

7. Конфиденциальность (RFC 1827)

Заголовок конфиденциальности (ESP-Encapsulating Security Payload) (рис.5) позволяет шифровать совокупность пакетов или их транспортные части. Так же как и аутентификация, конфиденциальность предполагает наличие ассоциации безопасности, включающей среди прочего ключ шифрования и индекс параметров безопасности.

Конфиденциальность имеет два режима:

- транспортный «от края до края», где информация протокола верхнего уровня (в основном транспортного протокола), включая его заголовок, шифруется;

- туннельный между двумя шлюзами безопасности, где пакеты шифруются целиком.

0	8	16	24	31
Индекс параметров безопасности				
Синхронизирующие данные (переменная длина)				
Зашифрованные данные (переменная длина)				

Рис. 5. Формат заголовка конфиденциальности

Перед шифрованием к сообщению добавляется необходимое количество битов выравнивания, число которых зависит от алгоритма шифрования. Опциональный номер последовательности может быть размещен в незашифрованной части заголовка.

Стандартным алгоритмом для шифрования является DES (Data Encryption Standard) [FIPS-46] и тройной DES в режиме CBC (Cipher Block Chaining) [FIPS-81]. Также предлагаются другие алгоритмы, такие как IDEA, RC5 или CAST-128.

Последние предложения описывают смешанный режим аутентификация/конфиденциальность, который обеспечивает аутентификацию, целостность, защиту от повторного использования и конфиденциальность – и все это используя единую АБ.

8. Управление ассоциациями безопасности и ключами

Существует два подхода к управлению ключами шифрования в сети. Наиболее простой – ручное управление ключами, состоящее в том, чтобы позволить каждому пользователю конфигурировать вручную систему ключей на каждом компьютере системы безопасности. Этот подход оказывается довольно не практичным в статической среде малых размеров. В случае локальной сети ручная конфигурация

ключей каждого маршрутизатора позволит шифровать маршрутизируемые данные и снижать риск вторжения на маршрутизатор. Однако ввиду быстрого разрастания сетей этот подход не годится надолго.

Другой подход – это автоматическое управление ключами, которое состоит в обмене ключами шифрования путем посылки соответствующих сетевых сообщений. В настоящее время разработано множество протоколов управления ключами для АБ:

- ISAKMP (Internet Security Association and Key Management Protocol) – доминирующее предложение на сегодняшний день. Оно определяет протокол для АБ, обеспечивающий создание, модификацию и распространение ключей. Обеспечивает также аутентификацию партнеров;

- Oakley – протокол аутентификации партнеров и управления ключами шифрования. Oakley базируется на алгоритме обмена ключей Диффи-Хеллмана;

- SKIP (Simple Key-Management for Internet Protocols) – позволяет аутентифицировать ключи. Не управляет базами данных АБ, но систематически отправляет необходимые криптографические данные в заголовке, предшествующем заголовкам АН и ESP;

- Photuris – протокол, реализующий аутентификацию и обмен публичными ключами.

Среди всех протоколов управления ключами и/или АБ только для ISAKMP, Oakley и Photuris компрометация долговременного ключа не компрометирует предварительно обменяемые ключи и, следовательно, конфиденциальность проведенного сеанса связи.

Литература: 1. Scott O. Bradner, Allison Mankin. IPng. Internet Protocol Next Generation. Addison-Wesley, Reading, Massachusetts. 1995. 307 p. 2. Huitema C. IPv6: The New Internet Protocol. Prentice Hall, Englewood Cliffs, New Jersey. 1996. 188 p. 3. Stephen A. Thomas. IPv6 and the TCP/IP Protocols. Wiley Computer Publishing. 1996. 481 p. 4. Gisèle Cizault. IPv6: Théorie et pratique. O'Reilly, Paris. 1998. 285 p.

Поступила в редколлегию 09.10.98

Рецензент: д-р техн. наук Долгов В.И.

Фрадков Сергей Александрович, аспирант кафедры АПВТ ХТУРЭ. Научные интересы: сетевые технологии, защита информации, техническая диагностика. Увлечения: программирование, путешествия, иностранные языки. Адрес: Украина, 310726, Харьков, пр.Ленина, 14, тел. +38 (0572) 40-93-26.

УДК 681.325

АЛГОРИТМЫ УСЛОВНОГО ДИАГНОСТИРОВАНИЯ ВЫЧИСЛИТЕЛЬНЫХ УСТРОЙСТВ

ХАХАНОВ В.И., СЫСЕНКО И.Ю.,
ПОБЕЖЕНКО В.В., МОНЖАРЕНКО И.В.

Предлагаются алгоритмы условного диагностирования введенного класса макродефектов вычислительных устройств с использованием методов обратного прослеживания и половинного деления на основе выполнения

безусловных процедур структурного анализа и моделирования результатов диагноза. Для выбора точки контроля используется граф функциональных связей эквивалентных линий, задаваемый в виде матрицы достижимостей.

1. Алгоритм обратного прослеживания

Представленный ниже алгоритм условного диагностирования, не дифференцируемый строго на процедуры контроля и поиска дефектов, описывается обобщенным уравнением диагноза:

$$F^*(F, T, D) \mid_{F, T, g^*} = \bigcup_i (g(T, F) \cap g^*(T, F, D_i)) = \emptyset,$$

где g , g^* – эталонная и экспериментальная реакции наблюдаемых линий цифрового устройства (ЦУ); F ,

T , D – функционал, проверяющий тест, наперед заданные дефекты.

Использование сигнатурного анализа [1, 2] определяет элементарную проверку $P_i = g^*(T, F, D_i)$ как получение сжатой реакции при подаче проверяющего теста T на выбранном наблюдаемом контакте i схемы. Проверка P_i считается положительной, если в точке контроля i эталонная сигнатура, вычисленная при отсутствии неисправностей в схеме, равна экспериментальной: $S_M = S_R$. Если же $S_M \neq S_R$, проверка P_i отрицательная. В общем случае идентификация проверки определяется выражением



Точкой контроля i является внешний контакт примитива, микросхемы, типового элемента замены (ТЭЗ), цифрового устройства. Два логических исхода проверки задают альтернативные пути поиска дефекта или определения технического состояния объекта:



где $D_S = D_0 \cup D$; $D^+ \cup D^- = D$; $D^+ \cap D^- = \emptyset$; D_0 – исправное техническое состояние; D – предполагаемая область существования дефектов; D^+ (D^-) – область неисправностей, определяемая положительной (отрицательной) проверкой P^+ (P^-).

Поэтому алгоритм диагностирования методом обратного прослеживания является условным и зондовым, он использует сигнатурный логический анализатор. Длительность и стоимость выполнения условного диагностического эксперимента на порядок выше, чем у безусловного. В отличие от метода половинного деления [1, 3] он ориентирован на поиск не только логических дефектов, но и на обнаружение разрывов линий. Стратегия обратного прослеживания неисправности по структуре объекта, связанная с введенным классом макродефектов, изначально была ориентирована на последовательное выполнение проверок линий функционально-логического подграфа [4], в целях восстановления работоспособности цифрового модуля на стадии производства или эксплуатации при использовании в качестве средства диагностирования "ложка из гвоздей" или автоматического зонда [5].

Диагностическая модель устройства представлена графом функционально-гальванических связей контактов микросхем и ЦУ:

$$G = \{L_{ij} \in L, F_{tr}^k \in F\},$$

где L_{ij} – (дуга) гальваническое отношение одного потенциала между контактами различных конструктивов или примитивов; F_{tr}^k – (дуга или дуги F_{tr}^k k -го ПЭ) функциональное отношение между входной t и выходной r переменной. Для построения алгоритма диагностирования необходимы: полный проверяющий тест относительно одиночных константных неисправностей T , эталонные сигнатуры $S_{\text{эТ}}$ всех внешних контактов микросхем и ТЭЗа, граф функционально-гальванических связей F^G цифрового модуля:

$$W = \{G, T, S_M\}.$$

Чтобы приблизить модели неисправностей к реальным, введем следующие типы состояний объекта:

$$D_S = \{D_0, D_1, D_2, D_3, D_4, D_5\},$$

где D_0 – исправное состояние объекта, определяется совпадением $S_M = S_R$ по всем выходным контактам устройства:

$$D_0 \Leftarrow [g(T, F) \cap g^*(T, F, D_i) = g(T, F)];$$

D_1 – отсутствие гальванической связи между контактами различных микросхем:

$$D_1 \Leftarrow [S_M(L_i) = S_R(L_i) \ \& \ S_M(L_j) \neq S_R(L_j)];$$

D_2 – неисправность на выходе k -го элемента или внутри него:

$$D_2 \Leftarrow \{\forall t [S_M(F_{tr}^k) = S_R(F_{tr}^k)] \ \& \ \exists r [S_M(F_{tr}^k) \neq S_R(F_{tr}^k)]\};$$

D_3 – отсутствие связи между входом и шиной константы $\equiv 0, \equiv 1$:

$$D_3 \Leftarrow [S_M(\{\equiv 0, \equiv 1\}) = S_R(\{\equiv 0, \equiv 1\}) \ \&$$

$$\ \& \ S_M(L_j = \{\equiv 0, \equiv 1\}) \neq S_R(L_j)];$$

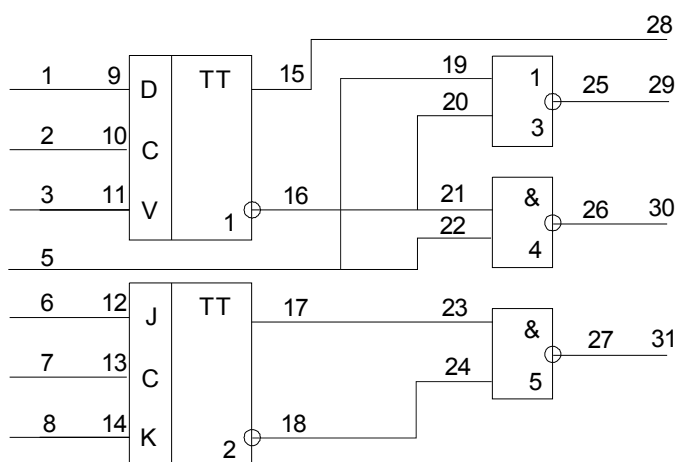
D_4 – неисправность внешнего входного контакта цифрового объекта:

$$D_4 \Leftarrow [S_M(L_i) \neq S_R(L_i) \ \& \ S_M(L_j) \neq S_R(L_j)];$$

D_5 – неисправность выходов, объединенных в монтажную логику:

$$D_5 \Leftarrow \{\forall i [S_M(L_i) \neq S_R(L_i)] \ \& \ [S_M(L_j) \neq S_R(L_j)]\}.$$

Построим алгоритм поиска дефектов методом обратного прослеживания для схемы, изображенной на рисунке.



Априорно все доступные контакты идентифицируются порядковыми номерами или топологическими идентификаторами <координата микросхемы, номер ножки>. Последовательность диагностирования контактов на топологии схемы определяется двумя направлениями: справа-налево – при отрицательной проверке; снизу-вверх – при положительной. (Направления могут быть и другими.) Такая стратегия задает в качестве очередной точки контроля при отрицательной проверке P^-_i на выходе элемента его первый нижний входной контакт. При фиксации положительного результата P^+_i на входном контакте примитива очередная точка контроля задается расположенной выше входной ножкой. Если в последнем случае проверка отрицательная, очередная точка контроля определяется выходным

Для предложенного примера построенный алгоритм диагностирования представлен в таблице.

$$G^n = \bigvee_j \{ \cap G_j \leftarrow [S_M(L_j^Y) \neq S_R(L_j^Y) \mid j=1..m] \}; \quad (1)$$

Pi	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17
Pi+	30	29	28	D 0	D 1	D 1	D 1	23	D 2	21	D 2	19	D 2	D 1	D 1
Pi-	27	26	25	15	24	22	20	18	17	5	16	16	5	14	14
Sign	21FE	31FE	41FE	51FE	21FE	31FE	41FE	11F4	1133	11F1	1110	1110	11F1	11F4	1133
Pi	16	15	14	13	12	11	10	9	8	7	6	5	3	2	1
Pi+	D 1	D 1	13	12	D 2	10	9	D 2	D 1	D 1	D 1	D 1	D 1	D 1	D 1
Pi-	11	11	8	7	6	3	2	1	D 4	D 4	D 4	D 4	D 4	D 4	D 4
Sign	1110	51FE	115E	110E	133E	11H E	11PE	13FE	115E	110E	133E	11F1	11H E	11PE	13FE

Состояние D_0 фиксируется, если все выходы дают положительную проверку; D_1 – на гальванической связи зафиксирована положительная проверка при отрицательной предыдущей; D_2 – при отрицательной проверке на выходе все входы имеют положительный результат сравнения сигнатур; D_3 – отрицательная проверка на входе, связанном с шинами $\equiv 0$, $\equiv 1$; D_4 – отрицательная проверка на внешнем входе цифрового устройства.

где G_j – подграф внутренних точек контроля схемы, являющихся предшественниками для линии L_j^y ; m – число внешних выходов схемы. Ограничение наличия в схеме одиночного дефекта является достаточно сильным, поэтому должны существовать весомые аргументы, чтобы его принять.

Для теста, активизирующего проверку каждого одиночного дефекта на всех выходах ЦУ, подозреваемая область при наличии одиночного (кратного) дефекта определяется разностью между подграфами с отрицательными и положительными по выходам результатами испытаний:

$$G = G^{\cap} \setminus \bigcup_j \{ \cup G_j \Leftarrow [S_M(L_j^Y) = S_R(L_j^Y) \mid j=1, m] \},$$

$$(G = G^U \setminus \bigvee_j \{ \cup G_j \Leftarrow [S_M(L_j^Y) = S_R(L_j^Y) \mid j=1..m] \}) .$$

Поскольку проектирование теста, активизирующего каждый из дефектов до всех наблюдаемых выходов, задача дорогостоящая, на практике для уменьшения подозрительности области следует пользоваться выражениями (1) или (2).

Пример. Пусть существует одиночный дефект $D_1(10, 2)$, который при диагностировании внешних выходов проявился на линиях 28 и 30.

В случае разрыва связи между линиями 2 и 10 (см. рисунок) последовательность выполнения проверок по таблице без структурного анализа имеет стоимость

$$(P_{30}^-, P_{26}^-, P_{22}^+, P_{21}^-, P_{16}^-, P_{11}^+, P_{10}^-, P_2^+) \Rightarrow D_1(10, 2).$$

С использованием структурного анализа подозреваемая область определяется подграфом линий:

$$G = G_{28} \cap G_{30} = \{L_1, L_9, L_2, L_{10}, L_3, L_{11}\}.$$

Стоимость диагностирования, равная числу элементарных проверок для установления диагноза на подграфе G , определяется последовательностью

$$(P_{11}^-, P_{10}^-, P_2^+) \Rightarrow D_1(10, 2),$$

что в 2,6 раза меньше базового алгоритма обратного прослеживания без структурного моделирования результатов сравнения эталонных и экспериментальных сигнатур по наблюдаемым выходам схемы.

2. Алгоритм половинного деления

Для изложения стратегии половинного деления введем вектор моделирования неисправной области $M = (M_1, M_2, \dots, M_i, \dots, M_n)$, где n – общее число точек контроля цифрового модуля. Подмножество наблюдаемых выходных контактов устройства обозначим в виде $M^Y \subset M$, $M^Y \neq \emptyset$. Значение координаты вектора $M_i \in M$ формируется в соответствии с выражением $(M_i = 1) \Leftarrow [S_M(L_i) \neq S_R(L_i) \ \& \ S_M(L_j^Y) \neq S_R(L_j^Y) \ \& \ L_j^Y = f(L_i)]$; в противном случае – $M_i = 0$.

В результате диагностического эксперимента по наблюдаемым выходам формируется подмножество $M^Y \subset M$ вектора моделирования:

$$\text{[Blank Box]} \quad (3)$$

Для $M^Y \subset M$ вычисляется подграф точек контроля цифровой схемы $M' \subset M$, неисправные сигнатуры которых могут сформировать определенное по (3) подмножество $M^Y \subset M$. Построение вектора моделирования неисправной области M для вычисленного подмножества $M^Y \subset M$ с использованием графа цифровой схемы основано на следующих правилах.

2.1. Процедура структурного моделирования

1. Состояния наблюдаемых линий определяются в соответствии с выражением (1) и не могут быть модифицированы с помощью двух следующих правил (пункты 2 и 3).

2. Входные контакты примитива t подозреваются неисправными, если существует выходной дефектный контакт: $(\forall i (M_i(X_t) = 1) \Leftarrow (\exists i (M_i(Y_t) = 1))$.

3. При различных технических состояниях (исправное и неисправное) входов одного потенциала разных примитивов t и f значение линии разветвления подозревается дефектным: $M_i = M_i(X_t) \vee M_i(X_f)$.

С учетом приведенных правил процедуры структурного моделирования и вычисленного подмножества $M^Y \subset M$ алгоритм определения состояний невыходных координат вектора моделирования неисправной области M заключается в последовательной обработке примитивов ациклической схемы методом обратного прослеживания от внешних выходных контактов схемы ко входным.

Для примера, представленного на рисунке, продемонстрируем выполнение процедуры структурного моделирования, исходя из условия, что

$$M^Y = \{M_{28} = 1, M_{29} = 0, M_{30} = 1, M_{31} = 0\}.$$

Результат моделирования на основе выполнения правил 2 и 3 дает вектор единичных переменных:

$$M = (1 \ 2 \ 3 \ 5 \ 9 \ 10 \ 11 \ 15 \ 16 \ 21 \ 22 \ 26 \ 28 \ 30).$$

На подграфе $G'(M)$, который представлен матрицей $Q = ||Q_{ij}||$, организуется условный диагностический эксперимент с выбором точки контроля, делящей подозреваемую область пополам.

2.2. Процедура выбора контрольной точки

Чтобы изложить стратегии выбора очередного контакта для зондирования схемы, количество единичных координат в вектор-строке предшественников для точки контроля i матрицы $Q = ||Q_{ij}||$ достижи-

мостей обозначим через $A_i = \text{card}(Q_{ij}) \mid j=1, n$; в вектор-столбце преемников – через $B_i = \text{card}(Q_{ji}) \mid j=1, n$. Определим также множество точек контроля предшественников и преемников в виде $\{A_i\}$, $\{B_i\}$. Тогда при стратегии выбора контрольной точки, делящей подозреваемую область пополам, необходимо максимизировать по параметру i выражение $(A_i + B_i)/n$ (n – мерность матрицы Q , соответствующей подграфу $G'(M)$), которое показывает мощность делимого подграфа $(A_i + B_i)$ по отношению к исходному $G'(M)$. Кроме того, минимизация разности предшественников и преемников точки контроля i $(A_i - B_i)/n$ показывает точность половинного деления структуры $G'(M)$. В результате получаем функционал

$$f = \text{MAX} \mid_i [(A_i + B_i)/n - (A_i - B_i)/n] = \text{MAX} \mid_i [(2/n)(B_i)]. \quad (4)$$

Учитывая, что коэффициент $(2/n)$ есть константа, ее можно исключить из выражения (4), считая при этом, что определение мощности B_i связано с выбором минимального значения из компонентов A_i , B_i :

$$f = \text{MAX} \mid_i [\text{MIN}(A_i, B_i)]. \quad (5)$$

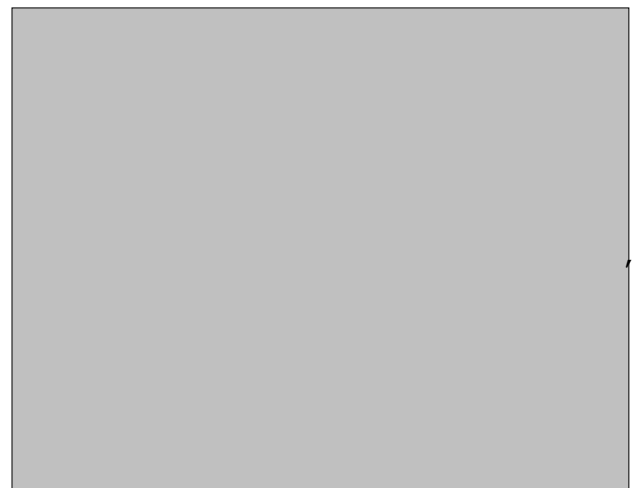
Если существует несколько одинаковых значений функционалов f , то для однозначности выбирается точка контроля с меньшим индексом i .

В случае отрицательной проверки на линии P_k область неисправностей задается множеством предшественников $\{A_k\}$ текущей матрицы достижимостей $Q = ||Q_{ij}||$, а при положительной – разностью между исходным множеством и предшественниками для линии P_k :

$$\text{[Blank Box]} \quad (6)$$

Пусть в схеме, представленной на рисунке, задана неисправность типа "разрыв гальванической связи между контактами 2 и 10": $D_1(10, 2)$. Выполним модельный условный диагностический эксперимент для поиска заданного дефекта при условии, что он сформировал неправильные реакции по наблюдаемым выходам, указанным в множестве M^Y . Выполним итеративную процедуру диагностирования на основе модификации матриц подграфов неисправных областей.

Вычисляя значения функционала f для каждой точки контроля исходной матрицы



заданной на векторе переменных M , который получен в результате выполнения процедуры структурного моделирования, определяем для всех строк и столбцов количество единичных координат:



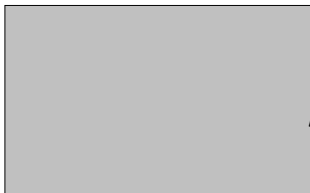
Критерию f удовлетворяет точка контроля P_{16} . После выполнения элементарной проверки на линии P_{16} область подозреваемых дефектов определяется вектором переменных $M(P_{16}) = (1\ 2\ 3\ 9\ 10\ 11\ 16)$, для которого подграф цифровой схемы задается уже в виде матрицы



Вычисление функционала f по данной матрице дает очередную точку контроля P_9 , в которой фиксируется положительная проверка, определяющая область существования дефекта в виде вектора линий:

$$M(P_9) = M(P_{16}) \setminus \{B_9\} = (1\ 2\ 3\ 9\ 10\ 11\ 16) \setminus \{1, 9\} = (2\ 3\ 10\ 11\ 16).$$

Данной области неисправных линий соответствует матрица



по которой вычисление функционала f определяет следующей точку контроля P_{10} . Элементарная проверка в P_{10} дает отрицательный результат, что позволяет вычислить по (6) область дефектов:

$$M(P_{10}) = \{A_{10}\} = (2, 10).$$

Очередная проверка на линии P_2 дает положительный результат, что является основанием для диагноза – неисправность $D_1(10, 2)$.

Таким образом, процедура диагностирования наперед заданного дефекта $D_1(10, 2)$ имеет стоимость, определяемую четырьмя проверками:

$$(P_{16}, P_9, P_{10}, P_2) \Rightarrow D_1(10, 2),$$

что только на одну больше, чем при структурном анализе, и это естественно, поскольку процедура структурного моделирования ориентирована на поиск как одиночных, так и кратных дефектов.

Предложенные алгоритмы реализуют условное диагностирование макродефектов на основе использования процедур: структурного анализа и структурного моделирования, а также методов: обратного прослеживания и половинного деления подозреваемой области, когда очередная точка контроля при анализе матрицы достижимостей вычисляется по критерию $MAXMIN_a$.

Выборочная статистика (на девяти схемах) числа зондирований для установления диагноза дефекта D_1 на одном из входов ЦУ дает среднюю оценку относительного уменьшения количества точек контроля, равную

$$q = \text{card}(AOP_6) / \text{card}(AOP_c) = 2,75.$$

Литература: 1. Ярмолик В.Н. Контроль и диагностика цифровых узлов ЭВМ. Минск: Наука и техника, 1989. 234с. 2. Гордон Д., Надиг Х. Локализация неисправностей в микропроцессорных системах при помощи шестнадцатеричных ключевых кодов // Электроника. 1977. №5. С.23–33. 3. Пархоменко П.П., Согомоян Е.С. Основы технической диагностики (Оптимизация алгоритмов диагностирования, аппаратные средства) / Под ред. П.П. Пархоменко. М.: Энергия, 1981. 320 с. 4. Кривуля Г.Ф., Кузуб В.А., Коновалов В.Б., Хаханов В.И. Автоматизированная система диагностирования цифровых модулей // Электронное моделирование / 1987. №2. С.57–61. 5. Байда Н.П., Кузьмин И.В., Шпилевой В.Т. Микропроцессорные системы поэлементного диагностирования. М.: Радио и связь, 1987. 256 с. 6. Хаханов В.И. Техническая диагностика элементов и узлов персональных компьютеров. К.: ІЗМН. 1997. 308 с.

Поступила в редколлегию 12.10.98

Рецензент: д-р техн. наук Кривуля Г.Ф.

Хаханов Владимир Иванович, д-р техн. наук, профессор кафедры автоматизации проектирования вычислительной техники ХТУРЭ. Научные интересы: техническая диагностика вычислительных устройств, систем, сетей и программных продуктов. Увлечения: баскетбол, футбол, горные лыжи. Адрес: Украина, 310726, Харьков, пр. Ленина, 14, тел. 40–93–26.

Сысенко Ирина Юрьевна, студентка кафедры автоматизации проектирования вычислительной техники ХТУРЭ. Научные интересы: техническая диагностика вычислительных устройств. Увлечения: аэробика, музыка. Адрес: Украина, 310726, Харьков, пр. Ленина, 14, тел. 40–93–26.

Побеженко Владимир Викторович, студент кафедры автоматизации проектирования вычислительной техники ХТУРЭ. Научные интересы: техническая диагностика вычислительных устройств. Увлечения: книги, иностранные языки. Адрес: Украина, 310726, Харьков, пр. Ленина, 14, тел. 40–93–26.

Монжаренко Ирина Витальевна, канд. техн. наук, ассистент кафедры автоматизации проектирования вычислительной техники ХТУРЭ. Научные интересы: техническая диагностика вычислительных устройств. Адрес: Украина, 310726, Харьков, пр. Ленина, 14, тел. 40–93–26.