального функционирования. Однако, эффективность и аппаратные расходы, связанные с этим методом в работе не упоминаются. В работе [19] авторы предлагают новую SoC архитектуру шины, которая может обнаружить вредоносное поведение шины, связанное с АЗ, защитить систему и системные шины от них и докладывать о вредоносном поведении в системный процессор без потери производительности самой шины.

Невстроенные оперативные методы обычно характеризуются значительной производительностью и энергопотреблением, однако они способны обеспечить 100% уверенность в ожидаемых результатах.

Невстроенные методы обнаружения АЗ в тестовом режиме. Существуют два основных подхода тестирования для обнаружения АЗ: основанные на логике тестирования, и те, которые основаны на измерении параметров побочных каналов, например, таких как мощность, задержка и т.д. Основным недостатком невстроенных методов является требование оригинальной промышленной ИМС или функциональной модели, а также достаточно сложные аппаратно-программные комплексы тестировании.

Подходы, основанные на логике тестирования: В работе [8] описан двухуровневый метод формирования тестовых последовательностей, как объединение стохастических источников по времени и множеству входов. Преимущество метода состоит в том, что он позволяет учитывать специфицированные протоколы обмена информацией объекта исследования с внешней средой при формировании тестовых последовательностей. Это свойство повышает вероятность активации АЗ. Недостатком предложенного метода является неточные оценки полноты тестирования.

Подход, основанный на анализе побочных каналов. Анализ побочных каналов, основан на выявлении АЗ посредством наблюдении их влияния на физические параметры, такие как замыкания цепи, потребляемая мощность или задержка.

В работе [20] авторы ввели понятие дактилоскопии ИС, где каждый экземпляр ИС связан с подписью, называемой «отпечаток пальцев», которая получается путем измерения одного или нескольких параметров побочных каналов. Из анализа «следов» используемых в качестве отпечатков пальцев ИС в этой работе, авторы смогли обнаружить АЗ размером 0,01% от общего размера цепи. Задержки распространения выходных портов были использованы в работе [22] как «отпечатки пальцев», с широкими характеристиками для изменения параметров процесса.

Преимущество этого подхода состоит в том, что если даже во время тестового испытания не удалось обнаружить АЗ, ее наличие может быть обнаружено с помощью некоторых параметров побочных каналов. Тем не менее, основные проблемы анализа побочных каналов связаны с большим разнообразием процессов в современных нано технологиях и помех при измерениях, которые могут маскировать последствие от АЗ, особенно для АЗ маленького размера.

Проведённый анализ угроз, исходящих от АЗ, и методов защиты от них показал, что

1) в настоящий момент не существует единого метода, который мог бы применяться для выявления любых классов АЗ;

2) в работах, посвященных рассматриваемой теме, практически, не рассматриваются формальные модели АЗ и методы борьбы с ними. Это не позволяет рассмотреть проблему с общих позиций.

## 3. ФОРМАЛЬНЫЕ ОСНОВЫ МЕТОДОВ, КОТОРЫЕ БЛОКИРУЮТ ДЕЙСТВИЕ АЗ В РЕАЛЬНОМ МАСШТАБЕ ВРЕМЕНИ

В теории компьютерной безопасности формальное моделирование политики безопасности является одним из методов, который позволяет оценить эффективность различных аспектов противодействия угрозам и обеспечить эффективные средства защиты формально подтвержденной алгоритмической базой.

Успешная разработка модели безопасности зависит от качества используемой модели самой ЭС, а также от моделей угроз АЗ. Формальные модели АЗ различных классов, использующие понятия объект, субъект, операции доступа для пары «объект-субъект» рассмотрены в [22].

Вышеупомянутым абстрактным понятиям поставим в соответствие такие физические представления в среде ЭС:

Объект ($O_j$) – часть ресурсов системы, находящаяся в дискретный момент времени в пассивном состоянии относительно информации, а также других аппаратных элементов этой системы.

Субъект ($S_i$) – электронный компонент, находящийся в дискретный момент времени в активном состоянии, а именно способный осуществить доступ к объекту. Будем рассматривать такой компонент, как пару: ресурс (объект, субъект) и доступ.

Следует отметить, что практически все компоненты ЭС в различные моменты времени могут выполнять функции хранения, получения, обработки и передачи информации. Следовательно,

одно и то же устройство может быть объектом, например, как в первом случае, или субъектом, в остальных случаях.

Рассмотрим понятие пользователя (злоумышленника) в рамках объектно-субъектного подхода, сформулируем важное свойство пользователя (злоумышленника) в виде следующей аксиомы.

**Аксиома.** Пользователь (злоумышленник) воспринимает объекты и получает информацию о состоянии ЭС через элементы, которые он должен активизировать, т.е. через субъекты.

Таким образом, для реализации своих целей, пользователь (злоумышленник) должен перевести некоторый элемент системы в активное состояние. Очевидно, что для злоумышленника таким компонентом системы будет АЗ.

Важно отметить, что, в отличие от злоумышленника, пользователь – физическое лицо, аутентифицируемое некоторой информацией и управляющее субъектом(ми) ЭС, использует только штатные ресурсы системы.

Пользователь (злоумышленник) является внешним субъектом или субъектом внешней среды ЭС.

**Понятие доступа** является одним из основополагающих в теории защиты информации, поскольку разрешение или запрет доступа для заданных множеств субъектов и объектов в конечном итоге определяет безопасность ЭС. Формализуем операцию доступа субъекта к объектам, как категорию субъектно-объектной модели.

Сначала, работу механизма доступа продемонстрируем на следующем примере. Допустим, некоторому процессу, протекающему в ЭС, необходимо прочитать данные с накопителя на жёстком диске. Для этого процесс в некоторый момент времени $t$, обращается к контролеру жесткого диска с соответствующим запросом. В этот момент времени устройство, которое инициирует получение данных, является субъектом, а контроллер жёсткого диска - объектом. При этом субъект изменяет содержимое внутренних регистров объекта, тем самым, изменяя его свойства и порождая новый субъект в ЭС. В следующий момент времени (t+1), порождённый субъект обращается к следующему объекту (непосредственно к контроллеру, управляющему механикой жёсткого диска) и передаёт ему соответствующие запросы, изменяя структуру последнего и тем самым, порождая новый субъект и т.д. Обобщим этот пример на функционирование АЗ.

Очевидно, что при активации и функционировании АЗ, в зависимости от ее типа, в системе будут порождаться неспецифицированные потоки команд ($P'$) и данных ($P''$). Рассмотрим случаи их возникновения.

Предположим, что в системе от объекта $O_j$ к объекту $O_m$ создается специфицированный поток данных $P''_{\text{сп}}$. Для выполнения этой операции в объекте $O_j$ необходимо активизировать (создать) субъект $S_j$, который, для данной операции, будет специфицированным субъектом системы. Чтобы активизировать в объекте $O_j$ субъект $S_j$ необходим специфицированный субъект $S_i$, не принадлежащий объекту $O_j$, который выполнит операцию с помощью специфицированного потока команд $P'_{\text{сп}}$. Этот процесс описывается парой операций доступа [22]:

$$\begin{aligned} &Create\,(S_i,\, O_j,\, P'_{\text{сп}}) \rightarrow S_j, \\ &Stream\,(S_j,\, O_j,\, P''_{\text{сп}}) \rightarrow O_m. \end{aligned} \qquad (1)$$

Если субъект $S_i$ играет роль нарушителя, а субъект $S_j$ – роль АЗ, тогда процесс описывается следующей парой операций доступа:

$$\begin{aligned} &Create\,(S_i, O_j,\, P') \rightarrow S_{A3}, \\ &Stream\,(S_{A3},\, O_j,\, P'') \rightarrow O_m. \end{aligned} \qquad (2)$$

Очевидно, что для данного процесса имеют место неспецифицированные потоки команд $P'$ и данных $P''$.

Используя субъектно-объектную модель АЗ, а также то, что, согласно аксиоме [23], все вопросы безопасности информации описываются доступами субъектов к объектам, с целью разработки модели ПБ, введем понятие **функции управления доступом.** Эта функция будет обеспечивать реализацию ПБ на логическом уровне.

Пары ($S_i$, $O_j$) связываются множеством разрешенных операций $P'_{\text{сп}}$. Это множество определяется ПБ и является подмножеством всего множества $P$ возможных операций для этой пары. В то же время, пары ($S_i$, $O_j$) могут связываться множеством запрещенных, с точки зрения ПБ, операций $P'$. Задачей ПБ является контроль и блокирование выполнения операций из множества $P'$. Очевидно, что $P = P'_{\text{сп}} \cup P'$.

Если учесть предположение о том, что АЗ может воспользоваться штатным каналом ЭС, т.е. каналом, который предназначен для поддержки операции доступа из множества $P_R'$, то $P'_{\text{сп}} \cap P' = \varnothing$. Таким образом, становится очевидно, что разрешение либо запрещение самого факта доступа для обеспечения заданной политики безопасности недостаточно.

Анализируя сказанное и операции доступа (2) приходим к важному выводу: для обеспечения гарантированного выполнения заданной политики безопасности **(**ПБ) в ЭС нужно контролировать не только факт доступа субъекта к объекту, но и неспецифицированные потоки команд $P'$ и данных $P''$.

Для управления операциями доступа, а так же для обнаружения и блокировки неспецифицированных потоков в системе предлагается использовать функцию управления доступом вида:

$$F = F\,(\overline{S},\, \overline{O},\, \overline{P'},\, t)\,. \qquad (3)$$

Аргументами этой функции являются: субъекты, объекты, легализованные операции и время $t$ осуществления доступа.

Определим область определения аргументов функции $F$. Конкретные значения этих аргументов определяются технической документацией на изделие.

Определим область определения функции управления доступом. Функция управления доступом может быть задана в любом виде, например, в виде таблицы, либо в виде алгоритма. Она может принимать значения 1, если доступ разрешен, и 0, если доступ запрещен.

Для реализации ПБ при управлении доступом на физическом уровне введем понятие оператора управления соединениями элементов ЭС. Теоретико-множественную модель топологии (архитектуры) ЭС представим следующим образом.

Обозначим множество элементов ЭС через $\overline{C} = (C_0, C_1, C_2, ..., C_N)$. Очевидно, что в некоторый момент времени $t$ $\overline{C} = (\overline{O}, \overline{S})$, где $\overline{O}$ — это множество объектов, а множество субъектов в этой системе — $\overline{S}$. Как было отмечено выше, каждый субъект и объект являются ресурсами системы, поэтому $\overline{S} \subseteq \overline{O}$.

Построим теоретико-множественную модель сопряжения элементов сетью каналов связи, обеспечивающих передачу сигналов между элементами.

Вход элемента $C_j$ состоит из $m_j$ входных контактов; контакт $X_i^{(j)}$ принимает элементарные сигналы $x_i^{(j)}(t)$; $i = 1, 2, ..., m_j$; $j = 1, 2, ..., N$. Аналогично выход элемента $C_j$ состоит из $r_j$ выходных контактов; контакт $Y_l^{(j)}$ выдает элементарные сигналы $y_l^{(j)}(t)$; $l = 1, 2, ..., r_j$.

Внешнюю среду можно представить в виде фиктивного элемента $C_0$, выход которого содержит — $r_0$ выходных контактов $Y_l^{(0)}$, а его вход состоит из $m_0$ входных контактов $X_i^{(0)}$.

Изложенные соображения приводят к заключению, что каждый $C_j$ (в том числе и $C_0$) как элемент ЭС достаточно характеризовать множеством входных портов (контактов):

$$\left\{X_i^{(j)}\right\}=\left(X_1^{(j)}, X_2^{(j)}, \ldots, X_{m_j}^{(j)}\right), j = \overline{0, N},$$

и множеством выходных портов (контактов):

$$\left\{Y_l^{(j)}\right\}=\left(Y_1^{(j)}, Y_2^{(j)}, \ldots, Y_{r_j}^{(j)}\right), j = \overline{0, N}.$$

Другими словами, математической моделью интерфейса элемента $C_j$, используемой для формального описания его сопряжения с другими элементами системы и внешней средой, является пара множеств: $\left\{X_i^{(j)}\right\}$ и $\left\{Y_l^{(j)}\right\}$.

Рассмотрим множество всех входных контактов всех элементов данной системы и внешней среды $\bigcup_{j=0}^{N}\left\{X_i^{(j)}\right\}, i = \overline{1, m_j}$, а также всех выходных контактов $\bigcup_{j=0}^{N}\left\{Y_l^{(j)}\right\}, l = \overline{1, r_j}$. В силу предположения, что каждому входному контакту $X_i^{(j)}$ соответствует не более чем один выходной контакт $Y_1^{(k)}$, с которым он связан элементарным каналом, можно ввести однозначный оператор сопряжения (отношения) $R$:

$$Y_1^{(k)} = R(X_i^{(j)}). \qquad (4)$$

с областью определения на множестве $\bigcup_{j=0}^{N}\left\{X_i^{(j)}\right\}, i = \overline{1, m_j}$, и областью значений на множестве $\bigcup_{j=0}^{N}\left\{Y_l^{(j)}\right\}, l = \overline{1, r_j}$. Фактически оператор $R$ **однозначно** сопоставляет входному контакту $X_i^{(j)}$ выходной контакт $Y_1^{(k)}$, которые связываются между собой элементарным каналом. Если в рассматриваемой системе к данному контакту $X_i^{(j)}$ не подключен никакой элементарный канал, то оператор (4) не определен на этом $X_i^{(j)}$.

Совокупность множеств $\left\{X_i^{(j)}\right\}$, $\left\{Y_l^{(j)}\right\}$ и оператора $R$ будем называть схемой сопряжения элементов в системе или **топологической моделью** системы. Рассмотренная формальная модель (4) содержит исчерпывающую информацию о соединениях компонентов системы.

Оператор сопряжения (4) можно задать в виде таблицы. В ней на пересечении строк с номерами элементов системы $j$ и столбцов с номерами выходных контактов $i$ располагаются пары чисел ($k$, $l$), указывающие номер элемента $k$ и номер его выходного контакта $l$, с которым соединен контакт $X_i^{(j)}$.

Как уже было показано выше, модель ЭС, связанная с реализацией ПБ, не укладывается в рамки простой модели взаимодействия электронных компонентов ЭС (4).

Во-первых, в процессе функционирования ЭС структура связей изменятся во времени под управлением выполняемых команд.

Во-вторых, структура связей должна изменяться в соответствии с правилами доступа, т.е. в соответствии с моделью безопасности.

Для учета эти факторов, в оператор сопряжения $R$ введем параметр времени и функцию управления доступом (3):

$$Y_l^{(k)} = K\left(X_i^{(j)}, t, F_i^j\right), \qquad (5)$$

где $t$ — время, $F_i^j$ — функция управления доступом между $O_i$ и $S_j$.

Фактически, оператор $K$ управляет доступом на физическом уровне, назовем его оператором управления соединением элементов ЭС. Он может принимать значения 1, если для пары элементов ($j$, $k$) имеется связь, либо 0, если для этой пары элементов связь отсутствует.

## ВЫВОДЫ

Анализируя результаты, полученные в работе, можно сделать следующие выводы.

1. Формальные модели АЗ [24], а также предложенные в настоящей работе функция управления доступом (3) и оператор управления соединением (5), могут быть использованы при построении формальной модели безопасности системы.

2. Формальная модель безопасности системы, основанная на концепции управления доступом, в свою очередь, может быть положена в основу, как архитектуры ЭС, способной блокировать действия АЗ, так и методов ее проектирования.

**Литература**


[1] DARPA, Arlington, VA, "Trust for integrated circuits," 2007. [Online]. Available: http://www.darpa.mil/MTO/solicitations/baa07-24/index.html

[2] *S.T. King, J. Tucek, A. Cozzie, C. Grier, W. Jiang, and Y. Zhou,* "Designing and implementing malicious hardware," in *Proc. 1st Usenix Workshop Large-Scale Exploits Emergent Threats (LEET)*, San Francisco,CA, 2008, pp. 1–8.

[3] *F. Wolff, C. Papachristou, S. Bhunia, and R. Chakraborty,* "Towards trojan-free trusted ICs: Problem analysis and detection scheme," in *Proc. Des. Autom. Test Euro. (DATE)*, Munich, Germany, 2008, pp. 1362–1365.

[4] ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення. Затверджено наказом Держстандарту України від 11.04.97р. №200.

[5] *Горбачев В.А., Степаненко В.В.* Сертификация периферийных устройств компьютерных систем.// Радиотехника: сб. научн. трудов. Выпуск 134.- Харьков: ХТУРЭ, 2003. С. 206-209.

[6] *Xiaoxiao Wang, Mohammad Tehranipoor and Jim Plusquellic:* Detecting Malicious Inclusions in Secure Hardware, Challenges and Solutions, 1st IEEE International Workshop on Hardware-Oriented Security and Trust (HOST'08), 2008.

[7] *Rajat Subhra Chakraborty, Seetharam Narasimhan and Swarup Bhunia*: Hardware Trojan: Threats and Emerging Solutions, Dept. of Electrical Engineering and Computer Science Case Western Reserve University Cleveland, Ohio, USA, 2010.

[8] *Горбачев В.А., Саранча С.Н., Степаненко В.В.* Сертификация сложных электронных систем с использованием функциональной модели объекта на полном наборе входных слов. Науково-технічний збірник. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Київ: КНУ-КПІ, 2002. Вип. 5. – С.139–144.

[9] *Benjamin Sanno:* Detecting Hardware Trojans, Ruhr-University Bochum, Germany, July 22, 2009.

[10] *Горбачев В.А., Иванисенко И.Н.* Классификация и формальные модели аппаратных закладных устройств. Прикладна радіоелектроніка та інформатика, Харьков: ХТУРЭ. Том 6, 2007. № 2. – С. 306-310.

[11] Hardware Trojan: Threats and Emerging Solutions (Invited Paper) Rajat Subhra Chakraborty, Seetharam Narasimhan and Swarup Bhunia Dept. of Electrical Engineering and Computer Science Case Western Reserve University Cleveland, Ohio, USA, 2009

[12] Chipworks, Inc., "Semiconductor Manufacturing - Reverse Engineering of Semiconductor components, parts and process". [Online]. Available: http://www.chipworks.com

[13] *J.A. Kash, J.C. Tsang and D.R. Knebel,* "Method and Apparatus for Reverse Engineering Integrated Circuits by Monitoring Optical Emission", United States Patent Number 6,496,022 B1, 2002.

[14] *M. Banga and M.S. Hsiao,* "VITAMIN: Voltage Inversion Technique to Ascertain Malicious Insertions in ICs", HOST, 2009.

[15] *R.S. Chakraborty and S. Bhunia,* "Security against Hardware Trojan through a Novel Application of Design Obfuscation", ICCAD, 2009.

[16] *M. Banga and M.S. Hsiao,* "VITAMIN: Voltage Inversion Technique to Ascertain Malicious Insertions in ICs", HOST, 2009.

[17] *J. Li and J. Lach,* "At-Speed Delay Characterization for IC Authentication and Trojan Horse Detection", HOST, 2008.

[18] *M. Abramovici and P. Bradley,* "Integrated Circuit Security - New Threats and Solutions", CSIIR Workshop, 2009.

[19] *L.W. Kim, J.D. Villasenor and C.K. Koc,* "A Trojan-resistant Systemon-chip Bus Architecture", Intl. Conf. on Military Communication, 2009

[20] *D. Agrawal et al,* "Trojan detection using IC fingerprinting", IEEE Symp. on Security and Privacy, 2007.

[21] *Y. Jin and Y. Makris,* "Hardware Trojan Detection Using Path Delay Fingerprint", HOST, 2008.

[22] *Горбачев В.А. Иванисенко И.Н.* Классификация и формальные модели аппаратных закладных устройств. Прикладна радіоелектроніка та інформатика, Харьков: ХТУРЭ. – том 6, 2007. № 2 С. 306-310.

[23] *Щербаков А.Ю.* Введение в теорию и практику компьютерной безопасности. – М.: издатель Молгачёва С.В., 2001. – 352 с., ил.

[26] Canadian Tusted Computer Product Evaluation Criteria, v. 3.0. Canadian System Security Centre, Communications Security Establishment, Government of Canada, 1993.


Поступила в редколлегию 5.03.2012

**Горбачев Валерий Александрович,** профессор кафедры ЭВМ ХНУРЭ. Область научных интересов: системный анализ.


УДК 638.235.231

**Формальні основі методів блокування апаратних закладних пристроїв** / В.О.Горбачов // Прикладна радіоелектроніка: наук.-техн. журнал. – 2012. – Том 11. № 2. – С. 275–280.



Розглядається класифікація апаратних закладних засобів, аналіз сучасних методів їх виявлення, та пропонуються формальні основи методів проектування складних електронних систем, що блокують апаратні закладні пристрої.



*Ключові слова:* модель апаратної закладки, класифікація апаратних закладок, модель операції доступу, функція управління доступом, оператор управління з'єднанням.

Іл. 1. Бібліогр.: 26 найм.

UDC 638.235.231

**Formal basis of malicious hardware blocking methods** / V.A. Gorbachov / / Applied Radio Electronics: Sci. Journ. – 2012. Vol. 11. № 2. – P. 275–280.



The paper considers the malicious hardware classification, analysis of modern detection methods and proposes a formal basis of methods of designing complex electronic systems that block the malicious hardware.



*Keywords:* malicious hardware model, malicious hardware classification, access operation model, access control functions, conjugator, electronic system element connection control operator.

Fig. 1. Ref.: 26 items.