Анатолий А. Чупринов[1], Дмитрий О. Смирнов[2]
[1]ФГБУ «Всероссийский научно-исследовательский институт радиоэлектроники», ул. Колпакова, 2а, Мытищи, Московская обл., 141002, Россия
[2]Общество с ограниченной ответственностью «Центр безопасности информации», ул. Ленинская, 11, Королёв, Московская обл., 141090, Россия
[1]e–mail: toliy1962@list.ru, https://orcid.org/0000-0002-8785-6797
[2]e–mail: space_dim@rambler.ru, https://orcid.org/0000-0001-5388-7547

МЕТОД КОСВЕННЫХ ПРИЗНАКОВ ДЛЯ ВЫЯВЛЕНИЯ АППАРАТНЫХ УГРОЗ ТЕХНИЧЕСКИХ СРЕДСТВ*

DOI: http://dx.doi.org/10.26583/bit.2022.2.01

Аннотация. Использование зарубежных систем автоматизированного проектирования (САПР) и отладки сложно-функциональных блоков (СФ- или IP-блоков) при разработке сверхбольших интегральных схем (СБИС) связано с рисками появления «закладок», не декларируемых разработчиками программных продуктов и готовых изделий (чаще именуемых за рубежом «троянами»). «Трояны» сравнительно несложно «встроить» так, что они не будут обнаружены сгенерированными той же зарубежной САПР тестами и тестовыми последовательностями при контроле готового изделия. Выявление «троянов» позволяет повысить уровень информационной безопасности радиоэлектронной аппаратуры (РЭА), в составе которой применяются СБИС иностранного производства. Процедурам выявления «троянов» следует подвергать и отечественные СБИС, разработанные и изготовленные с использованием зарубежных САПР и их элементов. В качестве объектов угроз снижения информационной безопасности выбраны четыре класса элементов: аппаратные, не имеющие встроенного программного обеспечения; аппаратные, не имеющие встроенного программного обеспечения, изменяющие реализуемые функции в зависимости от внешнего воздействия; программно-аппаратные, содержащие компьютерную программу и данные, которые не могут изменяться средствами пользователя; программно-аппаратные, содержащие компьютерную программу и данные, которые могут изменяться средствами пользователя. В общем виде угроза безопасности информации рассматривается как несвойственная компоненту функция, реализация которой наносит ущерб пользователю РЭА. В настоящей статье рассмотрена задача создания методического аппарата выявления информационных закладок в сверхбольших интегральных схемах (СБИС). Для решения задачи предложен метод косвенных признаков, позволяющий выявить наличие или вероятность наличия информационной угрозы в СБИС или РЭА, использующей данную СБИС. Сущность метода заключается в применении сигнатурного анализа, основанного на применении тестовых последовательностей, позволяющих установить однозначное соответствие между входными воздействиями и откликами тестируемой СБИС, зависящее только от ее внутренних параметров. Разработанный математический аппарат может быть положен в основу аппаратно-программных средств контроля информационной безопасности образцов РЭА двойного назначения.

Ключевые слова: элементная компонентная база, проверка, информационная безопасность, безопасность информации, сигнатура.

Для цитирования: ЧУПРИНОВ, Анатолий А.; СМИРНОВ, Дмитрий О. МЕТОД КОСВЕННЫХ ПРИЗНАКОВ ДЛЯ ВЫЯВЛЕНИЯ АППАРАТНЫХ УГРОЗ ТЕХНИЧЕСКИХ СРЕДСТВ. Безопасность информационных технологий, [S.l.], т. 29, № 2, с. 10–19, 2022. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1414. DOI: http://dx.doi.org/10.26583/bit.2022.2.01.

Благодарности. *Авторы выражают благодарность и свою признательность доктору технических наук, профессору Телец В.А. за высказанные редакционные предложения.*

Anatoliy A. Chuprinov[1], Dmitry O. Smirnov[2]
[1]*Federal State Budgetary Institution "All-Russian Research Institute of Radio Electronics", Kolpakova Str. 2a, Mytischi, 141002, Russia*
[2]*Limited Liability Company "Information Security Center", Leninskaya Str.,11, Korolev, 141090, Russia*
[1]*e–mail: toliy1962@list.ru, https://orcid.org/0000-0002-8785-6797*
[2]*e–mail: space_dim@rambler.ru, https://orcid.org/0000-0001-5388-7547*

Indirect signs method for detecting hardware threats of technical means*

DOI: http://dx.doi.org/10.26583/bit.2022.2.01

Abstract. The use of foreign computer-aided design (CAD) systems and debugging of IP-blocks in the development of ultra-large integrated circuits (VLSI) are associated with the risks of the appearance of "Trojans", not declared by developers of software and finished product. "Trojans" are relatively easy to embed, so that they will not be detected by tests and test sequences, generated by the same CAD system, when checking the finished product. The identification of "Trojans" allows increasing the level of information security of electronic equipment, which uses VLSI of foreign production. Procedures for detecting "Trojans" should also be subjected to domestic VLSI, developed and manufactured using CAD systems and the elements. Four classes of elements were selected as objects of threats to reduce information security: hardware, without embedded software; hardware, that do not have built-in software, changing the implemented functions depending on external influences; software and hardware, containing a computer program and data that cannot be changed by the users; software and hardware, containing a computer program and data that can be changed by the users. In general, the threat to information security is considered as a function that is not characteristic of the component, which implementation damages the user of the electronic equipment. The task of creating a methodological apparatus for identifying information Trojans in VLSI is considered in the paper. In order to solve the problem a method of indirect signs is proposed, which allows identifying the presence or probability of an information threat in the VLSI or electronic equipment, using this VLSI. The essence of the method consists in the application of signature analysis, based on the use of test sequences that help to establish an unambiguous correspondence between the input effects and the responses of the tested VLSI, depending on its internal parameters only. The developed mathematical apparatus can be used as the basis for hardware and software control of information security of the dual-use electronic equipment.

Keywords: electronic component base, verification, information security, information security, signature, database, software.
For citation: CHUPRINOV, Anatoliy A.; SMIRNOV, Dmitry O. Indirect signs method for detecting hardware threats of technical means. IT Security (Russia), [S.l.], v. 29, no. 2, p. 10–19, 2022. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1414. DOI: http://dx.doi.org/10.26583/bit.2022.2.01.

Acknowledgement. *The authors expresses their gratitude and appreciation to the Doctor of Technical Sciences, Professor V.A. Telets for the editorial suggestions made.*

Введение

Разработка современных и перспективных СБИС предполагает использование зарубежных систем автоматизированного проектирования (САПР) и отладки сложно-функциональных блоков (СФ- или IP-блоков), что потенциально связано с рисками появления «закладок», не декларируемых разработчиками программных продуктов и готовых изделий (чаще именуемых за рубежом «троянами»).

Для достижения максимального уровня информационной безопасности в сфере СБИС, как основы элементной компонентной базы (ЭКБ) для комплектования

радиоэлектронной аппаратуры (РЭА), следует подвергать специальной проверке не только интегральные микросхемы, которые проектировались и/или изготавливались за рубежом, но и отечественные СБИС, разработанные и изготовленные с использованием зарубежных САПР и их элементов.

«Трояны» сравнительно несложно «встроить» так, что они не будут обнаружены сгенерированными той же зарубежной САПР тестами и тестовыми последовательностями для контроля готового изделия. Поэтому проблема защиты информации и информационной безопасности радиоэлектронных систем различного назначения не теряет актуальности, что обусловлено возрастанием роли информационных ресурсов в конкурентной борьбе и широкими возможностями несанкционированного доступа к конфиденциальной информации.

Имея доступ к такой информации, можно нанести серьезный ущерб. Так, например, по оценкам западных экспертов, в современных условиях утечка 20% коммерческой информации в шестидесяти случаях из ста приводит к банкротству предприятия [1].

Прогнозируется, что в скором времени информационные системы практически всех центров управления, обработки данных и принятия решения силовых, финансовых и производственных систем будут подвергаться компьютерным атакам. Примеров таких атак в современной практике множество. Следовательно, защите информации в современных информационных системах управления должно уделяться самое серьезное внимание.

Защита информации в автоматизированной информационной системе – это совокупность мероприятий (рис. 1), обеспечивающих предупреждение физического уничтожения информации, ее модификации, искажения или несанкционированного получения[1].

Угроза безопасности информации – действие или событие, которое может привести к разрушению, искажению или несанкционированному использованию (утечке) информационных ресурсов, включая хранимую, передаваемую и обрабатываемую информацию[1].

Угроза может быть реализована путем непосредственного воздействия на носители информации в автоматизированных информационных системах (АИС) (бумажные документы, магнитные носители), а также путем косвенного воздействия на компоненты технического, программного обеспечения или персонал АИС.

Количество возможных угроз безопасности информации, а также путей их реализации достаточно велико (рис. 2), поэтому для защиты от этих угроз в автоматизированных системах применяют системы защиты информации.

Система защиты информации в автоматизированной системе – это единый комплекс, совокупность взаимосвязанных правовых норм, организационных мер, технических и программных средств, обеспечивающий защищенность информации.

[1]ГОСТ Р 53113.1-2008. Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1.

Рис. 1. Защита информации в АИС центра обработки данных
Fig. 1. Information protection in automated information systems of the data processing center

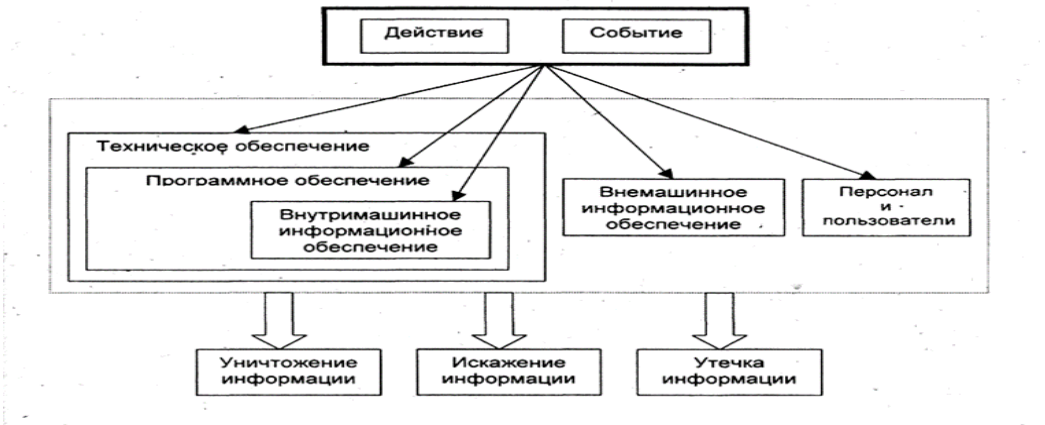

Рис. 2. Понятие угрозы безопасности в автоматизированных информационных системах
Fig. 2. The concept of a security threat in automated information systems

1. Метод косвенных признаков

Для всестороннего анализа угроз, направленных на снижение информационной безопасности аппаратных средств передачи и обработки данных в ИС выделяются четыре класса элементов, которые входят в состав технических средств [2–4]:

1. Аппаратные, не имеющие встроенного программного обеспечения, предназначенные для реализации функций, не управляемых внешним воздействием. Режим функционирования таких элементов задается исключительно аппаратными средствами.

2. Аппаратные, не имеющие встроенного программного обеспечения, изменяющие реализуемые функции в зависимости от внешнего воздействия.

3. Программно-аппаратные, технические средства, содержащие компьютерную программу и данные, которые не могут изменяться средствами пользователя.

4. Программно-аппаратные, технические средства, содержащие компьютерную программу и данные, которые могут изменяться средствами пользователя.

Функции, выполняемые элементами первого класса, являются фиксированными, свойственными каждому элементу. Их изменение возможно лишь при отказе элемента. Отказ элемента приведет к нарушению работоспособности объекта, в котором этот элемент установлен. Причина отказа устанавливается последующей диагностикой.

Функции, выполняемые элементами второго класса, могут регулироваться внешними воздействиями. В этом случае все множество функций $К_N$, выполняемых элементом, предусматривает разработчик, а выполнение функции, не входящей во множество $К_N$, обуславливается либо отказом элемента, либо *несанкционированным* внешним воздействием. Функции, выполняемые элементами третьего класса, зависят от программного обеспечения и данных, заложенных в ПЗУ элемента. В этом случае разработчик имеет возможность предусмотреть выполнение элементом только множества функций $К_N^{Дкл}$, декларируемых изготовителем. Выполнение функции, не входящей во множество $К_N^{Дкл}$, обуславливается либо отказом элемента, либо внутренним сбоем, либо внутренней программой, запущенной нарушителем (агентом нарушителя). Функции, выполняемые элементами четвертого класса, зависят от программного обеспечения и данных, полностью определяемых разработчиком. В этом случае разработчик определяет необходимое множество функций $К_N^{Разр}$, реализуемых элементом. Выполнение функции, не входящей во множество $К_N^{Разр}$, обуславливается либо отказом элемента, либо внутренним сбоем, либо изменением программы, заложенной разработчиком.

Таким образом, в общем виде угроза безопасности информации, может быть представлена как функция (F_i), реализуемая элементом компонентной базы, не свойственная данному элементу $\left(F_i \not\subset К_N^{Разр}\right)$, выполнение которой приводит к возникновению ущерба (C_i) владельцам, пользователям информации и поддерживающей ее структуре.

Угроза безопасности информации (F_i) возникает в момент времени t_0 и существует до момента блокирования t_1 на протяжении периода времени

$$T_{угр} = t_1 - t_0.$$

Очевидно, что чем меньше время существования угрозы (F_i), тем меньшим будет ущерб (C_i).

Для аппаратных элементов характерны внутренние отказы, вызванные естественными причинами [5, 6]. Время наступления угрозы в данном случае может быть определено, исходя из показателей надежности элемента. Например, соответствовать среднему времени наработки до отказа.

В более общем случае рассчитать среднее время наработки до отказа возможно по формуле:

$$T_1 = \int_0^\infty tf(t)dt = \int_0^\infty [1 - F(t)]\,dt, \quad (1)$$

где $f(t)$ – плотность распределения наработки до отказа, $F(t)$ – функция распределения наработки до отказа.

На величину наработки до отказа влияют деструктивные воздействия внешних факторов [7, 8], как природного, так и техногенного характера (например, влажность, радиация и т.п.), однако, эти факторы учитываются разработчиком при предъявлении требований к ЭКБ.

Учитывая вышесказанное, запишем результирующий вид формальной модели угрозы информации в системе обработки информации.

Предположим, что имеем техническое средство A, состоящее из i отдельных компонентов, $A = \{a_1, a_2, \dots, a_i\}$.

Функционирование компонента a_n, где $n = 1, 2, \dots, i$, в составе технического средства A в течение времени t в общем случае описывается выражением:

$$\vec{\sigma}_{a_n}(t) = F_{a_n}\left(\overrightarrow{X_{a_n}}, \overrightarrow{H_{a_n}}, t\right), \quad (2)$$

где: t – время функционирования компонента a_n; $\overrightarrow{X_{a_n}} = \left\{x_1^{a_n}, x_2^{a_n}, \dots, x_q^{a_n}\right\}$ – множество внешних воздействий на компонент; q – число внешних воздействий на компонент; $\overrightarrow{H_{a_n}} = \left\{h_1^{a_n}, h_2^{a_n}, \dots, h_p^{a_n}\right\}$ – множество внутренних параметров компонента; p – число внутренних параметров компонента.

Внешними (входными) воздействиями на компонент в описываемой модели являются:

статические входные сигналы;

динамические сигналы, изменяющиеся во времени по заданным законам.

$$\vec{x} = \{U^{\text{ст}}, U^{\text{дин}}\}, \quad (3)$$

где: $U^{\text{ст}} = \{U_1^{\text{ст}}, U_2^{\text{ст}}, \dots, U_k^{\text{ст}}\}$ – множество статических входных сигналов; k – число статических входных сигналов; $U^{\text{дин}} = \left\{U_1^{\text{дин}}, U_2^{\text{дин}}, \dots, U_l^{\text{дин}}\right\}$ – множество динамических входных сигналов; l – число динамических входных сигналов.

Выходными характеристиками электронного компонента в данной модели являются:

потребляемая мощность $\text{Р}_{\text{Потр}}^{\text{а}}$ при статических воздействиях;

интегральная потребляемая мощность $\text{Р}_{\text{Потр}}^{\text{дин}}$ при динамических воздействиях в течение времени воздействия $t^{\text{дин}}$;

величины временных задержек реакции исследуемого компонента на входные динамические воздействия τ.

$$\overrightarrow{\sigma_{a_n}}(t) = F_{a_n}(U^{\text{ст}}, U^{\text{дин}}) = \left\{P_{\text{Потр}}^{\text{ст}}, P_{\text{Потр}}^{\text{дин}}, \tau\right\}, \quad (4)$$

где: F_{a_n} – закон функционирования компонента a_n; $\overrightarrow{\sigma_{a_n}}(t) = \left\{q_1^{a_n}, q_2^{a_n}, \dots, q_s^{a_n}\right\}$ – множество выходных характеристик (откликов) компонента a_n; $P_{\text{Потр}}^{\text{ст}} = \left\{P_{\text{Потр1}}^{\text{ст}}, P_{\text{Потр2}}^{\text{ст}}, \dots, P_{\text{Потр}k}^{\text{ст}}\right\}$ – множество величин потребляемых мощностей при воздействиях статических входных сигналов $U^{\text{ст}}$; k – число статических входных сигналов; $P_{\text{Потр}}^{\text{дин}} = \left\{P_{\text{Потр1}}^{\text{дин}}, P_{\text{Потр2}}^{\text{дин}}, \dots, P_{\text{Потр}l}^{\text{дин}}\right\}$ – множество величин интегральных потребляемых мощностей при воздействиях динамических входных сигналов $U^{\text{дин}}$ в течение времени воздействия $T^{\text{дин}}$; l – число динамических входных сигналов; $\tau = \{\tau_1, \tau_2, \dots, \tau_l\}$ – множество временных задержек реакции исследуемого компонента на входные динамические воздействия.

Учитывая существующий разброс внутренних параметров компонентов a_n, методические ошибки, ошибки оператора, погрешности измерений, необходимо набрать статистическую информацию о множестве выходных характеристик $\overrightarrow{\sigma_n^{\text{Эт}}}(t)$ эталонных компонентов $a_n^{\text{Эт}}$, определить законы распределения каждой из них, требования к измерительным приборам, и задать интервалы, при выходе за пределы которых будет считаться, что в компоненте a_n существуют конструктивно-технологические изменения, а, следовательно, существует угроза информационной безопасности $y_i \in Y = \{y_1, y_2, \dots, y_m\}$.

Если $\left| \overrightarrow{\sigma_{a_n}}(t) - \overrightarrow{\sigma_n^{\text{Эт}}}(t) \right| < |\xi| \Rightarrow Y = \{\emptyset\}$ – угрозы не существует.

В противном случае, если $\left|\overrightarrow{\sigma_{a_n}}(t) - \overrightarrow{\sigma_n^{\text{Эт}}}(t)\right| > |\xi| \Rightarrow Y \neq \{\emptyset\}, \exists \text{у}_i = f\left(\overrightarrow{\sigma_{a_n}}(t)\right) \in Y$ – считается, что объект подвержен угрозе, где ξ – граница интервала; $Y = \{y_1, y_2, \dots, y_m\}$ – множество угроз информационной безопасности; i – номер элемента в множестве.

В соответствии с определением, приведенным в ГОСТ Р 50922-2006[2], под угрозой подразумевается совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Предположим, что система обработки информации (СОИ) подвержена множеству угроз Y.

Для реализации *i*-й угрозы необходимо наличие условий и факторов:

$$\text{у}_i = \{C_i, F_i\}, \tag{5}$$

где: у_i – i-я угроза; C_i – множество условий реализации *i*-й угрозы $C_i = \{c_1^i, c_2^i, \dots, c_k^i\}$; F_i – множество факторов реализации *i*-й угрозы $F_i = \{f_1^i, f_2^i, \dots, f_l^i\}$; c_k^i – *k*-е условие осуществления *i*-й угрозы; f_l^i – *l*-й фактор осуществления *i*-й угрозы; *k* и *l* – число условий и факторов реализации *i*-й угрозы, соответственно.

Формальная модель угроз будет выглядеть следующим образом:

$$Y = \{C_1, F_1\} \cup \{C_2, F_2\} \cup \dots \cup \{C_i, F_i\}. \tag{6}$$

Пусть $Q = \{q_1, q_2, q_3, \dots q_t\}$ – множество требований безопасности информации, которым соответствует СОИ.

Множество актуальных угроз Y так отображается на множество требований безопасности информации Q, которым соответствует СОИ, что любому элементу множества Y, должен соответствовать хотя бы один из элементов множества Q. Можно записать:

$$\forall y \in Y \ \exists q \in Q : \ y = f(q). \tag{7}$$

Целевая функция нейтрализации угроз формально выражается следующим образом:

$$\max_{\{Y\},A} f(Q_A, t) = 1 - \sum_{n=1}^{i} \frac{\gamma_n}{i}, \tag{8}$$

где γ_n – значение безопасности *n*-го элемента технического средства A (значение безопасности лежит в пределах [0,1])

$$\gamma_n = 1 - \vartheta_n(Y), \tag{9}$$

где $\vartheta_n(Y)$ – функция определения наличия угроз в *n*-м компоненте технического средства A, определенная на множестве угроз Y.

Для конкретизации модели угроз введем более строгое определение понятия сигнатуры (так как есть математическое строгое определение, завязанное на квадратичные формы).

Предположим, что диагностируемая угроза характеризуется устойчивым набором признаков (представительным набором) или отсутствием этих признаков

[2]Национальный стандарт РФ ГОСТ Р 50922-2006 «Защита информации Основные термины и определения» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. N 373-ст)

(антипредставительным набором), тогда будем говорить о возможности построения для данной угрозы диагностически ценного набора признаков [9–11].

Определение. Под сигнатурой угрозы *n*-го компонента технического средства будем понимать конечную совокупность характеристик компонента технического средства ∂, которая позволяет однозначно определить наличие угрозы y.

Определение. Под тестовой сигнатурой *n*-го компонента технического средства будем понимать однозначное соответствие между внешними воздействиями X_n, множеством откликов φ_n и множеством внутренних параметров H_n на промежутке от t_{start} до t_{finish} (время начала и окончания тестирования соответственно) – интервал ξ, достаточное для идентификации состояния отсутствия угрозы y.

Множество угроз Y представлено множеством сигнатур ∂, соответствующим количеству угроз: $\partial = \{\partial_1, \partial_2, \dots \partial_m\}$ – множество известных сигнатур угроз компонентов технического средства A

$$\vartheta_n(\partial) = \frac{\beta_n}{\partial}, \tag{10}$$

где $\beta_n = \theta(\rho_n, X_n, H_n, t)$ – сигнатура тестируемого *n*-го компонента технического средства A, полученная посредством функции θ; ρ_n – тестовый набор внешних воздействий для проверки *n*-го компонента технического средства A; X_n – множество внешних воздействий на *n*-й компонент; φ – множества фиксируемых (так как интересуют наблюдаемые характеристики) откликов от *n*-го компонента, представленных множеством B на интервале ξ; H_n – множество внутренних параметров *n*-го компонента; t – время воздействия.

Причём, если не доступен набор характеристик $\{X_n, \varphi, t\}$ то получим сигнатуру тестирования по принципу «чёрного ящика».

Если доступен набор характеристик $\{X_n, \varphi, t\}$, а связанные внутренние характеристики H_n не известны, но могут быть получены из множества выходных характеристик компонента $\vec{\sigma}_{An}(t)$ на том же промежутке времени, то получим сигнатуру тестирования по принципу «серого ящика»

$$\vartheta_n(\partial) = \frac{\beta_n}{\partial} \Rightarrow$$

$$\begin{cases} \beta_n \in \partial \rightarrow \vartheta_n(\partial) = 1 \text{ – наличие угрозы;} \\ \beta_n \notin \partial \rightarrow \vartheta_n(\partial) = 0 \text{ – отсутствие угрозы;} \\ \mathrm{B} = \{\beta_{n1}, \beta_{n2}, \dots \beta_{nk}\}, \mathrm{D} = \{\partial_{l1}, \partial_{l2}, \dots \partial_{lm}\} \Rightarrow B \subseteq D \rightarrow \vartheta_n(\partial) =]0,1[\text{ –} \\ \text{возможное наличие угрозы с вероятностью } P(\vartheta_n(\partial)). \end{cases} \tag{11}$$

Таким образом, если угроза отсутствует, значение целевой функции определяется как $f\left(Q_{A_n}(t)\right) = 1$; если угроза существует, значение целевой функции определяется как $f\left(Q_{A_n}(t)\right) = 0$.

В том случае, когда отношение сигнатуры *n*-го образца на тестовом массиве имеет совпадение на отдельных участках с сигнатурой *j*-й угрозы из массива сигнатур угроз, то вычисляется значение вероятности наличия угрозы в техническом средстве A в соответствии с математическим аппаратом целевой функции, ее значение находится в пределах]0,1[.

Использование описанного математического аппарата целесообразно перед процедурами разрушающего контроля для определения множества тех аппаратных закладок, сигнатуры которых будут выявлены [12]. То же относится и к сигнатурам программных закладок.

Заключение

Разработанный метод косвенных признаков позволяет выявить наличие или вероятность наличия информационной угрозы в СБИС или РЭА, использующей данную СБИС, и оценить их информационную безопасность при создании как коммуникационного оборудования – основы создания локальных и глобальных сетей передачи данных, так и образцов вычислительной техники, являющихся основой вычислительных кластеров, серверов обработки и хранения данных в центрах обработки данных производств и отраслей промышленности.

Разработанный математический аппарат может быть положен в основу аппаратно-программных средств контроля информационной безопасности образцов РЭА двойного назначения.

СПИСОК ЛИТЕРАТУРЫ:

1. Утечка 20% коммерческой информации в 60% приводит к банкротству фирмы. URL: https://www.securitylab.ru/news/214346.php (дата обращения: 26.04.2022).
2. Петров С.В. Информационная безопасность: учебное пособие. Петров С.В., Кисляков П.А. Саратов: Ай Пи Ар Букс, 2015. – 326 с. ISBN 978-5-906-17271-6. URL: https://www.iprbookshop.ru/33857.html (дата обращения: 26.04.2022).
3. Разработка промышленной технологии создания аппаратно-программного комплекса оценки соответствия активной элементной компонентной базы первичного уровня требованиям безопасности информации», ОКР «Дамба». Научно-технический отчёт, главный конструктор ОКР Чуприков А.А. 2016. – 174 с. URL: https://zakgo.ru/view/2198203 (дата обращения: 26.04.2022).
4. Балыбин С.В., Белов Е.Н., Федорец. В.Н. Проблемы информационной безопасности военной техники, использующей интегральные схемы иностранного производства. 2011, № 12, с. 11–21. URL: https://www.elibrary.ru/item.asp?id=17452281 (дата обращения: 26.04.2022).
5. Белов Е.Н., Пономарев А.А., Семенов А.В., Федорец В.Н. Угрозы информационной безопасности вооружения и военной специальной техники, укомплектованных электронной компонентной базой иностранного производства. 2013, № 12, с. 35–43. URL: https://www.elibrary.ru/item.asp?id=21004772 (дата обращения: 26.04.2022).
6. Наливкин И.В. Отечественная электроника для телекоммуникаций: реалии и перспективы. Электросвязь. 2010, № 4, с. 18–22. URL: https://elibrary.ru/item.asp?id=15177587 (дата обращения: 26.04.2022).
7. Jin, Y., Kupp, N. & Makris, Y. Experiences in hardware trojan design and implementation, in Hardware-Oriented Security and Trust, 2009. HOST ’09. IEEE Inter- national Workshop on, p. 50–57. URL:https://www.eecs.ucf.edu/~jinyier/courses/EEE4932/lab1_AES/source/Experiences%20in%20Hardware%20Trojan%20Design%20and%20Implementation.pdf (дата обращения 14.05.2022).
8. Defense Science Board Task Force On HIGH PERFORMANCE MICROCHIP SUPPLY, Office of the Under Secretary of Defense For Acquisition, Technology, and Logistics Washington, D.C. 20301-3140, February 2005. URL: https://zadereyko.info/downloads/2005-02-HPMS_Report_Final?ysclid=l363w77ea5 (дата обращения: 14.05.2022).
9. Семенов А.В., Новиков В.А., Ломако А.Г. Костюк А.В. Выявление аппаратных угроз кибербезопасности. Труды Института системного анализа РАН. Методы обеспечения информационной кибербезопасности, т. 27 (дополнительный выпуск). Под. ред. д-ра тех. наук. А.Г. Ломако. М.: КомКнига. 2013, с. 168–182.
10. The 2017 Symposium On Cybersecurity Of The Digital Economy (CDE'17) Book of Abstracts. 2017 Издательство: Издательский Дом «Afina» (Санкт-Петербург). URL: https://elibrary.ru/item.asp?id=35637281& (дата обращения: 14.05.2022).
11. Рао С.Р. Линейные статистические методы и их применения. Наука.: М. 1968. – 548 с.
12. Swarup Bhunia and Kaushik Roy. Dynamic Supply Current Testing for Analog Circuits Using Wavelet Transform. URL: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.118.2280&rep=rep1&type=pdf (дата обращения: 14.05.2022).

REFERENCES:

[1] Leakage of 20% of commercial information in 60% leads to the bankruptcy of the company. URL: https://www.securitylab.ru/news/214346.php (accessed: 26.04.2022) (in Russian).

[2] Petrov S.V. Information security: a textbook. Petrov S.V., Kislyakov P.A. Saratov: AI Pi Ar Books, 2015. – 326 p. ISBN 978-5-906-17271-6. URL: https://www.iprbookshop.ru/33857.html (accessed: 26.04.2022) (in Russian).

[3] Development of industrial technology for the creation of a hardware and software complex for assessing the compliance of the active element component base of the primary level with information security requirements, OKR "Damba". Scientific and technical report, chief designer of the OCD Chuprinov A.A. 2016. – 174 p. URL: https://zakgo.ru/view/2198203 (дата обращения: 26.04.2022) (in Russian).

[4] Balybin S.V., Belov E.N., Fedorets V.N. Problems of information security of military equipment using integrated circuits of foreign manufacture. 2011, no. 12, p. 11–21. URL: https://www.elibrary.ru/item.asp?id=17452281 (accessed: 26.04.2022) (in Russian).

[5] Belov E.N., Ponomarev A.A., Semenov A.V., Fedorets V.N. Threats to the information security of weapons and military special equipment equipped with an electronic component base of foreign production. 2013, no. 12, p. 35–43. URL: https://www.elibrary.ru/item.asp?id=21004772 (accessed: 26.04.2022) (in Russian).

[6] Nalivkin I.V. Domestic electronics for telecommunications: realities and prospects. Telecommunication. 2010, no. 4, p. 18–22. URL: https://elibrary.ru/item.asp?id=15177587 (accessed: 26.04.2022) (in Russian).

[7] Jin Y., Kupp N. & Makris Y. Experiences in hardware trojan design and implementation, in Hardware-Oriented Security and Trust, 2009. HOST '09. IEEE Inter- national Workshop on, p. 50–57. https://www.eecs.ucf.edu/~jinyier/courses/EEE4932/lab1_AES/source/Experiences%20in%20Hardware%20Trojan%20Design%20and%20Implementation.pdf (accessed: 14.05.2022).

[8] Defense Science Board Task Force On HIGH PERFORMANCE MICROCHIP SUPPLY, Office of the Under Secretary of Defense For Acquisition, Technology, and Logistics Washington, D.C. 20301-3140, February 2005. URL: https://zadereyko.info/downloads/2005-02-HPMS_Report_Final?ysclid=l363w77ea5 (accessed: 14.05.2022).

[9] Semenov A.V., Novikov V.A., Lomako A.G. Kostyuk A.V. Identification of hardware threats to cybersecurity. Proceedings of the Institute of System Analysis of the Russian Academy of Sciences, Methods of ensuring information cybersecurity, vol. 27 (additional issue). Edited by Dr. of Technical Sciences. A.G. Lomako. M.: KomKniga. 2013, p. 168–182.

[10] The 2017 Symposium On Cybersecurity Of The Digital Economy (CDE'17) Book of Abstracts. 2017 Publishing house: "Afina" (St. Petersburg). URL: https://elibrary.ru/item.asp?id=35637281& (accessed: 14.05.2022) (in Russian).

[11] Rao S.R. Linear statistical methods and their applications. Nauka: M. 1968. – 548 p. (in Russian).

[12] Swarup Bhunia and Kaushik Roy. Dynamic Supply Current Testing for Analog Circuits Using Wavelet Transform. URL: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.118.2280&rep=rep1&type=pdf (accessed: 14.05.2022).

Поступила в редакцию – 2 декабря 2021 г. Окончательный вариант – 16 Мая 2022 г.
Received – December 02, 2021. The final version – May 16, 2022.