УДК 004.056

Методы проектирования аппаратного обеспечения, предусматривающие снижение риска кражи особенностей реализации

© Е.В. Глинская, А.В. Фенске

МГТУ им. Н. Э. Баумана, Москва, 105005, Россия

В статье рассмотрены подходы, которые используются для предотвращения кражи особенностей реализации аппаратного обеспечения. Определены механизмы противодействия атакам данного рода. К ним относятся механизмы обеспечения защищенности от несанкционированного вскрытия, механизмы предоставления доказательств взлома, а также сигнализирующие о его наличии, механизмы обеспечения контрмер, принимаемых при обнаружении попытки взлома. Представлен перспективный метод использования «исчезающей» электроники, который является примером механизма обеспечения защищенности от несанкционированного вскрытия. Такие электронные программируемые устройства способны быстро самоуничтожаться, в зависимости от заданных условий. Одним из наиболее значимых преимуществ «исчезающей» электроники является возможность высокой, по сравнению с традиционной электроникой, скорости утилизации под действием окружающей среды. Исследовано положение дел, касающееся данной темы, в России и США.

Ключевые слова: *аппаратное обеспечение, информационная безопасность, «исчезающая электроника», атаки на аппаратное обеспечение.*

Введение. При конструировании аппаратных средств особое внимание следует направить на предотвращение проведения атак на корпус, печатные платы, прошивку, рассмотрение и выбор различных мер, направленных на предотвращение проведения атак, способных привести к нежелательным проблемам.

Принятие во внимание мер по обеспечению безопасности в процессе проектирования аппаратного обеспечения зачастую упускается из виду, создавая, таким образом, множество уязвимостей, которые могут привести к «краже» особенностей реализации. Например, разработанные технологии могут попасть в руки врага и быть использованы для создания похожих технологий или для нанесения ущерба бывшему обладателю ценного оборудования. В большинстве случаев устройство может быть перепроектировано злоумышленником после проведения успешной атаки, а это, в свою очередь, увеличивает общие расходы на разработку и время выхода устройства на рынок.

Как следствие, существует необходимость предотвращения полного или хотя бы частичного попадания технологий в чужие руки, т. е. предотвращения получения злоумышленником доступа внутрь устройства.

Целью данной работы является рассмотрение возможных способов защиты аппаратуры от атак, одним из которых является исполь-

зование так называемой «исчезающей электроники». На сегодняшний день технологии этой категории находятся на стадии научного исследования. Существуют некоторые прототипы, которые пока еще нельзя считать полнофункциональными.

Необходимость инвестирования в систему безопасности. Средства защиты не являются инструментом непосредственного извлечения доходов. Поэтому при оценке систем безопасности говорят не о заработанных деньгах, а о предотвращении возможных потерь. Впервые термин Returnon Investment for Security (ROSI) был введен в употребление специалистами в области IT Security в начале 2002 года.

Обоснование расходов на безопасность включает в себя следующие утверждения:

- расходы на безопасность являются составляющей стоимости проектирования;
- расходы на безопасность родственны расходам на страхование;
- безопасность является одним из аспектов управления рисками;
- заказчик имеет право подать на компанию в суд, если она отказывается соблюдать минимальные стандарты безопасности;
- нежелание вкладывать денежные средства в безопасность означает нежелание следовать общим тенденциям развития.

Существует несколько методов подсчета необходимых инвестиций в систему защиты. Контрмеры по обеспечению безопасности направлены на достижение следующих эффектов: уменьшение вероятности инцидента и/или снижение уровня последствий, если инцидент все-таки случится.

Меры, снижающие вероятность, называются профилактическими, а меры, снижающие последствия, называются лечебными (табл. 1). Вероятность происшествия описана семью уровнями от «незначительного» до «экстремального» (табл. 2).

Таблица 1

Типы защиты

Тип защиты	Пример
Профилактический	1. Стандарты, процедуры, должностные инструкции. 2. Аудит системы безопасности. 3. Системы обнаружения вторжений. 4. Формирование архивов.
Лечебный	1. Механизмы обеспечения защищенности от несанкционированного вскрытия. 2. Механизмы предоставления доказательств о проведении взлома. 3. Механизмы, сигнализирующие о наличии взлома. 4. Механизмы обеспечения контрмер, принимаемых при обнаружении попытки взлома. 5. Новые технологии.

Таблица 2

Вероятности угроз и частота событий

Уровень вероятности	Описание, частота (для конкретной разработки)
Незначительный	Вряд ли произойдет
Очень низкий	Событие происходит два-три раза в пять лет
Низкий	Событие происходит не более одного раза в год
Средний	Событие происходит один раз в полгода или реже
Высокий	Событие происходит один раз в месяц или реже
Очень высокий	Событие происходит несколько раз в месяц
Экстремальный	Событие происходит несколько раз в день

Последствия от нарушения политики безопасности также описаны шестью уровнями от «несущественного» к «критическому», и каждому уровню соответствуют потери в случае ликвидации нарушений (табл. 3).

Таблица 3

Степень тяжести и потери

Степень тяжести нарушения	Описание, потери в руб. (для конкретной разработки)
Несущественная	При осознанной угрозе нарушение не будет иметь последствий
Низкая	Нарушение не ведет к финансовым потерям, но выяснение характера происшествия потребует незначительных затрат
Существенная	Происшествие принесет некоторый материальный и моральный вред
Угрожающая	Потеря репутации, конфиденциальной информации. Затраты на восстановление данных, проведение расследований
Серьезная	Восстановление практически всех схем (в т.ч. на электронных и бумажных носителях)
Критическая	Потеря системы или перевод в другую безопасную среду

Чтобы определить эффект от внедрения системы защиты, нужно вычислить показатель ожидаемых потерь (Annualised Loss Expectancy — ALE). По оценкам экспертов [10], правильно установленная и настроенная система защиты дает 85% эффективности в предупреждении или уменьшении потерь от нарушений политики безопасности. Следовательно, финансовая выгода обеспечивается ежегодными сбережениями, которые получает компания при внедрении системы безопасности:

$$AS = ALE * E - AC, \quad (1)$$

где AS — ежегодные сбережения (Annual Saving); ALE — показатель ожидаемых потерь (Annualised Loss Expectancy); E — эффективность системы защиты (около 85 %); AC — ежегодные затраты на безопасность (Annual Cost).

Теперь рассчитаем показатель ALE, используя форму таблицы TRA (см. табл. 2), в которой сопоставляются вероятности угроз, степень тяжести нарушения и частота событий. Показатель ALE мы вычисляем по формуле

$$ALE = f * L. \quad (2)$$

где f — частота возникновения потенциальной угрозы, уровень которой определяется на основании вероятности (см. табл. 2); L — величина потерь в рублях, которая определяется на основании степени тяжести нарушения (см. табл. 3).

Период окупаемости инвестиционных проектов, связанных с внедрением информационных технологий, не должен превышать трех лет, поэтому период оценки эффективности данного проекта внедрения равен трем годам.

Затраты на внедрение системы защиты информации рассчитываются по следующей формуле:

$$СВН = СЛ + СПР + \sum_{i=1}^{N} C_i, \quad (3)$$

где СВН — затраты на внедрение; СЛ — затраты на покупку лицензий; СПР — затраты на проектные работы; C_i — затраты на техническую поддержку; N — количество разрабатываемых аппаратных средств.

Затраты на внедрение комплекса безопасности рассчитываются для всех элементов разрабатываемых аппаратных средств, затем подсчитывается итоговое значение показателя ожидаемых потерь и эффективность инвестиций в систему безопасности.

Методы противодействия атакам на аппаратное обеспечение. Меры по обеспечению безопасности в процессе проектирования аппаратного обеспечения зачастую связаны с конструированием корпуса в целях предотвращения доступа внутрь устройства. Если печатная плата станет доступна злоумышленнику, он сможет спроектировать ее посредством реверс-инжиниринга, а затем определить векторы тех или иных атак [1]. Результаты анализа помогут понять, как устройство взаимодействует с внешним миром и какую информацию можно получить от него без осуществления физического доступа.

Внешние интерфейсы являются пограничными пунктами между устройством и внешним миром. Они могут использоваться для достижения ряда целей, включая соединение с периферийными устройствами, тестирование во время разработки устройства и т.д. Примерами таких интерфейсов являются, например, USB, Ethernet, JTAG IEEE и т. п. Зачастую в устройствах реализованы те интерфейсы, которые обычно не применяются пользователем. Их сокрытие с помощью потайных отверстий не является хорошим решением, поскольку, в конечном итоге, они все равно могут быть обнаружены (рис. 1) [2].

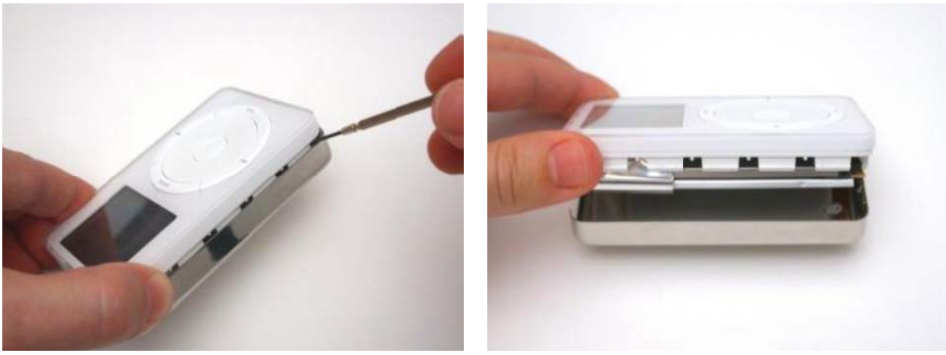

Рис. 1. Вскрытие корпуса AppleIpod ювелирной отверткой

Когда злоумышленник получает доступ к внешнему интерфейсу, он начинает исследовать его протокольную часть для определения его функциональности. Это достигается путем мониторинга реакции устройства на тестовые сигналы (используя мультиметр, осциллограф, логический анализатор).

Если особенности интерфейса станут известны злоумышленнику, то вышеописанный мониторинг станет для него тривиальной задачей, которая решается посредством использования специального анализатора протокола или программно-ориентированной утилиты. Проведение атаки на известный протокол заключается в генерировании заведомо дефектных пакетов данных (например, используя возможности анализатора протоколов) и получении результатов по ее проведению. Если в этом случае в устройстве не предусмотрена обработка ошибок или недопустимых пакетов, то возникшая ошибка может вызвать непредусмотренную алгоритмом работы устройства операцию, которая может выдать полезную информацию для злоумышленника [1].

На рис. 2 изображен пример внешнего интерфейса брелока, применяемого для аутентификации.

Анализируемым внешним интерфейсом устройства в этом случае являются пять горизонтальных металлических точек. Они станут доступны после удаления наклейки с задней части корпуса. Наклейка

может быть заменена после атаки, скрывая все следы ее проведения. Желательно шифровать трафик для уменьшения вероятности проведения успешной атаки. Секретная информация и важные компоненты не должны быть доступны через внешние интерфейсы, должна передаваться только общедоступная информация.

Рис. 2. Внешний интерфейс аутентификационного устройства

Целью введения в конструкции устройств механизмов противодействия атакам является предотвращение любой попытки злоумышленника провести физическую или электронную атаку по отношению к устройству. Формально механизмы противодействия можно разделить на 4 группы: механизмы обеспечения защищенности от несанкционированного вскрытия, механизмы предоставления доказательств о проведении взлома, механизмы, сигнализирующие о проведении взлома и механизмы обеспечения контрмер, принимаемых при обнаружении попытки взлома. Данные механизмы наиболее часто используются для предотвращения доступа к важным элементам устройства. Их основной целью является физическая безопасность встраиваемых систем. С точки зрения разработчика важным является то, чтобы цена успешной атаки превышала потенциальное вознаграждение [3].

Зачастую, устройства, имеющие такие механизмы, могут быть исследованы только путем их разборки. Может потребоваться изучение злоумышленником большого количества устройств для обнаружения механизмов защиты. Если они будут изучены, то противник сможет сформировать гипотезу обходного пути.

Механизмы обеспечения защищенности от несанкционированного вскрытия направлены на то, чтобы путем использования специальных материалов сделать взлом устройства сложным. Это может быть реализовано по-разному: с помощью использования закаленной стали при разработке корпуса, замков, изоляции или специальных болтов. Плотная упаковка компонентов и печатных плат в пределах

корпуса может увеличить сложность исследования внутреннего устройства продукта. Преимуществом механизмов данной группы является то, что о проведении атаки будут сигнализировать физические изменения, которые можно определить визуально и станет очевидно, было ли атаковано устройство [4].

При проектировании корпуса, для которого требуется использование винтов, необходимо рассмотреть возможность использования специальных односторонних винтов, которые способны обеспечить дополнительную защиту. Хотя противник может просверлить эти винты, они все же увеличивают сложность проведения атаки.

Обеспечение уплотнения корпуса с двух сторон ведет к разрушению устройства в случае, если злоумышленник попытается вскрыть его для анализа. Уплотнение корпуса с применением термостойкого клея или ультразвуковой сварки позволяет уменьшить количество успешных атак на устройство. При использовании клея необходимо выбрать такой, который имеет более высокую температуру плавления с целью увеличения видимости доказательств нарушений. Ремонтопригодность устройства может быть причиной того, что оно будет кем-то вскрыто, а этим человеком может оказаться как легитимный пользователь, так и злоумышленник [2].

Изоляция целой печатной платы путем использования эпоксидных или других специальных смол поможет защитить схемотехнику устройства. Однако основным применением такой изоляции является ее использование только для особо важных компонентов устройства. Специальные покрытия обычно используются для защиты печатной платы от влажности, плесени, пыли, коррозии или от проведения атак. Они также защищают ее компоненты от термического воздействия. Например, полиуретан дает прочное надежное покрытие, обеспечивающее стойкость к растворителям. Эпоксидные смолы также способны обеспечить хорошую устойчивость к влаге и растворителям.

Существуют химические соединения, которые могут удалить защитное покрытие, поэтому нужно быть уверенным в выбранном соединении. Для противодействия такого рода химическим атакам в качестве добавки к применяемому химическому соединению можно использовать алюминиевую пудру. Однако при этом некоторые соединения способны растворить алюминий, разъедая вышеупомянутые компоненты, делая устройство бесполезным [3].

28 января 2013 года Агентство по перспективным оборонным научно-исследовательским разработкам США DARPA (англ. *Defense Advanced Research Projects Agency* — агентство передовых оборонных исследовательских проектов) объявило о запуске программы Vanishing Programmable Resources (VAPR), в рамках которой будут создаваться электронные программируемые устройства, способные

быстро самоуничтожаться по сигналу. Заявленное время уничтожения составляет 5 секунд [5].

О временной, или исчезающей, электронике известно уже несколько лет, но раньше говорилось главным образом об устройствах, растворяющихся в условиях большого количества воды (рис. 3). Например, о микрочипах, согревающих раны для быстрого заживления или борьбы с инфекциями при хирургических вмешательствах, а потом без вреда разлагающихся в человеческом организме. Теперь же американское агентство поставило целью создание микрочипов, самоуничтожающихся и без присутствия в водной среде [8].

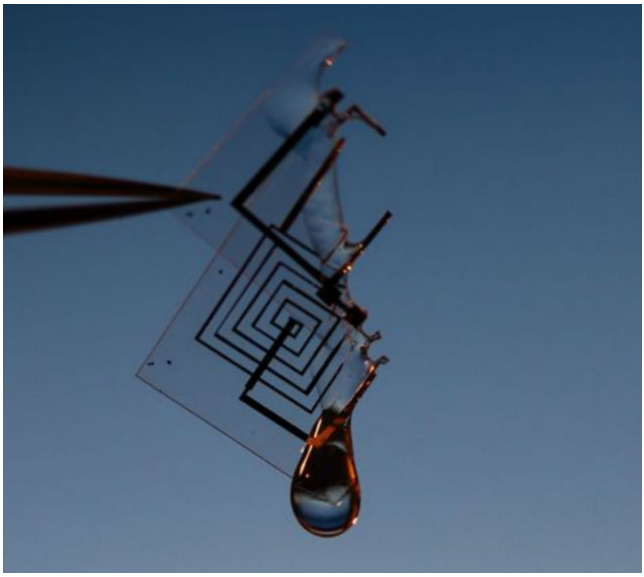

Рис. 3. Разрушение микросхемы при взаимодействии с водой

«Исчезающая» электроника, разрабатываемая в рамках программы VAPR, должна иметь функциональность и прочность обычных электронных устройств. Однако при наступлении определенного события она должна полностью или частично разрушаться под воздействием окружающей среды, после чего электроника будет бесполезна для любого противника, которому станет доступна.

Целью программы DARPA является создание микрочипов, способных взаимодействовать с удаленным пользователем и разрушающихся в обычных условиях, без погружения в воду.

Планы DARPA заключаются в постановке новых задач перед индустрией информационной безопасности.

Разработка новых временных чипов, способных обмениваться информацией с удаленным пользователем и в заданное время исчезать в обычных условиях, без необходимости погружения в водную среду, ставит новые задачи в области информационной безопасности.

Следует ожидать появления шпионских камер и прослушивающих жучков, самоуничтожающихся без видимых следов сразу же после выполнения задания. Кроме того, некоторые из этих шпионских устройств, возможно, будут состоять из распространенных органических веществ, к примеру целлюлозы или крахмала, что затруднит детектирование.

Рис. 4. Утилизация традиционной электроники

Некоторые виды пластика, входящие в состав традиционной электроники, разлагаются более 1000 лет, что создает огромные проблемы хранения и переработки отслуживших устройств.

Как будет обеспечено саморазрушение, представители DARPA не говорят. Вероятно, без изменений останется принцип создания временного электронного устройства, согласно которому микрочип покрывается постепенно разрушающимся изолирующим материалом, например шелком. После разрушения шелка начинается разрушение и микрочипа, неустойчивого во внешней среде. Структура и толщина изоляционного материала позволяют устанавливать определенное время работы электронного устройства — от минут и дней до нескольких лет. Однако нельзя исключить и то, что будут созданы какие-либо новые механизмы самоуничтожения, например, разрушающее вещество будет находиться рядом с чипом в специальном контейнере и начнет воздействовать на него по внешнему сигналу. Также можно предположить, что в качестве разрушающего вещества будут использоваться кислород или пары воды содержащиеся в воздухе, либо фермент в том случае, когда микрочип будет состоять из органических веществ.

«Исчезающая» электроника принесет человечеству немало преимуществ. Она гораздо быстрее разлагается по сравнению с традиционной электроникой и меньше засоряет и загрязняет окружающую

среду. Это поможет решить проблему со свалками мобильных телефонов, телевизоров и ноутбуков, которые разлагаются тысячелетиями.

Для разложения электроники можно применять специальные штаммы микроорганизмов. Некоторые виды полимеров, необходимых для «исчезающих» чипов, могут продуцироваться микроорганизмами, что открывает огромные просторы деятельности для биотехнологической отрасли [6].

Что касается России, то на данный момент Министерство обороны Российской Федерации совместно с Агентством стратегических инициатив при содействии Министерства образования и науки Российской Федерации и МГТУ им Н.Э.Баумана объявило о начале Первого Всероссийского конкурса научно-исследовательских работ для Вооруженных сил. Главная цель конкурса — привлечь интеллектуальную элиту страны вне зависимости от возраста к разработке передовых технологий, направленных на укрепление обороноспособности государства.

Конкурсная программа включает в себя пять основных направлений: информационно-телекоммуникационные системы, перспективные виды вооружения, военной и специальной техники, транспортные и космические системы, наука о жизнеобеспечении, энергоэффективность.

Как сообщили в оргкомитете конкурса, Минобороны не стремится ограничивать конкурсантов и будет всячески приветствовать предложения и по другим направлениям, таким, в частности, как создание систем разведки, высокоточных средств поражения и радиоэлектронной борьбы, разработка технологий и изделий двойного назначения и других [9].

Возможности механизмов предоставления доказательств о проведении взлома будут приносить пользу только в том случае, когда существует возможность проверки того, была ли осуществлена попытка атаки или владелец устройства заметил деформацию. Если злоумышленник покупает устройство с намерением его взлома, данные механизмы не смогут предотвратить такую атаку.

Механизмы, сигнализирующие о проведении взлома, позволяют устройству узнать о его попытке. Их условно можно разделить на три группы [1]:

1. *Переключатели*: микропереключатели, ртутные переключатели, позволяющие определить факт вскрытия устройства, брешь, связанную с физическим нарушением границ безопасности устройства или смещением конкретного компонента устройства.

2. *Сенсоры*: сенсоры температуры, давления, определяющие изменения окружающей среды, сенсоры напряжения, сенсоры мощности, сенсоры радиации.

3. *Схемы*: нихромовая проволока или волоконная оптика, обвитая вокруг важных схем или специфичных компонентов на плате. Данные материалы используются с целью определения того, была ли выполнена попытка взлома или попытка модификации корпуса. Например, если сопротивление нихромовой проволоки изменяется или мощность света, проходящего через оптический кабель, уменьшается, система может предположить, что была осуществлена попытка физического взлома.

Механизмы обеспечения контрмер, принимаемых при обнаружении попытки взлома обеспечивают полное отключение устройства или стирание важных фрагментов памяти с целью предотвращения получения злоумышленником секретных данных. Для особо защищенных устройств может быть реализовано физическое уничтожение путем использования маленького взрывчатого заряда. Данные методы также могут обеспечить аудит информации и анализ проведенной атаки [1].

Однако такие механизмы могут случайно сработать в процессе эксплуатации устройства, даже если легитимный пользователь будет держать устройство в рамках поставленных ограничений. Большинство устройств, имеющих данные механизмы защиты, спроектировано и разработано таким образом, что они никогда не будут вскрыты — легитимно или нет.

Определение множества параметров измерений защищаемой системы. В настоящие время используется эвристическое определение (выбор) множества параметров измерений защищаемой системы, использование которого должно дать наиболее эффективное и точное распознавание атак. Наиболее предпочтительное решение — определение необходимых параметров оценки в процессе работы. Один из возможных методов оценки — использование статистики Байеса.

Пусть $A_1 \ldots A_n$ – n измерений, используемых для определения факта атаки в любой момент времени. Пусть каждое измерение A_i имеет два значения: 1 — измерение аномальное, 0 — нет. Пусть I — гипотеза того, что в системе имеются процессы вторжения. Достоверность и чувствительность каждого измерения определяется показателями

$$P(A_i = 1|I) \, u \, P(A_i = 1|\neg I). \tag{4}$$

Вероятность вычисляется при помощи теоремы Байеса.

$$P\left(I|A_1, A_2, \ldots, A_n\right) = P(A_1, A_2, \ldots, A_n|I) \frac{P(I)}{P(A_1, A_2, \ldots, A_n)}. \tag{5}$$

Для событий I и $\neg I$, скорее всего, потребуется вычислить условную вероятность для каждой возможной комбинации множества измерений. Для упрощения вычислений, но теряя в точности, мы можем предположить, что каждое измерение A_i зависит только от I и

условно не зависит от других измерений A_j, где $i \neq j$. Это приведет к соотношениям

$$P(A_1, A_2, \ldots, A_n|I) = \prod_{i=1}^{n} P(A_i|I) \tag{6}$$

и

$$P(A_1, A_2, \ldots, A_n|\neg I) = \prod_{i=1}^{n} P(A_i|\neg I). \tag{7}$$

Отсюда

$$\frac{P\left(I|A_1, A_2, \ldots, A_n\right)}{P\left(\neg I|A_1, A_2, \ldots, A_n\right)} = \frac{P(I)\prod_{i=1}^{n} P(A_i|I)}{P(\neg I)\prod_{i=1}^{n} P(A_i|\neg I)}. \tag{8}$$

Теперь можно определить вероятность атаки, используя значения измерений аномалий, вероятность вторжения и вероятности появления каждого из измерений аномальности, которые были зафиксированы во время вторжений.

Однако для получения более реалистичной оценки $P(I|A_1 \ldots A_n)$, необходимо учитывать влияние измерений A_i друг на друга.

В практической деятельности накоплен значительный опыт решения проблем обнаружения атак. Применяемые методы в значительной степени основаны на эмпирических схемах процесса их обнаружения. Дальнейшее совершенствование связано с конкретизацией методов синтеза и анализа сложных систем в применении к системам безопасности.

Заключение. Целью данной статьи являлось освещение темы противодействия злоумышленнику для предотвращения кражи особенностей реализации аппаратного обеспечения. Основная часть посвящена аспектам процесса проектирования аппаратных средств с учетом мер безопасности.

Поскольку на сегодняшний день не существует механизмов, способных полностью растворить устройство в воздухе, было отмечено, что при проектировании продукта необходимо разработать политику безопасности, которая определяет ее цель, так как нужно осознавать, что в первую очередь надо защищать. Были выбраны методы, которые определяют возможные пути решения вышеописанной проблемы, одним из которых является перспективный на сегодняшний день метод использования «исчезающей» электроники.

ЛИТЕРАТУРА

[1] Gutmann P. Data Remanence in Semiconductor Devices. *Tenth security symposium*, 2001. URL: http://static.usenix.org/publications/library/proceedings/sec01/gutmann.html (дата обращения 16.05.2013).

[2] Anderson R. *Security Engineering. A Guide to Building Dependable Distributed systems*. John Wiley&Sons, 2001.

[3] Grand J. *Hardware Hacking: Have Fun While Voiding Your Warrantly*. Syngress Publishing, 2004.

[4] Huang A. Hacking the Xbox: an Introduction to Reverse Engineering. *Starch Press*, 2003.

[5] *This Web Feature Will Disappear in 5 Seconds.* DARPA, News Events, 2013. URL: http://www.darpa.mil/NewsEvents/Releases/2013/01/28.aspx (дата обращения 16.05.2013).

[6] «*Исчезающая электроника»: возможности и угрозы новых военных технологий*. СITфорум, 2013. URL: http://citforum.ru/news/29781/ (дата обращения 16.05.2013).

[7] Рудый Ю. *DARPA хочет встроить в оружие исчезающую электронику*. Вести.ru, 2013. URL: http://www.vesti.ru/doc.html?id=1018258 (дата обращения 16.05.2013).

[8] Загорская Д. *Американцы создали исчезающие электронные микросхемы*. Вести.ru, 2012. URL: http://www.vesti.ru/doc.html?id=922635&cid=2161 (дата обращения 16.05.2013).

[9] *Пресс-релиз Департамента развития информационных и телекоммуникационных технологий об объявлении первого Всероссийского конкурса научно-исследовательских работ среди граждан Российской Федерации в интересах Вооруженных Сил Российской Федерации.* Министерство обороны Российской Федерации. Документы. 2012. URL: http://stat.doc.mil.ru/documents/quick_search/more.htm?id=11403957@egNPA (дата обращения 16.05.2013).

[10] Петренко С.А., Курбатов В.А. *Политики информационной безопасности*. Москва, ДМК Пресс, 2006, 400 с.

Статья поступила в редакцию

Ссылку на эту статью просим оформлять следующим образом:

Глинская Е.В., Фенске А.В. Методы проектирования аппаратного обеспечения, предусматривающие снижение риска кражи особенностей реализации. *Инженерный журнал: наука и инновации*, 2013, вып. 11. URL: http://engjournal.ru/catalog/it/security/990.html

Глинская Елена Вячеславовна окончила МВТУ им. Н.Э.Баумана в 1981 г. Старший преподаватель кафедры «Информационной безопасности» МГТУ им. Н.Э. Баумана. Область научных интересов : комбинаторика, дискретная математика, имитационное моделирование, управление информационной безопасностью, сети и информационные системы, проектирования электронного оборудования. e-mail: glinskaya@bmstu.ru

Фенске Антон Вячеславович — студент 5-го курса кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана. Занимается использованием механизмов моделирования деятельности по принятию решения на основе бизнес-процессов в автоматизированной системе, а также исследованием механизмов информационной безопасности. e-mail: fenske@yandex.ru