УДК 629.7.052

РАЗРАБОТКА СЦЕНАРИЕВ ОБНАРУЖЕНИЯ ВОЗДЕЙСТВИЯ ДЕСТРУКТИВНЫХ ЭМИ НА БОРТОВЫЕ ЦИФРОВЫЕ ВЫЧИСЛИТЕЛЬНЫЕ КОМПЛЕКСЫ

В.А. Михайлов, генеральный директор ОАО «НИИ «Аргон», к.т.н.
Л.О. Мырова, начальник отдела ОАО «МНИРТИ», д.т.н.; lmyrova@rambler.ru
А.В. Царегородцев, профессор МИЭМ ВШЭ, д.т.н.

Ключевые слова: *бортовой цифровой вычислительный комплекс, электромагнитное воздействие, интеллектуальная система, нейронная сеть, нечеткость, классификатор.*

Введение. В последнее десятилетие при создании различных вычислительных средств возникла необходимость учета требований по обеспечению защищенности элементов и узлов инфокоммуникационных систем от высокоэффективных электромагнитных излучений (ВЭИ). Это объясняется новейшими достижениями в области генерации сверхмощных широкополосных электромагнитных полей (СШП ЭМП), повышением требований к защите ответственной информации, наличием значительных по протяженности распределенных кабельных сетей. Особенно это относится к современным бортовым цифровым вычислительным комплексам (БЦВК), занимающим особое место в системах управления и контроля и все в большей степени оснащаемыми электронными элементами, чувствительными к электромагнитным воздействиям.

В связи с этим особо стоит задача по защите БЦВК от воздействия сверхкороткоимпульсного электромагнитного излучения (СКИ ЭМИ). С каждым годом появляются все более мощные стационарные и мобильные излучатели, которые не только формируют периодические и однократные СКИ ЭМИ, но и обладают принципиально новыми качествами, отсутствующими у традиционных источников ЭМИ: соразмерностью длительностей воздействующих импульсов и информационных сигналов.

Одним из эффективных методов защиты от таких нестандартных воздействий является обнаружение воздействия на БЦВК деструктивных ЭМИ с целью своевременного принятия решения по защите.

Методологический подход к созданию интеллектуальной системы анализа устойчивости БЦВК к деструктивному воздействию ЭМИ. Будем отталкиваться от предлагаемого представления интеллектуальной системы анализа устойчивости (ИСАУ) БЦВК (рис. 1) к деструктивному воздействию ЭМИ.

Обозначим G — множество рекомендаций, формируемых ИСАУ и направленных на повышение стойкости БЦВК (Network) к воздействию ЭМИ. Пусть $Network_G$ — исходная конфигурация БЦВК с реализованным в ней множеством рекомендаций G; $SecurityLevel\ (Network_G) \to \max$ — функция, результатом которой является уровень стойкости БЦВК *Network* к деструктивным воздействиям ЭМИ.

Тогда целевой функцией в методе анализа устойчивости БЦВК к воздействию ЭМИ будет повышение общего уровня стойкости комплекса $SecurityLevel\ (Network_G) \to \max$ (в частном случае целевая функция может быть задана в виде $SecurityLevel\ (Network_G) \to SL_{\text{ТРЕБ}}$, где $SL_{\text{ТРЕБ}}$ — требуемый уровень стойкости) при соблюдении следующих *требований* к остальным свойствам ИСАУ.

1. *Своевременность*: $P_{\text{СВ}}(t \le T^{\text{ДОП}}) \ge P_{\text{СВ}}^{\text{ДОП}}$, где $P_{\text{СВ}}^{\text{ДОП}} = 0{,}99$, допустимое время проведения анализа $T_{\text{пр}}^{\text{ДОП}} = T_{\text{пр}}^{\text{ТР}}$, где на этапе проектирования $T_{\text{пр}}^{\text{ТР}} = 45$ мин и эксплуатации $T_{\text{ж}}^{\text{ТР}} = 25$ мкс ($T_{\text{эк}}^{\text{ТР}} > T_{\text{пр}}^{\text{ТР}}$ поскольку на этапе эксплуатации автоматизируются все мероприятия данного этапа методологии).

2. *Обоснованность*: $N_C \ge \max\limits_{s \in S} N_C^S$; $N_У \ge \max\limits_{s \in S} N_У^S$ и $N_П \ge \max\limits_{s \in S} N_П^S$, где N_C, $N_У$, $N_П$ — количество анализируемых сценариев воздействий ЭМИ на элементы и узлы БЦВК (количество обнаруженных уязвимостей и учитываемых па-

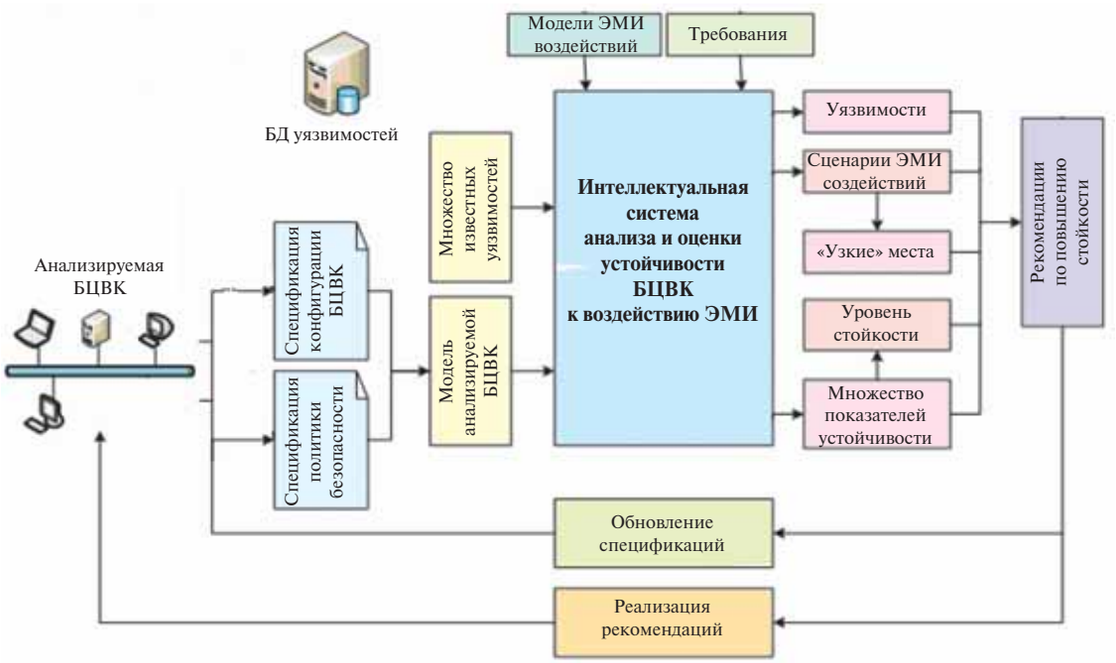

Рис. 1. **Интеллектуальная система анализа устойчивости БЦВК к деструктивному воздействию ЭМИ**

раметров разработанным прототипом ИСАУ); S — множество существующих систем; N_C^S, N_y^S, $N_П^S$ — количество анализируемых сценариев воздействий ЭМИ на элементы и узлы БЦВК (обнаруженных уязвимостей и учитываемых параметров разрабатываемой ИСАУ s, соответственно).

Множество параметров можно определить путем учета:

а) конфигурации анализируемого БЦВК (различные операционные системы, топологии и др.);

б) политики безопасности (правил фильтрации, экранирования, зоннирования и др.);

в) параметров ЭМИ (место воздействия, временных, частотных, энергетических характеристик и т.д.);

г) общих параметров (обновление БД ЭМИ воздействий, сценариев ЭМИ воздействий, возможность задания множества анализируемых хостов);

3. *Ресурсопотребление*: $P_{\text{РЕС}}(r \le R^{\text{ДОП}}) \ge P_{\text{РЕС}}^{\text{ДОП}}$, где $P_{\text{РЕС}}^{\text{ДОП}} = 0{,}99$, $R^{\text{ДОП}}$=0,15 (15% от общего ресурса, доступного для решения задач) для критических ресурсов БЦВК.

Исходные данные для анализа и оценки устойчивости, реализующей разрабатываемую методологию, представляются в виде:

$$\left(SDL, SPL, VDB, P_{\text{ЭМИ}}, P_{\text{АУ}}, R\right),$$

где SDL — спецификация анализируемой БЦВК; SPL — спецификация реализуемой в бортовой сети политики безопасности; VDB — внешняя база данных ЭМИ воздействий; $P_{\text{ЭМИ}}$ — множество параметров, характеризующих ЭМИ воздействия; $P_{\text{АУ}}$ — множество параметров, характеризующих процесс анализа устойчивости; R — требования к уровню стойкости БЦВК.

В процессе анализа и оценки устойчивости БЦВК необходимо определить комплекс мер, реализация которых позволит максимально повысить стойкость анализируемого комплекса в условиях заданных ресурсов обеспечения стойкости. Таким образом, ИСАУ должна позволить определять множество $\{V, AR, W, M, G\}$ при условии:

$$SecurityLevel\,(Network_G) \to \max;$$

или

$$SecurityLevel\,(Network_G) \to SL_{\text{ТРЕБ}},$$

где $Network_G$ — исходная конфигурация БЦВК*Network* с реализованным в ней комплексом мер G; V - множество обнаруженных уязвимостей; AR — сценарии ЭМИ воздействий; W — «узкие» места в электромагнитной безопасности анализируемого комплекса; M — множество показателей устойчивости; G — множество рекомендаций по повышению общего уровня стойкости БЦВК; *SecurityLevel (Network)* — функция, результатом которой является уровень стойкости БЦВК*Network*.

Модель ИСАУ элементов и узлов БЦВК к деструктивному воздействию ЭМИ. Моделирование служит основным средством верификации, позволяющим предотвратить ошибки проектирования сложных кибернетических систем, к которым относится интеллектуальная система анализа и оценки устойчивости БЦВК к деструктивному воздействию ЭМИ. В ИСАУ имеет место взаимосвязь событии: источник ЭМВ – угрозы ЭМВ – фактор (уязвимость) – угроза ЭМВ (действие) – последствия (деструктивное ЭМВ – ДЭМВ). При изменении множества известных ЭМВ и условий эксплуатации БЦВК может проявиться ряд новых уязвимостей, не отраженных в исходной модели, и соответственно потенциальная возможность нарушения функционирования отдельных подсистем БЦВК.

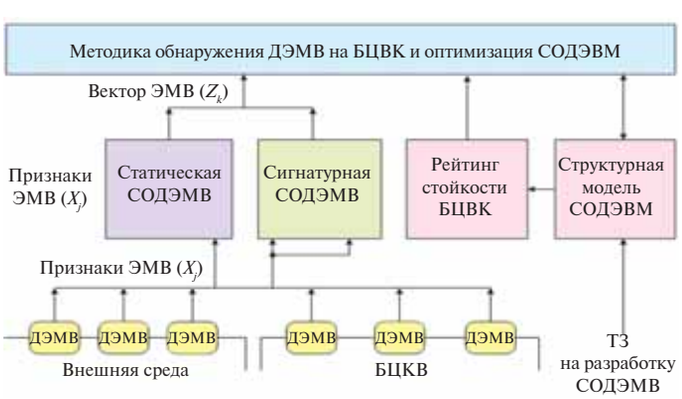

Рис. 2. **Модель системы обнаружения ДЭМВ**

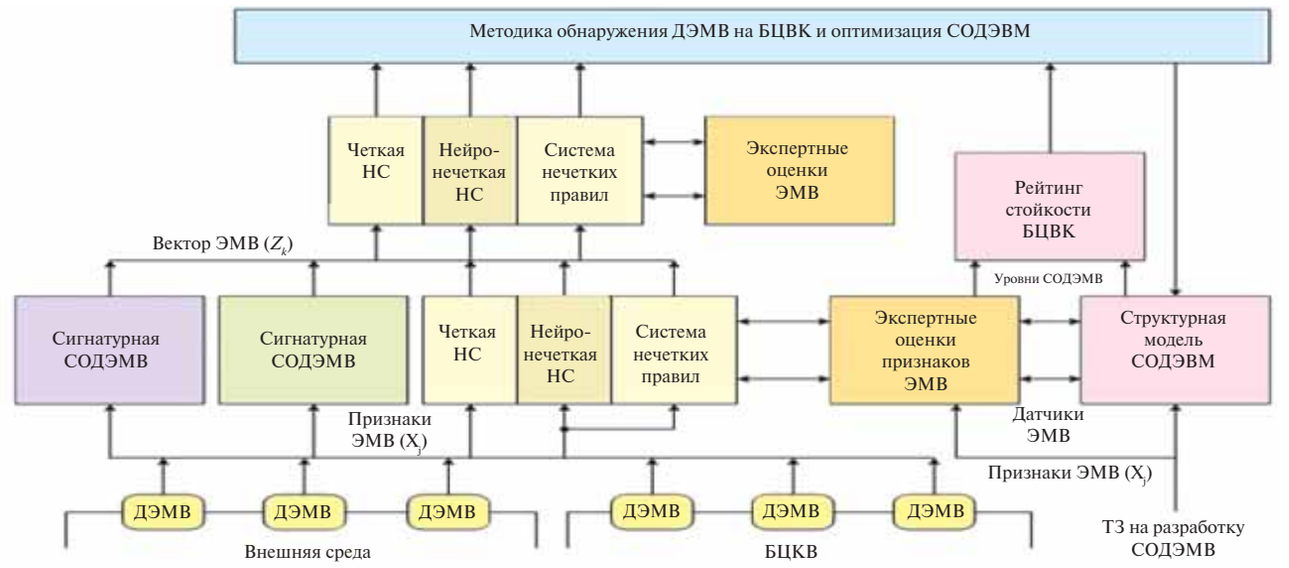

Рис. 3. **Модель ИСАУ**

Предложенная модель учитывает наличие в структуре БЦВК интегрированной интеллектуальной системы анализа и оценки устойчивости БЦВК к деструктивному воздействию ЭМИ, которая включает СОДЭМВ (систему обнаружения ДЭМВ), множество ДЭМВ, средства сигнатурного и статистического анализа, взаимосвязанных как с внешней средой, так и с аппаратно-программными компонентами самого БЦВК. Формируемый ДЭМВ вектор признаков ЭМВ (рис. 2) может обрабатываться блоками статистической СОДЭМВ или сигнатурной СОДЭМВ и обобщаться с помощью методики обнаружения ДЭМВ и оптимизации СОДЭМВ.

Для придания ИСАУ свойств автоматической и оперативной реакции на изменение вектора признаков ЭМВ в СОДЭМВ вводятся адаптивные уровни идентификации ЭМВ и обобщения опыта обнаружения ДЭМВ на БЦВК. Основным элементом модели ИСАУ является методика обнаружения ДЭМВ и оптимизации СОДЭМВ, которая координирует взаимосвязь адаптивных уровней (в виде нейро-нечетких сетей (НС) и систем нечетких продукционных правил), структурной модели СОДЭМВ, инструментальных средств расчета показателей стойкости и рейтинга стойкости БЦВК (рис. 3). Важное качество ИСАУ – возможность накопления опыта, фиксируемого в информационных полях нейронных и нейро-нечетких сетей системы обнаружения ДЭМВ.

Структура СОДЭМВ формируется в виде иерархии уровней датчиков ЭМВ, а опыт экспертов по ЭМС представляется матрицами экспертных оценок и системами нечетких продукционных правил для классификации ДЭМВ по их признакам. Системы нечетких продукционных правил представляются в виде НС, которые определяются на заданном подмножестве входных векторов признаков ЭМВ. Одновременно определяются и классификаторы в виде четких НС.

Разработка сценариев обнаружения воздействия на БЦВК деструктивных ЭМИ. Результаты экспериментальных исследований показали, что при воздействии ЭМИ очень важно зафиксировать начало воздействия ЭМИ и принять своевременные меры по предотвращению деструктивного для БЦВК воздействия. Необходимо отметить, что отличительной чертой воздействия ЭМИ на современное бортовое оборудование и его телекоммуникационную инфраструктуру является не физическое разрушение элементной базы БЦВК и каналов связи, а нарушение логической целостности информации, передаваемой по этим линиям связи и обрабатываемой БЦВК.

Рассмотрим сценарии работы СОДЭМВ по обнаружению воздействия на БЦВК деструктивных ЭМИ, действующих на основе методов анализа:

- параметров искажений информационного потока в условиях воздействия ЭМИ;
- информации датчиков обнаружения ЭМВ.

Параметры наводок на внешнем детектирующем элементе и анализ параметров искажений информационного потока являются основными исходными данными для функционирования СОДЭМВ и формирования сигнала о начале воздействия ЭМИ.

Сценарий работы СОДЭМВ на основе метода анализа параметров искажений информационного потока в условиях воздействия ЭМИ. Сценарий базируется на анализе информационного потока, обрабатываемого инфокоммуникационными узлами БЦВК, и выявлении закономерности появления искаженных пакетов информации. При обнаружении факта воздействия известных источников ЭМИ принимается решение на блокировку искаженной информации.

Основными признаками воздействия источников ЭМИ на информационный поток являются периодичность и кратность частоты появления искаженных пакетов частоте формирования импульсов известными источниками ЭМИ.

Из канала связи на вход БЦВК поступает последовательность сигналов, которая некоторым образом преобразуется и подается на вход СОДЭМВ, где происходит ее анализ. Если входные данные вследствие воздействия ЭМИ на канал передачи данных (ПД) искажены и не соответствуют требованиям по уровню или форме сигнала (задаются применяемыми в БЦВК протоколами), то данные на выходе БЦВК также не будут соответствовать требованиям телекоммуникационного протокола. Таким образом, появляется возможность определить наличие воздействия ЭМИ на канал ПД и управления путем проведения сравнительного анализа соответствия данных, поступающих на шину обмена данными БЦВК, требованиям используемого телекоммуникационного протокола.

Введем следующие переменные: i – единица информации (бит); v_i – скорость ПД, определяемая телекоммуникационным протоколом (бит/с); $T_{\text{исп}}$ – время, необходимое для выявления закономерности появления искаженной

информации (обычно несколько секунд при $v_i \geq 5$ Мбит/с); $\lambda_{i,\text{исп}} = v_i\, T_{\text{исп}}$ – количество информационных единиц, передаваемых и обрабатываемых элементами и узлами БЦВК за $T_{\text{исп}}$; α – размерность пакета информации, определяемая телекоммуникационным протоколом; $p = \alpha \times i \times 8$ – информационный пакет (например, для сети Ethernet 32 байта, т.е $\alpha = 32$); $\lambda_{p,\text{исп}} = \dfrac{\lambda_{e,\text{исп}}}{\alpha}$ – количество информационных пакетов, передаваемых и обрабатываемых элементами и узлами БЦВК за $T_{\text{исп}}$; $\tau_p = \dfrac{T_{\text{исп}}}{\lambda_{p,\text{исп}}}$ – средняя длительность одного информационного пакета; $F_{\text{ген}}$ – частота формирования ЭМИ; τ_e – время длительности наведенной помехи на элементы БЦВК единичным ЭМИ; $\lambda_{e,\text{исп}} = F_{\text{ген}}\, T_{\text{исп}}$ – количество ЭМИ за $T_{\text{исп}}$; $\omega_{\text{единич СКИ}} = \begin{cases} \omega_{\max} = \dfrac{\tau_e}{\tau_p} + 2; \\ \omega_{\min} = \dfrac{\tau_e}{\tau_p} \end{cases}$ – количество искаженных информационных пакетов единичным ЭМИ; $\omega_{\text{исп}} = \omega_{\text{единич СКИ}}\, \lambda_{e,\text{исп}}$ – количество искаженных информационных пакетов за $T_{\text{исп}}$; $p_{\text{ср}} = \dfrac{\omega_{\text{исп}}}{\lambda_{p,\text{исп}}}$ – среднее значение вероятности появления искаженного пакета.

Согласно методу биноминального распределения, искажение информационного пакета (событие А) появляется с вероятностью p, при этом вероятность непоявления события А равна $q = 1 - p$. При условии, что n – количество переданных информационных пакетов, m – частота появления события А в n переданных информационных пакетах, суммарная вероятность всех возможных комбинаций исходов равна 1, т.е.

$$1 = p^n + np^{n-1}(1-p) + C_n^{n-2} p^{n-2}(1-p)^2 + \ldots$$

$$\ldots + C_n^m p^m (1-p)^{n-m} + \ldots + (1-p)^n,$$

где p_n – вероятность того, что в n испытаниях А появится n раз; $P_m = C_n^m p^m (1-p)^{n-m}$ – вероятность того, что в n испытаниях А произойдет m раз и не произойдет (n—m) раз; $C_n^m = \dfrac{n!}{m!(n-m)!}$ – число сочетаний из n по m.

При возникновении случайных искажений можно воспользоваться распределением Пуассона. При росте n и зафиксированном значении произведения $n\,p = \mu > 0$ биноминальное распределение сходится к распределению Пуассона. Таким образом, случайная величина, имеющая распределение Пуассона с параметром μ, принимает значения с вероятностью $P_m = \dfrac{\mu^m e^{-\mu}}{m!}$.

При условии нормального функционирования бортовой сети и отсутствия ДЭМВ телекоммуникационными протоколами допускается появление искаженного пакета 1 раз в день при скорости передачи данных 5 Мбит/с, что соответствует вероятности появления искаженного пакета порядка $1 \cdot 10^{-14}$. По результатам экспериментальных исследований функционирования БЦВК при отсутствии воздействия ЭМИ вероятность появления искаженного пакета составляла $1 \cdot 10^{-8}$. Однако в условиях воздействия СКИ ЭМИ источника с $F_{\text{ген}} = 100$ кГц среднее значение вероятности появления искаженного пакета $p_{\text{ср}}$ возрастало до $0{,}6 - 0{,}7 \cdot 10^{-2}$ при $T_{\text{исп}} = 1$ с.

Сегодня в наборе функциональных возможностей телекоммуникационных адаптеров есть встроенные программно-реализованные механизмы определения искажений в пакетах информационного потока. Как правило, БЦВК имеет несколько сетевых адаптеров, а обработка информационных пакетов и анализ трафика, проходящего через адаптеры,

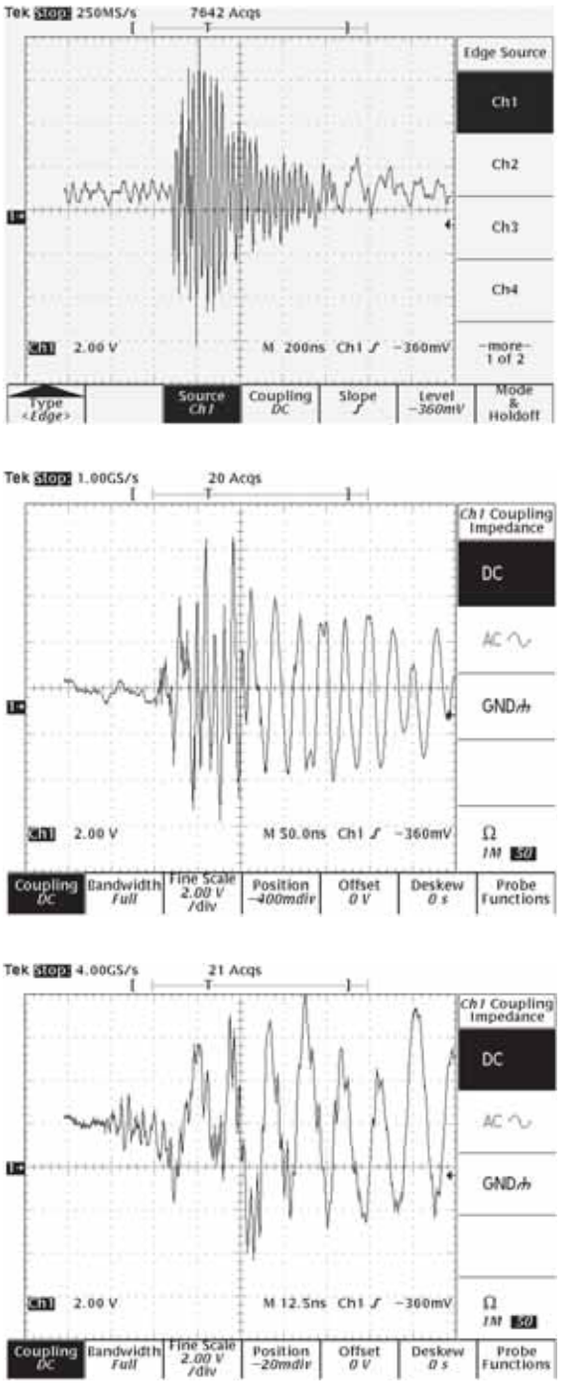

Рис. 4. **Форма сигнала наводки на бортовом сетевом кабеле при воздействии СКИ ЭМИ: на развертке 200 нс/дел (*а*), 50 нс/дел (*б*) и 12,5 нс/дел (*в*)**

осуществляется программным методом. Таким образом, становится возможна программная реализация алгоритма анализа частоты поступления искаженных информационных пакетов, определение частоты повторения фактов искажения информационных единиц (бит, байт), и, как следствие, обнаружение воздействия ЭМИ на БЦВК

Сценарий работы СОДЭМВ на основе метода анализа информации внешних средств обнаружения ЭМИ. Для обнаружения воздействия на БЦВК деструктивных ЭМИ предлагается использовать датчики ЭМВ. Совокупность применяемых датчиков должна представлять собой разветвленную сеть, элементы которой размещаются в каналах ПД и вычислительных узлах БЦВК. При фиксации датчиками факта воздействия ЭМИ от

а)

б)

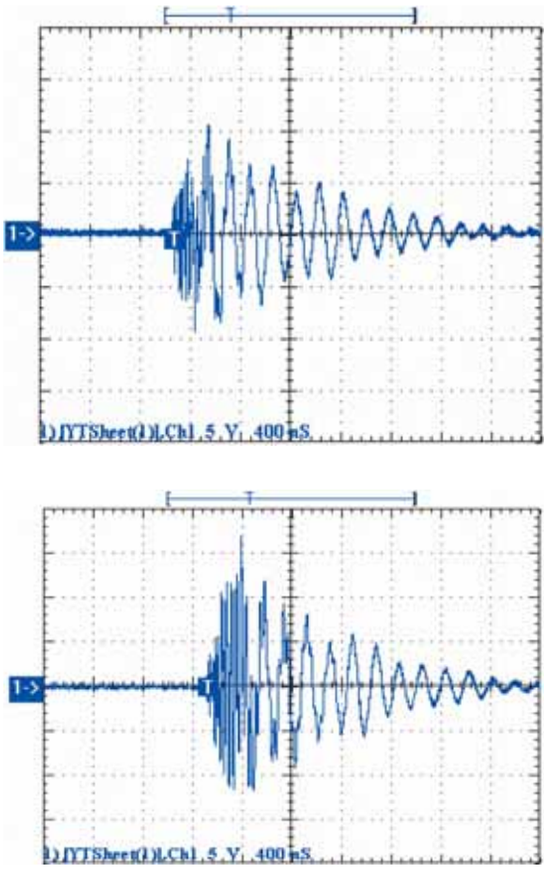

Рис. 5. **Форма сигнала наводки на бортовом сетевом кабеле при воздействии СКИ ЭМИ (100% потерь информационных пакетов): $\tau_и$ = 790 пс (*а*), $\tau_и$ = 170 пс (*б*)**

датчиков в СОДЭМВ передается сигнал о регистрации факта воздействия ЭМИ на элементы бортовой сети. При поступлении такого сигнала СОДЭМВ вырабатывает команды управления, поступающие по каналам ПД на системную шину БЦВМ, коммутаторов и других элементов БЦВК. При этом поступающие команды управления учитывают особенности функционирования всех устройств, входящих в состав БЦВК, а также особенности и характер сбоев в их работе.

Проведение широкого спектра экспериментальных исследований позволило определить уровни функционального поражения элементов БЦВК и составить базу команд управления для принятия мер защиты БЦВК в целом. Так, при своевременном поступлении команды управления о временном прекращении работы операционной системы БЦВМ, бортовой комплекс оставался работоспособным и не нарушал функционирование бортовой сети.

Исследование воздействия ЭМИ на элементы БЦВК имеет важное значение при выработке специальных команд для каждого элемента бортовой сети с учетом характера реакции элемента на деструктивное воздействие и его времени для восстановления функционирования. При воздействии на БЦВК сверхширокополосного импульсного излучения основным наблюдаемым эффектом становится искажение передаваемой по бортовой сети информации. Типовые осциллограммы сигнала наводки на сетевом кабеле, соединяющем вычислитель 1, коммутатор и вычислитель 2 в момент передачи информации при воздействии СКИ ЭМИ, приведены на рис. 4 ($\tau_и$ = 170 пс, 30% потерь информационных пакетов) и рис. 5.

Во время исследований в качестве датчиков ЭМВ использовались полосковые преобразователи, подключенные к СОДЭМВ. Также учитывалась особенность функционирования каждого элемента, входящего в состав БЦВК, для определении наиболее эффективного способа приостановки его функционирования. При этом добивались минимальных потерь и разрушений в передаваемом/обрабатываемом массиве данных. Хранение и передачу информации в ИСАУ следует организовывать в виде распределенных информационных полей НС: поля идентификации известных ЭМВ классификаторов нижнего уровня и поля накопления опыта классификатора верхнего уровня СОДЭМВ.

Процесс адаптации информационного поля идентификации известных ЭМВ связан с решением задач классификации ЭМВ по их признакам, приводящим к коррекции информационного поля идентификации на нижнем уровне СОДЭМВ. Процесс адаптации информационного поля накопления опыта связан с решением задач кластеризации ЭМВ по совокупному вектору их признаков, формируемому статистической, сигнатурной и адаптивной СОДЭМВ.

Классификаторы адаптивных уровней СОДЭМВ организованы по схеме: система нечетких продукционных правил → «нечеткая НС» → самообучающаяся НС. Самообучающаяся НС необходима для решения задачи кластеризации. В процессе самообучения НС добиваются такого разбиения векторов обучающей выборки на группы (за счет уменьшения размеров допустимой окрестности кластеров), чтобы число групп в четком классификаторе совпало с числом правил в системе нечетких продукционных правил.

Последнее условие необходимо для создания адаптивного классификатора. При изменении вектора посылок он изменяет размерность вектора заключений, т.е. решая задачу кластеризации, четкая НС изменяет размерность вектора заключений. Это способствует добавлению новых правил в систему нечетких продукционных правил и соответствующих формальных нейронов в нечеткую НС. Обучение нечеткой НС и анализ весов связей вновь введенных формальных нейронов позволяют сформировать спецификацию на отсутствующие датчики ЭМВ в СОДЭМВ.

Заключение. Предложенная иерархическая модель интеллектуальной системы анализа устойчивости элементов и узлов БЦВК к деструктивному воздействию ЭМИ включает СОДЭМВ, множество ДЭМВ, средства сигнатурного и статистического анализа, взаимосвязанных как с внешней средой, так и с аппаратно-программными компонентами самого БЦВК. В процессе работы СОДЭМВ происходит накопление опыта по обнаружению ДЭМВ за счет адаптации информационных полей нейронных и нейро-нечетких сетей, систем нечетких продукционных правил, матриц экспертных оценок. Коррекция матриц экспертных оценок изменяет систему показателей стойкости БЦВК, которая позволяет отслеживать (с помощью методики обнаружения ДЭМВ и оптимизации СОДЭМВ) динамику стойкости БЦВК и принимать решение о расширении структуры и состава ДЭМВ в многоуровневой ИСАУ.

ЛИТЕРАТУРА

1. **Михайлов В.А., Мырова Л.О., Царегородцев А.В.** Структура интеллектуальной системы анализа и оценки устойчивости БЦВК к деструктивному воздействию ЭМИ // Системы и средства связи, телевидения и радиовещания. – 2012. – № 1, 2. – С. 116–120.
2. **Михайлов В.А., Мырова Л.О., Царегородцев А.В.** Интеллектуальная система анализа и оценки устойчивости БЦВК к деструктивному воздействию ЭМИ // Электросвязь. – 2012. – № 8. – С. 36–40.

Получено 24.04.13