Бурцев Михаил Николаевич, магистр 1го курса,
Информационная безопасность
Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича
Россия, Санкт-Петербург

АНАЛИЗ МЕТОДОВ ДЕТЕКТИРОВАНИЯ АППАРАТНЫХ ЗАКЛАДОК В ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМАХ И СЕТЕВОЙ ИНФРАСТРУКТУРЕ

Аннотация. В статье рассматриваются методы детектирования аппаратных закладок в вычислительных системах и сетевой инфраструктуре. Проведена классификация закладок по способу внедрения и функциональному поведению. Описаны основные подходы к их обнаружению: визуальный осмотр, электрический анализ, радиочастотный контроль, поведенческий анализ и методы реинжиниринга. Для оценки эффективности предложена формализованная модель расчёта на основе чувствительности, затрат и устойчивости к условиям эксплуатации. Результаты сравнительного анализа показывают целесообразность комплексного применения методов для повышения надёжности обнаружения угроз.

Ключевые слова: Аппаратные закладки, вычислительные системы, сетевая инфраструктура, детектирование закладок, электрический анализ, радиочастотный контроль, поведенческий анализ, сравнительное тестирование, реинжиниринг, информационная безопасность, пассивные закладки, активные закладки, мониторинг сетевых устройств.

Annotation. The article discusses methods for detecting hardware bookmarks in computing systems and network infrastructure. Bookmarks are classified according to the method of implementation and functional behavior. The main approaches to their detection are described: visual inspection, electrical analysis, radio frequency monitoring, behavioral analysis and reengineering methods. To assess the effectiveness, a formalized calculation model based on sensitivity, cost, and resilience to operating conditions is proposed. The results of the comparative analysis show the

expediency of the integrated application of methods to increase the reliability of threat detection.

Keywords: Hardware bookmarks, computing systems, network infrastructure, bookmark detection, electrical analysis, radio frequency monitoring, behavioral analysis, comparative testing, reengineering, information security, passive bookmarks, active bookmarks, monitoring of network devices.

В зависимости от способа внедрения аппаратные закладки можно условно разделить на три основные группы. Первая группа включает закладки, размещаемые на уровне печатных плат. Такие устройства могут быть интегрированы в существующие цепи или добавлены в конструкцию платы скрытным образом, затрудняющим их обнаружение при визуальном осмотре. Вторая группа состоит из закладок, встроенных непосредственно в микросхемы. Эти изменения могут быть внесены ещё на стадии проектирования или производства интегральных схем, что делает их особенно опасными и труднодоступными для стандартных методов контроля. Третью группу образуют закладки, встроенные в периферийные устройства, такие как сетевые адаптеры, клавиатуры или принтеры. В этом случае закладка может маскироваться под обычную функциональность устройства, усложняя процесс выявления [1].

Обобщённая классификация аппаратных закладок по указанным признакам представлена в Таблице 1.

Таблица 1. Классификация аппаратных закладок

Критерий	Тип	Описание
Способ внедрения	На уровне печатной платы	Интеграция дополнительных элементов или изменение трассировки.
	В структуре микросхем	Встраивание закладки в архитектуру интегральной схемы.
	В периферийных устройствах	Размещение закладки в внешних подключаемых устройствах.
Функциональное поведение	Пассивные	Сбор данных без явного воздействия до активации.

	Активные	Нарушение работы системы или передача информации в активном режиме.

Эффективное выявление аппаратных закладок в вычислительных системах и сетевой инфраструктуре требует применения разнообразных методов, каждый из которых имеет свои преимущества и ограничения. Комплексный подход к детектированию позволяет повысить вероятность обнаружения скрытых угроз, минимизируя риски несанкционированного доступа или нарушения функционирования систем.

Одним из наиболее простых и широко применяемых способов является визуальный осмотр оборудования. При проведении визуального контроля специалисты обращают внимание на наличие нештатных элементов, изменения в компоновке печатных плат, следы пайки, дополнительные соединения или физические повреждения компонентов [2]. Для повышения надёжности также используются методы неразрушающего контроля, включающие рентгенографию, термографию и оптическую микроскопию. Например, рентгеновское сканирование позволяет получить изображение внутренней структуры устройства без его вскрытия, что способствует выявлению скрытых модификаций.

Когда визуальный осмотр не позволяет с достаточной степенью надёжности обнаружить закладки, применяются электрические методы анализа. Они основаны на измерении электрических характеристик — сопротивления, ёмкости, индуктивности, токов утечек — и последующем сравнении этих данных с эталонными характеристиками устройства [3]. Отклонение измеряемого параметра ΔP от базового значения P_0 определяется по формуле 1:

$$\Delta P = P_{\text{исследуемое}} - P_0 \quad (1)$$

Согласно формуле 1, если отклонение превышает допустимое значение, устройство признаётся подозрительным и подлежит более глубокому обследованию.

Ещё одним важным методом является радиочастотный контроль, направленный на обнаружение закладок, использующих радиоканалы для передачи информации. Такие закладки могут периодически или постоянно излучать сигналы, отличающиеся от рабочих частот основного устройства. С помощью спектроанализаторов проводится исследование частотного спектра излучений, где появление стабильных внеполосных сигналов свидетельствует о возможной активности закладки. Для анализа сигнала строится модель фонового шума, и наличие устойчивых отклонений в определённых диапазонах частот фиксируется как аномалия.

Поведенческий анализ устройств позволяет выявлять закладки, воздействующие на функциональность оборудования без прямого физического присутствия. Суть метода заключается в длительном мониторинге параметров работы устройств и построении математической модели нормального поведения [4]. При этом фиксируются характеристики, такие как время обработки сетевых пакетов, энергопотребление, температурные режимы. Отклонение времени обработки Δt можно определить по формуле 2:

$$\Delta t = t_{\text{наблюдаемое}} - t_0 \qquad (2)$$

Где $t_{\text{наблюдаемое}}$ — фактическое время отклика, а t_0 — среднее значение в нормальном режиме. Согласно формуле 2, если Δt систематически превышает допустимый порог, это может указывать на вмешательство стороннего элемента.

Наиболее глубокий анализ обеспечивают методы сравнительного тестирования и реинжиниринга. При сравнительном тестировании исследуемое устройство сопоставляется с эталонным экземпляром того же типа. Даже небольшие функциональные или конструктивные различия позволяют предположить наличие нештатных компонентов [5]. Реинжиниринг включает в себя полную реконструкцию схем и программного обеспечения устройства с целью выявления встроенных закладок, зачастую скрытых на уровне физического дизайна или логики функционирования микросхем.

Для обоснованного сравнения методов детектирования аппаратных закладок введём логическую модель на основе реальных факторов:

- Насколько метод чувствителен к разным типам закладок,
- Какие затраты он требует,
- Насколько он надёжен в реальных условиях.

Далее необходимо сформировать параметры оценки, что отображено в таблице 2.

Таблица 2. Параметры оценки

Параметр	Обозначение	Пояснение
Чувствительность к пассивным закладкам	S_p	0–1 (где 1 — полностью обнаруживает)
Чувствительность к активным закладкам	S_a	0–1
Зависимость от условий (доступность, шумы)	Z	0–1 (где 1 — полностью независим)
Стоимость и ресурсоёмкость	C	0–1 (где 1 — минимальные затраты)
Время применения	T	0–1 (где 1 — быстрое применение)

Итоговая эффективность метода E будем рассчитывать согласно формуле 3, представленной ниже.

$$E = \alpha S_p + \beta S_a + \gamma Z + \delta C + \epsilon T \quad (3)$$

Где коэффициенты веса выбираем логично:

- Надёжность важнее всего: $\alpha = 0.3$, $\beta = 0.3$.
- Остальные факторы важны, но чуть меньше: $\gamma = 0.2$, $\delta = 0.1$, $\epsilon = 0.1$

Теперь на основе уже описанных ранее особенностей заполним реальные оценки для каждого метода, что представлено в таблице 3.

Таблица 3. Оценка методов по параметрам

Метод	S_p (пассивные)	S_a (активные)	Z (условие)	C (затраты)	T (время)
Визуальный осмотр	0.3	0.5	0.8	0.9	0.9
Электрические методы	0.7	0.7	0.6	0.6	0.5
Радиочастотный контроль	0.1	0.8	0.4	0.7	0.5
Поведенческий анализ	0.6	0.7	0.5	0.5	0.4

Продолжение таблицы 3

Метод	S_p (пассивные)	S_a (активные)	Z (условие)	C (затраты)	T (время)
Сравнительное тестирование и реинжиниринг	0.9	0.9	0.9	0.2	0.2

Оценки были выставлены согласно характерным особенностям каждого из методов, а именно:

- Визуальный осмотр быстро проводится, малозатратен, но малоэффективен против скрытых (пассивных) закладок.
- Электрический метод лучше ловит оба типа закладок, но требует приборов.
- Радиоконтроль практически не ловит пассивные закладки, зато эффективен против активных.
- Поведенческий анализ универсален, но ресурсозатратен.
- Реинжиниринг точен, но очень дорогой и долгий.

Теперь рассчитаем E для каждого метода по формуле (3):

Визуальный осмотр: $E = 0.3 \times 0.3 + 0.3 \times 0.5 + 0.2 \times 0.8 + \times 0.1 \times 0.9 = 0.58$

Электрические методы: $E = 0{,}3 \times 0{,}7 + 0{,}3 \times 0{,}7 + 0{,}2 \times 0{,}6 + 0{,}1 \times 0{,}6 + 0{,}1 \times 0{,}5 = 0.65$

Радиочастотный контроль: $E = 0{,}3 \times 0{,}1 + 0{,}3 \times 0{,}8 + 0{,}2 \times 0{,}4 + 0{,}1 \times 0{,}7 + 0{,}1 \times 0{,}5 = 0.47$

Поведенческий анализ: $E = 0{,}3 \times 0{,}6 + 0{,}3 \times 0{,}7 + 0{,}2 \times 0{,}5 + 0{,}1 \times 0{,}5 + 0{,}1 \times 0{,}4 = 0.58$

Реинжиниринг: $E = 0{,}3 \times 0{,}9 + 0{,}3 \times 0{,}9 + 0{,}2 \times 0{,}9 + 0{,}1 \times 0{,}2 + 0{,}1 \times 0{,}2 = 0.76$

Систематизируем полученные данные в таблице 4, представленной ниже.

Таблица 4. Сравнительная эффективность методов

Метод	Итоговая эффективность E
Сравнительное тестирование и реинжиниринг	0.76
Электрические методы анализа	0.65
Визуальный осмотр и НК	0.58
Поведенческий анализ	0.58
Радиочастотный контроль	0.47

Анализ полученных данных показывает, что наивысшую интегральную эффективность демонстрируют методы сравнительного тестирования и реинжиниринга, что обусловлено их высокой чувствительностью как к пассивным, так и к активным закладкам, а также минимальной зависимостью от условий эксплуатации. Однако их применение связано с существенными затратами ресурсов и времени, что ограничивает возможность их регулярного использования в масштабных системах.

Электрические методы анализа, обладая хорошей чувствительностью при относительно умеренных требованиях к ресурсам, показывают высокую практическую эффективность. Их применимость в реальных условиях, особенно в случаях отсутствия полной информации об устройстве, делает их оптимальным выбором для большинства обследований.

Визуальный осмотр и неразрушающий контроль, а также поведенческий анализ продемонстрировали сопоставимые результаты эффективности, однако каждый из этих методов имеет свои ограничения: визуальный осмотр ограничен в обнаружении высококачественно интегрированных закладок, а поведенческий анализ требует значительного времени на сбор и обработку данных.

Наименее эффективным оказался радиочастотный контроль, что связано с его ограниченной способностью выявлять исключительно активные типы закладок, в то время как пассивные закладки этим методом практически не обнаруживаются.

Таким образом, для построения надёжной системы детектирования целесообразно использовать комбинацию методов, опираясь на электрический

анализ в качестве основного средства, дополняя его сравнительным тестированием и поведенческим мониторингом при необходимости повышения надёжности.

Список источников информации

1. Гельфанд А. М., Волкогонов В. Н., Карамова М. Р. Анализ и управление рисками информационной безопасности объекта критической информационной инфраструктуры // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2020. – Т. 1. – С. 21–27.
2. Воронов Д. С., Черников В. В. Метод взвешенного голосования для обнаружения аппаратных закладок // Молодой ученый. — 2016. — № 18 (122). — С. 64–68. — URL: https://moluch.ru/archive/122/33793/ (дата обращения: 28.04.2025).
3. Шемякин С. Н., Гельфанд А. М., Орлов Г. А. Критическая информационная инфраструктура // Наука и инновации – современные концепции. – 2020. – С. 114–118.
4. Нечай А. А. Выявление недекларированных возможностей аппаратно-программного обеспечения // Экономика и социум. — 2014. — № 5. — С. 103–106. — URL: https://cyberleninka.ru/article/n/vyyavlenie-nedeklarirovannyh-vozmozhnostey-apparatno-programmnogo-obespecheniya (дата обращения: 28.04.2025).
5. Артамонова А. А. Аппаратные закладки как компонент вредоносного аппаратного обеспечения: обзор, классификация и анализ угрозы // Научный результат. Серия «Информационные технологии». — 2018. — Т. 4, № 3. — С. 45–52. — URL: https://cyberleninka.ru/article/n/apparatnye-zakladki-kak-komponent-vredonosnogo-apparatnogo-obespecheniya-obzor-klassifikatsiya-i-analiz-ugrozy (дата обращения: 28.04.2025).