Дмитрий О. Смирнов
Наноцентр МИРЭА,
5-я улица Соколиной горы, 22, Москва, 105118, Россия
e-mail: space_dim@rambler.ru, https://orcid.org/0000-0001-5388-7547

ФУНКЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ И НЕДОВЕРЕННАЯ ЭЛЕКТРОННАЯ КОМПОНЕНТНАЯ БАЗА*

DOI: http://dx.doi.org/10.26583/bit.2022.2.10

Аннотация. В условиях технологической зависимости отказаться от применения недоверенных изделий электронной компонентной базы (ЭКБ) невозможно, а в ряде случаев нецелесообразно. Существующие технологии допускают внесение конструктивно-технологических изменений (КТИ), которые могут нести скрытые угрозы. Рассмотрено применение терминов «функциональная безопасность» (ФБ) и «информационная безопасность». Отмечено, что термины трактуются в нормативной документации неоднозначно и нуждаются в корректировке. Проведен анализ существующей нормативной базы обеспечения ФБ критически важных объектов (КВО) в условиях технологической зависимости от изделий ЭКБ иностранного производства. Установлено, что существующие требования ФБ ограничиваются требованиями к отказоустойчивости изделий ЭКБ. Отмечено, что документы международного и национального уровня, законодательной и нормативной баз не учитывают влияние на ФБ КВО угроз, обусловленных применением недоверенной ЭКБ. Выявлено отставание нормативной документации от требований документов, определяющих стратегию кибербезопасности национального уровня и законодательной базы в современных условиях. Отмечена необходимость предъявления требований к информационной безопасности изделий ЭКБ на функциональном уровне КВО. Разработаны предложения по совершенствованию нормативной базы с целью учета угроз, обусловленных применением недоверенной ЭКБ. Сделано заключение о необходимости закрепления в нормативно-технической документации требований к выявлению КТИ в изделиях недоверенной ЭКБ и внесения соответствующих изменений в документы, определяющие стратегию кибербезопасности национального уровня, законодательной и нормативной баз в области кибербезопасности КВО.

Ключевые слова: функциональная безопасность, информационная безопасность, кибербезопасность, недоверенная электронная компонентная база, критически важный объект, конструктивно-технологические изменения, нормативная база, угроза.

Для цитирования: СМИРНОВ, Дмитрий О. ФУНКЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ И НЕДОВЕРЕННАЯ ЭЛЕКТРОННАЯ КОМПОНЕНТНАЯ БАЗА. Безопасность информационных технологий, [S.l.], т. 29, № 2, с. 128–143, 2022. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1423. DOI: http://dx.doi.org/10.26583/bit.2022.2.10.

***Благодарности.** Автор выражает благодарность и свою признательность директору наноцентра МИРЭА кандидату технических наук Беспалову А.В. за высказанные редакционные предложения.*

Dmitry O. Smirnov
MIREA Nanocenter,
5th street of Sokolinaya Gora, 22, Moscow, 105118, Russia
space_dim@rambler.ru, https://orcid.org/0000-0001-5388-7547

Functional Security and an Untrusted Electronic Component Base*

DOI: http://dx.doi.org/10.26583/bit.2022.2.10

Abstract. In the presence of technological dependence, it is impossible to abandon the use of untrusted electronic component base products, and in some cases it is impractical. Existing technologies allow for structural and technological modifications that may carry hidden threats. It is noted that the terms "functional security" and "information security" are interpreted ambiguously in the regulatory documentation and need to be corrected. The analysis of the existing regulatory framework for the

provision of critical facilities in terms of technological dependence on foreign-made untrusted electronic components is carried out. It is established that the existing requirements of the functional security are limited by the requirements for fault tolerance of electronic components. The documents of the international and national level, legislative and regulatory frameworks do not take into account the impact on the functional security of the critical facilities of threats caused by the use of an untrusted electronic components is noted. The lag between the regulatory documentation and the requirements of the documents defining the cybersecurity strategy at the national level and the legislative framework in modern conditions has been revealed. The necessity of presenting requirements for the information security of electron components at the functional level of the critical facilities is noted. Proposals have been developed to improve the regulatory framework in order to take into account the threats caused by the use of untrusted electronic components. Was made a conclusion about the need to consolidate in the regulatory and technical documentation the requirements for the identification of structural and technological modifications in products of untrusted electronic components and to make appropriate changes to the documents defining the national-level cybersecurity strategy, legislative and regulatory frameworks in the field of cybersecurity of the critical facilities.

Keywords: functional security, information security, cybersecurity, untrusted electronic components, critical object, structural and technological modifications, regulatory framework, threat.

For citation: SMIRNOV, Dmitry O. Functional Security and an Untrusted Electronic Component Base. IT Security (Russia), [S.l.], v. 29, no. 2, p. 128–143, 2022. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1423. DOI: http://dx.doi.org/10.26583/bit.2022.2.10.

***Acknowledgement.** The author expresses his gratitude and appreciation to the director of the MIREA Nanocenter, Candidate of Technical Sciences Alexey V. Bespalov for the editorial suggestions made.*

Введение

Одной из важнейших задач в обеспечении функциональной безопасности (ФБ) критически важных объектов (КВО) является преодоление технологической зависимости от изделий электронной компонентной базы (ЭКБ) иностранного производства (ИП). Одномоментно отказаться от использования изделий ЭКБ, произведенных недоверенными производителями, невозможно, а в ряде случаев и нецелесообразно.

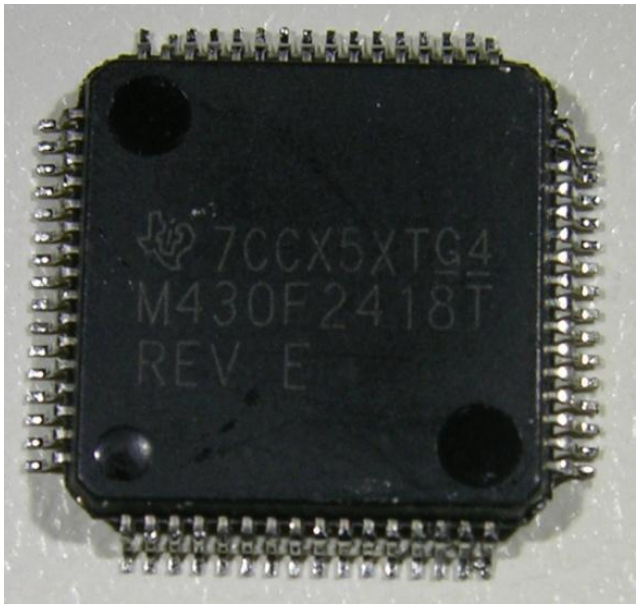
Существующие технологии производства допускают внесение конструктивно-технологических изменений (КТИ) в конструкцию изделий ЭКБ без ведома разработчика [1]. Внесенные КТИ могут нести угрозу функциональной безопасности технического средства, в котором будет использовано модифицированное изделие ЭКБ.

Классическим примером возможности внедрения вредоносного аппаратного фрагмента путем изменения топологии микроэлектронного устройства стал так называемый Illinois Malicious Processor (IMP). В разработанный процессор был добавлен дополнительный фрагмент, который позволил провести атаку типа login backdoor, позволяющую нарушителю полный доступ к машине. Для реализации угрозы потребовался 1 341 дополнительный вентиль, причем с помощью этих дополнительных вентилей могли быть организованы и другие атаки [2].

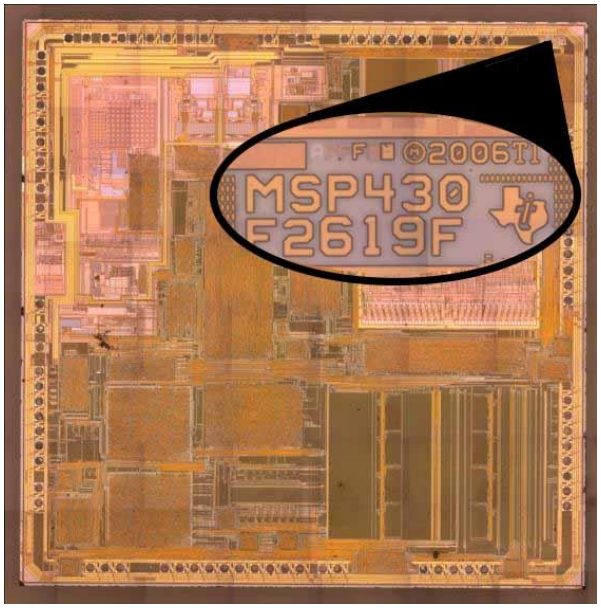
Еще один пример – интегральная микросхема (ИМС) MSP430F2418, в корпусе которой автор обнаружил кристалл более высокого уровня MSP430F2619 (рис. 1).

Технические средства с установленными ИМС MSP430F2418 подвергались различного рода испытаниям, по результатам которых были допущены к серийному производству. Подмена кристалла ИМС сделала результаты испытаний ложными, а оценку ФБ неверной.

Одной из особенностей применения изделий ЭКБ является то, что недоверенное изделие ЭКБ вовсе не обязательно должно быть установлено на фабрике при изготовлении устройства. Большу́ю угрозу могут представлять ремонтные организации и субподрядчики, выступающие в качестве посредника при закупках оборудования.



Внешний вид ИМС MSP430F2418
Case appearance



Отличие в маркировке
The difference in labeling

Рис. 1. ИМС MSP430F2418 до и после декапсуляции
Fig. 1. IC MSP430F2418 before and after decapsulation

Нарушитель, внедрившийся в такую организацию, знает назначение закупаемой техники и, в то же время, имеет возможность незаметно подменить здоровые чипы зараженными. Или, к примеру, перепрограммировать микрокод программируемых ИМС[1].

Приведенные примеры иллюстрируют наличие потенциальных угроз, и доказывают необходимость комплексного подхода к решению задачи обеспечения ФБ в части применения недоверенных изделий ЭКБ.

Существующая нормативная база, по ряду причин, в должной мере не учитывает опасность применения изделий ЭКБ, произведенных в условиях недоверенных производств, и нуждается в адаптации к современным условиям.

1. Функциональная безопасность

Термин «функциональная безопасность» в различных источниках определяется по-разному.

ГОСТ Р МЭК 61511-1-2018 содержит следующее определение: функциональная безопасность: Часть общей безопасности процесса и основной системы управления процессом, которая зависит от правильного функционирования приборной системы безопасности и других слоев защиты.

ГОСТ Р МЭК 61508-4-2012[2] определяет функциональную безопасность (functional safety), как часть общей безопасности, обусловленную применением управляемого оборудования (УО) и системы управления УО, и зависящая от правильности функционирования состоящих из электрических и/или электронных, и/или

[1]В ожидании троянского дракона. URL: https://kiwibyrd.org/2013/09/20/804/ (дата обращения: 16.05.2022).
[2]ГОСТ Р МЭК 61508-4-2012 Национальный Стандарт Российской Федерации. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Термины и определения.

программируемых электронных (Э/Э/ПЭ) систем, связанных с безопасностью и других средств по снижению риска.

ГОСТ Р МЭК 62061-2015[3] использует модифицированное определение МЭК 61508-4-2012 (п. 3.1.12): функциональная безопасность (functional safety): Часть безопасности машины и системы управления машины, которая зависит от корректного функционирования связанные с безопасностью электрические системы управления, систем, связанных с безопасностью, основанных на других технологиях и внешних средствах снижения риска.

ГОСТ Р ИСО 26262-1-2020[4] дает определение функциональной безопасности, как отсутствию неоправданного риска вследствие опасностей, вызванных отклонением от предписанного функционирования электрических и/или электронных (Э/Э) систем. При этом считается, что Э/Э система включает программируемые электронные элементы.

Наличие различных определений одного и того же термина свидетельствует о его неоднозначности, зависимости от контекста, и требует конкретизации или изменения глубины классификации в зависимости от области применения[5].

В свете вышеизложенного примером корректного определения может служить значение термина «функциональная безопасность» в отношении системы управления и обеспечения безопасности движения поездов, приведенное в ГОСТ 33358-2015[6]: Функциональная безопасность (системы управления и обеспечения безопасности движения поездов): Способность системы управления и обеспечения безопасности движения поездов выполнять требуемые функции безопасности при всех предусмотренных условиях эксплуатации в течение заданного периода времени.

В [3] отмечено, что функциональная безопасность – это часть безопасности, которая обеспечивает уверенность в том, что система выполнит стоящую перед ней соответствующую задачу, когда это потребуется.

Анализ приведенных выше определений позволяет заметить, что функциональная безопасность в настоящее время используется в качестве свойства, характеризующего систему.

Существует множество определений понятия «система»[7]. Примем определение термина, приведенное в п. 4.1.44 ГОСТ Р 57193-2016[8], как установленное в качестве общей основы для описаний процессов и применяемое в отношении жизненного цикла систем, созданных человеком. Под системой в дальнейшем будем понимать комбинацию взаимодействующих элементов, организованных для достижения одной или нескольких поставленных целей. В стандарте имеется примечание, разъясняющее, что интерпретация термина «система» зачастую уточняется с помощью ассоциативного существительного, например: система самолета. Такой подход позволяет определять элементы системы, которые сами могут являться системами.

---

[3]ГОСТ Р МЭК 62061-2015 Группа Т51. Национальный стандарт Российской Федерации. Безопасность оборудования Функциональная безопасность систем управления электрических, электронных и программируемых электронных, связанных с безопасностью.

[4]ГОСТ Р ИСО 26262-1-2020 Дорожные транспортные средства. Функциональная безопасность. Часть 1. Термины и определения.

[5]ПР 50.1.024-2005 Группа Т54. Правила стандартизации. Основные положения и порядок проведения работ по разработке, ведению и применению общероссийских классификаторов. ОКС 01.140.30.

[6]ГОСТ 33358-2015 Межгосударственный стандарт. Безопасность функциональная. Системы управления и обеспечения безопасности движения поездов. Термины и определения.

[7]Определения системы. URL: https://systems-analysis.ru/system_def.html? (дата обращения: 16.05.2022).

[8]ГОСТ Р 57193-2016 Национальный стандарт Российской Федерации. Системная и программная инженерия. Процессы жизненного цикла систем.

Действующий ГОСТ 12.0.002-2014[9] определяет термин «безопасность», с одной стороны, как состояние объекта или процесса, при котором отсутствует недопустимый риск, связанный с возможностью причинения вреда, с другой, как обеспечение состояния объекта или процесса, при котором отсутствует недопустимый риск, связанный с возможностью причинения вреда. В примечании указывается, что это многозначный термин, смысл которого зачастую окончательно ясен только из контекста, и что большинство русскоязычных законодательных документов определяют «безопасность» формально, как состояние защищенности от угроз. Там же указано, что безопасность может рассматриваться в аспектах социальном, что соответствует англоязычному понятию «security», и техническом, соответствующем понятию «safety», предусматривающем защиту человека от травм, а имущественного комплекса производства – от аварий. Отдельные авторы[10] англоязычное понятие «security» трактуют в техническом смысле, как информационную безопасность, что, скорее всего, допустимо. В дальнейшем, используя термин «безопасность», будем иметь в виду технический аспект этого термина, а в качестве критерия – отсутствие недопустимого риска, связанного с возможностью причинения вреда человеку и/или имущественному комплексу.

Причиненный вред можно оценить, используя стандартизованное понятие «ущерб»[11].

Обобщение вышеизложенного, позволяет определить функциональную безопасность, как *свойство системы, заключающееся в том, что риск ущерба при ее функционировании не превысит допустимого*.

Формально можно описать это определение следующим выражением:

$$R(F_{\text{Сист}}) = P_{\text{Ущ}}(F_{\text{Сист}}) \times V_{\text{Ущ}}(F_{\text{Сист}}) \leq R_{\text{Доп}}(F_{\text{Сист}}),$$

где:

$F_{\text{Сист}}$ – функция (или множество функций), выполняемая системой;

$R(F_{\text{Сист}})$ – риск ущерба при функционировании системы;

$P_{\text{Ущ}}(F_{\text{Сист}})$ – вероятность возникновения ущерба при функционировании системы;

$V_{\text{Ущ}}(F_{\text{Сист}})$– размер ущерба при функционировании системы;

$R_{\text{Доп}}(F_{\text{Сист}})$ – допустимый риск при функционировании системы.

Введенное определение является универсальным для систем и допускает декомпозицию ФБ системы на составные части, позволяющие учитывать свойства системы, значимые для оценки риска ущерба.

Требования к ФБ должны задаваться в техническом задании на разработку системы, а их выполнение – подтверждаться результатами соответствующих испытаний.

2. Информационная безопасность

На практике термины безопасность информации[12] (БИ) и информационная безопасность используют не всегда корректно.

[9]ГОСТ 12.0.002-2014 Межгосударственный стандарт. Система стандартов безопасности труда. Термины и определения.

[10]Функциональная безопасность – старшая сестра информационной безопасности. URL: https://habr.com/ru/post/308634/ (дата обращения: 16.05.2022).

[11]ГОСТ Р 22.10.01-2021 Национальный стандарт Российской Федерации. Безопасность в чрезвычайных ситуациях. ОЦЕНКА УЩЕРБА. Термины и определения.

[12]ГОСТ Р 50922-2006 Группа Э00. Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения.

Так, ГОСТ Р ИСО/МЭК 27000-2021[13] определяет информационную безопасность, как сохранение конфиденциальности, целостности и доступности информации, что аналогично понятию «безопасность информации».

ГОСТ Р 53113.1-2008[14] трактует понятие информационная безопасность следующим образом. **Информационная безопасность** (information security): Все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации или средств ее обработки.

В разделе Общие положения Основ государственной политики Российской Федерации в области международной информационной безопасности[15] под международной информационной безопасностью понимается такое состояние глобального информационного пространства, при котором, в том числе, исключены возможности деструктивного и противоправного воздействия на элементы национальной критической информационной инфраструктуры (КИИ).

Указ Президента РФ[16] отмечает растущее число преступлений, совершаемых с использованием информационно-коммуникационных технологий, ставит задачу предупреждения и пресечения правонарушений и преступлений, совершаемых с использованием информационно-коммуникационных технологий. Вопросам ИБ посвящен одноименный раздел этого документа. В п. 51 прямо указывается, что Вооруженные силы иностранных государств отрабатывают действия по *выведению из строя* объектов критической информационной инфраструктуры Российской Федерации. Далее, в п. 57, указывается, что достижение цели обеспечения ИБ осуществляется путем реализации государственной политики, направленной на решение задач, в числе которых приводятся:

– развитие системы прогнозирования, выявления и предупреждения угроз ИБ Российской Федерации, определения их источников, оперативной ликвидации последствий реализации таких угроз;

– предотвращение деструктивного информационно-технического воздействия на российские информационные ресурсы, включая объекты КИИ Российской Федерации;

– совершенствование средств и методов обеспечения ИБ на основе применения передовых технологий, включая технологии искусственного интеллекта и квантовые вычисления;

– обеспечение приоритетного использования в информационной инфраструктуре Российской Федерации российских информационных технологий и оборудования, отвечающих требованиям ИБ.

Последние два документа трактуют понятие ИБ значительно шире, учитывая возможность оказания деструктивного информационного воздействия на КИИ Российской Федерации, тем самым признавая, что ущерб при реализации угрозы ИБ может быть нанесен не только безопасности информации, но и элементам КИИ, нарушая их нормальное функционирование. Но нарушение нормального функционирования, при

[13]ГОСТ Р ИСО/МЭК 27000-2021 Национальный стандарт Российской Федерации. Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология.

[14]ГОСТ Р 53113.1-2008 Группа Т00. Национальный стандарт Российской Федерации. Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения.

[15]«Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года» (утв. Президентом РФ 24.07.2013 N Пр-1753).

[16]Указ Президента РФ от 2 июля 2021 г. N 400 «О Стратегии национальной безопасности Российской Федерации».

котором возрастает риск ущерба, является нарушением ФБ. Следовательно, *ИБ является составной частью ФБ, а нарушение безопасности информации в этом случае должно рассматриваться как частный случай нарушения функциональной безопасности, результатом которого будет ущерб вследствие нарушения конфиденциальности, целостности или доступности защищаемой информации*.

На практике зачастую ИБ технического средства при использовании в его составе ЭКБ ИП определяется как состояние защищенности технического средства от повреждения, отказа или нарушения его функционирования в результате несанкционированного воздействия через изделия ЭКБ ИП. Очевидно, что смысл понятия «информационная безопасность» в этом случае соответствует сути Приказа ФСТЭК России от 14.03.2014 № 31.

Известны прецеденты, свидетельствующие о существовании проблемы нештатного функционирования АСУ технологическими процессами (АСУ ТП) – подрыв участка самой протяженной газовой магистрали СССР Уренгой-Сургут-Челябинск в 1982 г. [4], червь Stux-net[17], червь Shamoon[18], взлом серверов и кража информации OaSyS SCADA Telvent (Schneider Electric).[19] Во всех перечисленных случаях инциденты нарушения функциональной безопасности являлись результатом перевода оборудования АСУ ТП в нештатный режим работы в результате компьютерных атак. При этом только взлом серверов и кража информации явились инцидентом информационной безопасности, остальные – инцидентами нарушения безопасности функциональной.

3. Анализ требований нормативных документов

Критическая информационная инфраструктура Российской Федерации представляет совокупность автоматизированных систем управления (АСУ) критически важных объектов (КВО) и обеспечивающих их взаимодействие информационно-телекоммуникационных сетей, предназначенных для решения задач государственного управления, обеспечения обороноспособности, безопасности и правопорядка, нарушение (или прекращение) функционирования которых может стать причиной наступления тяжких последствий[20]. Безопасность АСУ КВО определяется, как состояние, при котором обеспечивается соблюдение проектных пределов значений параметров выполнения ею целевых функций (штатный режим функционирования) при проведении в отношении ее компьютерных атак.

«Основные направления научных исследований в области обеспечения информационной безопасности Российской Федерации»[21] определяют ряд проблем, непосредственно касающихся информационной безопасности. Одной из первых отмечена

[17]Rootkit.Win32.Stuxnet.a, ЗАО «Лаборатория Касперского». URL:https://web.archive.org/web/20110128191738/http://www.securelist.com/ru/descriptions/15071647/Rootkit.Win32.Stuxnet.a (дата обращения: 24.03.2022).

[18]Shamoon – что это было?, авт. nuklearlord, URL: https://habr.com/ru/post/159049/ (дата обращения: 16.05.2022).

[19]Kim Zetter, Security 09.26.2012 03:56 PM, Maker of Smart-Grid Control Software Hacked. URL: https://www.wired.com/2012/09/scada-vendor-telvent-hacked/ (дата обращения: 16.05.2022).

[20]Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации Утверждены Президентом Российской Федерации Д. Медведевым 3 февраля 2012 г. № 803.

[21]«Основные направления научных исследований в области обеспечения информационной безопасности Российской Федерации» (утв. Секретарем Совета Безопасности Российской Федерации Н.П. Патрушевым 31 августа 2017 г.), выписка. URL: http://www.scrf.gov.ru/security/information/document155/ (дата обращения: 16.05.2022).

проблема формирования понятийного (терминологического) аппарата в области информационной безопасности. В числе научно-технических проблем обеспечения информационной безопасности упомянута проблема обеспечения технологической независимости России в области создания и использования отечественной электронной компонентой базы и микропрограммного обеспечения, доверенных информационных технологий, вычислительной техники, телекоммуникации и связи. Отдельно выделена проблема предотвращения возможности включения в информационные технологии скрытых вредоносных функций, снижения опасности их применения. Отмечена проблема совершенствования кадрового обеспечения в области информационной безопасности Российской Федерации, что свидетельствует о комплексном подходе к решению задачи обеспечения информационной безопасности в целом.

Федеральными органами исполнительной власти (ФОИВ), курирующими вопросы информационной безопасности в пределах своих полномочий, в России определены:

1. Федеральная служба технического и экспортного контроля. Участвует в пределах своей компетенции в разработке и реализации мероприятий по обеспечению информационной безопасности Российской Федерации[22].
2. Федеральная служба безопасности[23], что закреплено в Положении о Федеральной службе безопасности.[24]
3. Министерство обороны. Организует деятельность по обеспечению информационной безопасности в Вооруженных Силах[25].
4. Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации. Наделено правом самостоятельно принимать требования к информационной безопасности информационных систем, в том числе информационных систем персональных данных (за исключением информационных систем критически важных объектов), информационно-телекоммуникационных сетей и других сетей связи[26].

Такое количество ФОИВ, отвечающих за информационную безопасность в рамках своих полномочий, предполагает координации взаимодействия в рамках межведомственных комиссий при принятии концептуальных решений, к которым относится решение о включении ИБ в состав безопасности функциональной.

Анализ документов, определяющих стратегию национальной кибербезопасности международного[27] и национального уровня, законодательной и нормативной баз, применяемых в области кибербезопасности КВО, показывает, что существующие меры по

[22]«Положение о Федеральной службе по техническому и экспортному контролю» (утв. Указом Президента Российской Федерации от 16 августа 2004 г. N 1085). URL: https://fstec.ru/normotvorcheskaya/eksportnyj-kontrol/98-ukazy/219-ukaz-prezidenta-rossijskoj-federatsii-ot-16-avgusta-2004-g-n-1085? (дата обращения: 16.05.2022).

[23]Федеральный Закон О федеральной службе безопасности*(с изменениями на 1 июля 2021 года). URL: https://docs.cntd.ru/document/9011123 (дата обращения: 16.05.2022).

[24]Положение о Федеральной службе безопасности Российской Федерации (утв. Указом Президента РФ от 11 августа 2003 г. N 960). URL: https://base.garant.ru/12132066/? (дата обращения: 16.05.2022).

[25]Положение о Министерстве обороны Российской Федерации (с изменениями на 4 мая 2022 года) (утв. Указом Президента Российской Федерации от 16 августа 2004 года N 1082). URL: https://docs.cntd.ru/document/901905920?marker=65E0IS (дата обращения: 16.05.2022).

[26]Постановление Правительства Российской Федерации от 2 июня 2008 года N 418 «О Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации» (с изменениями на 17 декабря 2021 года) (редакция, действующая с 1 января 2022 года). URL: https://docs.cntd.ru/document/902103611 (дата обращения: 16.05.2022).

[27]Руководство по разработке национальной стратегии кибербезопасности. Стратегическая деятельность по обеспечению кибербезопасности. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-R.pdf (дата обращения: 16.05.2022).

защите технических средств направлены, в основном, на противодействие террористическим угрозам, программным воздействиям, хищениям денежных средств.

На обеспечение штатного функционирования критически важных объектов, потенциально опасных объектов, а также объектов, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, направлен приказ ФСТЭК России от 14.03.2014 г № 31[28]. Он устанавливает требования к обеспечению защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также иных неправомерных действий в отношении такой информации, в том числе от деструктивных информационных воздействий (компьютерных атак), следствием которых может стать нарушение функционирования АСУ. При этом устанавливаются организационные, нормативные и методические ограничения на использование АСУ ТП и их компонентов. Меры по защите технических средств сводятся к исключению несанкционированного доступа к стационарным техническим средствам, обрабатывающим информацию, исполнительным устройствам, и в помещения, в которых они постоянно расположены, обеспечению защиты технических средств от внешних воздействий, а также защите информации, представленной в виде информативных электрических сигналов и физических полей. По отношению к ПО указанный документ требует обеспечивать выявление, анализ и устранение разработчиком уязвимостей ПО АСУ, определенного заказчиком, на всех этапах жизненного цикла, а также контроль принимаемых мер по выявлению, анализу и устранению уязвимостей со стороны заказчика и (или) оператора АСУ. Состав мер защиты информации, приведенный в документе, не предусматривает выявления уязвимостей или наличия опасных КТИ в аппаратной составляющей АСУ ТП.

Проанализируем требования стандартов группы ФБ в части обеспечения аппаратной составляющей безопасности.

Стандарт ГОСТ Р МЭК 61131-6-2015 на изделие, являющееся программируемым логическим контроллером, удовлетворяющим требованиям функциональной безопасности[29] (ПЛК-ФБ), положения которого должны применять к области программируемых контроллеров и связанных с ними периферийных устройств устанавливает методы оценки для множества параметров/критериев ПЛК-ФБ. Аппаратная составляющая ФБ учитывается только в части отказоустойчивости.

Стандарт ГОСТ Р МЭК 61508-1-2012[30] устанавливает общий подход к вопросам обеспечения безопасности для всех стадий жизненного цикла систем, состоящих из Э/Э/ПЭ элементов, которые используются для выполнения функций обеспечения безопасности. Стандарт был разработан для обеспечения охвата всего диапазона сложности, присущей таким системам и включает технические требования к разработке концепции, области применения, анализа явных опасных событий и рисков. При

[28]Приказ ФСТЭК России от 14.03.2014 № 31 (ред. от 23.03.2017) «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» (Зарегистрировано в Минюсте России 30.06.2014 N 32919).

[29]ГОСТ Р МЭК 61131-6-2015. Национальный стандарт Российской Федерации. Контроллеры программируемые. Часть 6. Безопасность функциональная.

[30]ГОСТ Р МЭК 61508-1-2012 Группа Т51. Национальный стандарт Российской Федерации. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1. Общие требования.

определении ФБ в части аппаратной составляющей учитывается только отказоустойчивость.

Стандарт ГОСТ Р МЭК 61508-2-2012[31] рассматривает все соответствующие стадии жизненных циклов всей системы безопасности, Э/Э/ПЭ системы безопасности и ПО системы безопасности (например, от первоначальной концепции, через проектирование, реализацию, эксплуатацию, техническое обслуживание вплоть до снятия с эксплуатации), в ходе которых Э/Э/ПЭ системы используются для выполнения функций безопасности.

Рассмотренные стандарты при обеспечении безопасности предусматривают только аппаратную отказоустойчивость. Методы обеспечения ФБ направлены на защиту от случайных отказов аппаратных средств, вызванных физическим старением или внутренними дефектами изделий ЭКБ, а также на защиту от систематических отказов, вызванных несовершенством конструктивных решений.

Стандарт МЭК 61508 при обеспечении полноты безопасности рассматривает только случайные и систематические отказы. В качестве случайных отказов рассматривается выход из строя аппаратных компонентов. Парируются такие отказы резервированием, самодиагностикой, физическим и электрическим разделением компонентов, повышением устойчивости к внешним воздействиям и т.п. Основной причиной систематических отказов считаются ошибки проектирования, в т.ч., ошибки ПО, ошибки эксплуатации и внешние экстремальные воздействия (климатические, механические, радиационные и другие) [5]. Устранение систематических отказов возможно путем совершенствования процессов проектирования и разработки, тестирования, управления конфигурацией и т.п. Применяется диверсное резервирование, при котором резервные каналы разрабатываются с использованием различного программного и аппаратного обеспечения. В качестве дополнительной причины отказов в [6] упоминается информационная безопасность, но рассматривается исключительно в ключе кибератак.

В стандарте ГОСТ Р МЭК 61511-1-2018[32] приводится определение полноты безопасности аппаратных средств приборных систем безопасности, которое учитывает составляющую полноты безопасности, связанную со случайными отказами аппаратных средств и не рассматривает в качестве вероятных причин отказов (сбоев) скрытые возможности аппаратных средств. Приводится обширный перечень требований к безопасности прикладного и встроенного ПО, среди которых есть требование защиты от записи в память интеллектуальных датчиков с целью предотвращения неосторожных изменений, вследствие неправильного выполнения процедур (человеческий фактор). Установлены требования к верификации прикладного ПО. Скрытые возможности аппаратных средств не упоминаются.

При определении факторов возникновения угроз БИ методика оценки угроз безопасности информации[33] ограничивается недостатками качества, надежности ПО, программно-аппаратных средств. В качестве основных способов реализации угроз

[31]ГОСТ Р МЭК 61508-2-2012. Национальный стандарт Российской Федерации. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 2. Требования к системам.

[32] ГОСТ Р МЭК 61511-1-2018. Группа Т51. Национальный Стандарт Российской Федерации. Безопасность Функциональная. Системы безопасности приборные для промышленных процессов. Часть 1. Термины, определения и технические требования.

[33]«Методика оценки угроз безопасности информации» (утв. Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г.). URL: https://www.garant.ru/products/ipo/prime/doc/400325044/? (дата обращения: 16.05.2022).

упоминается использование недекларированных возможностей ПО и/или программно-аппаратных средств.

Ни в одном из перечисленных источников не поднимаются вопросы влияния на ФБ КВО недоверенной ЭКБ.

Естественным следствием выявленного ограничения является тот факт, что существующий банк данных угроз безопасности информации[34], ведение которого осуществляет ФСТЭК России в соответствии с подпунктом 21 пункта 8 Положения о ФСТЭК России, не содержит сведений об угрозах, обусловленных применением изделий ЭКБ, произведенных недоверенными производителями.

Конечному пользователю не важна причина нарушения нормального функционирования технического средства (ТС) – важен сам факт нарушения ФБ. В этом ключе ИБ ТС должна рассматриваться, как составная часть безопасности функциональной, а требования к ИБ изделий ЭКБ должны предъявляться на функциональном уровне КВО или составной части (СЧ) КВО.

Инцидентом нарушения информационной безопасности можно считать отказ или сбой[35], вызванный воздействием на компонент ЭКБ по информационному каналу. Назовем такой отказ управляемым. Отказ компонента ЭКБ, возникающий при наступлении какого-либо события (истечение определенного времени, достижение определенного состояния, появление внешнего воздействующего фактора и т.п.), по существу является предопределенным. Внешние проявления как управляемого, так и предопределенного отказов будут аналогичны внешним проявлениям отказов, вызванных другими причинами (естественное старение, несовершенство конструкции и материалов и т.п.)[36].

Отказ или некорректную работу технического средства, вызванные применением изделий ЭКБ с опасными КТИ, нельзя отнести к случайным или систематическим отказам в силу природы их возникновения. Например, внедренная в изделие ЭКБ и сработавшая «временная бомба» будет интерпретироваться как случайный отказ. При существующем нормативно-методическом обеспечении выявление истинной причины отказа, вызванного подобной модификацией изделия ЭКБ, невозможно. В стандарте МЭК 61508 не упоминается сама возможность возникновения подобных отказов. В то же время при сертификации на соответствие требованиям МЭК 61508 необходимо доказать, с одной стороны, что используемый механизм ФБ является необходимым и достаточным, а с другой – что необходимый и достаточный набор методов применялся в процессе разработки. Без учета отказов, возникающих вследствие скрытых свойств недоверенных компонентов ЭКБ, набор методов, применяемых для разработки КВО или СЧ КВО, будет неполным.

В [7] рассмотрена оптимизация затрат на комплексное координированное обеспечение ИБ и ФБ только в том случае, когда для их обеспечения применяются одни и те же методы. При этом аспекты количественного оценивания функциональной безопасности рассматриваются, как составная часть теории надежности, в свете требований стандарта МЭК 61508 к выбору методов для защиты от отказов аппаратных и

[34]БДУ – Банк данных угроз безопасности информации. URL: https://bdu.fstec.ru/threat (дата обращения: 16.05.2022).
[35]ГОСТ Р 27.102-2021 Национальный стандарт Российской Федерации. Надежность в технике. Надежность объекта. Термины и определения.
[36]РД 50-699-90. Методические указания. Надежность в технике. Общие правила классификации отказов и предельных состояний. Государственный комитет СССР по управлению качеством продукции и стандартам. Москва 1991.

программных компонентов. Вопросы скрытых возможностей аппаратной составляющей в [7] не рассматриваются.

Длительное время усилия экспертов по безопасности были направлены на поиск уязвимостей в программной части, что вполне объяснимо, учитывая сложность и высокую стоимость исследований аппаратной составляющей. Однако даже программную закладку на уровне ИМС можно реализовать только при соответствующем аппаратном обеспечении – наличии необходимого объема памяти, вычислителя и т.п. признаков с высокой вероятностью выявляемых при проведении соответствующих тематических исследований.

Скрытое вмешательство на аппаратном уровне оказывается опасной и вполне реализуемой на практике технологией. В [1], оценивая риск внедрения в ИМС схемотехнических решений, предназначенных для реализации нерегламентированных функций, отмечено, что «спрятать» несколько тысяч транзисторов в массиве из многих миллионов – не проблема. Практически в любом современном чипе может существовать множество скрытых внутренних функций, к которым у пользователей нет прямого доступа, и о существовании которых они не подозревают.

Одинаковые изделия ЭКБ, применяемые в различных ТС, будут подвергаться различным воздействиям: температурным, радиационным, механическим и т.д. Необходимо разработать соответствующую модель угроз, учитывающую все возможные (или наиболее вероятные) факторы, воздействующие на изделия ЭКБ в составе конкретного ТС. Определить совокупность критических изделий ЭКБ в составе КВО или СЧ КВО, посредством которых могут быть реализованы угрозы. На основании модели угроз разработать программу и методики сертификационных испытаний изделий ЭКБ. Обосновать необходимость проведения процедур разрушающего контроля в отношении выбранных изделий ЭКБ, например, если существуют подозрения в отношении внесения несанкционированных КТИ при производстве, и т.п.

Учитывая, что средством нарушения ФБ зачастую служит нарушение ИБ [8], к понятию ФБ, в части ИБ, вполне применима классификация факторов, воздействующих на безопасность защищаемой информации, приведенная в ГОСТ Р 51275-2006[37]. Этот документ предусматривает опасность применения закладочных устройств (ЗУ) в целях перехвата информации или несанкционированного воздействия на информацию и/или ресурсы автоматизированной информационной системы, но рассматривает ЗУ, как отдельные технические средства (устройства) со своими «местами установки» и не учитывает возможность их размещения в изделиях ЭКБ. Применяются понятия «программная закладка», «недекларированные возможности программного обеспечения», «вредоносная программа», «компьютерный вирус», но не учитывается, что в случае размещения ПО с вредоносной программой или вирусом в памяти ИМС эти понятия автоматически становятся признаком, присущим конкретной ИМС. Стандарт не учитывает влияния потенциальных опасных элементов в изделиях ЭКБ недоверенных производителей. В то же время, многие определяемые документом факторы воздействуют на информацию опосредованно, нарушая нормальное функционирование средств обработки информации. Условия для их реализации могут быть заложены в изделия ЭКБ посредством внесения КТИ.

Совокупность критических изделий ЭКБ, подлежащих углубленному исследованию, можно определить, например, оценивая риски угроз, реализуемых посредством этих изделий, приняв в качестве критерия степень допустимого риска,

[37]ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения».

независимо от возможности конфигурирования или наличия памяти в исследуемом изделии ЭКБ. Такой подход позволит исследовать конечные автоматы, потенциальная возможность несанкционированных КТИ, которых также существует.

В том случае, если предполагается проведение разрушающего контроля, на основании модели угроз необходимо определить, какие элементы изделия ЭКБ будут подвергаться исследованию, и перечень признаков, подлежащих выявлению. Модель угроз должна разрабатываться и согласовываться с Заказчиком на этапе разработки технического предложения[38] после изучения и анализа технического задания на разработку конечного изделия. Следует принимать в расчет, что избыточное число исследуемых элементов приведет к существенному удорожанию проекта и значительным временным затратам, недостаточное – к снижению вероятности выявления искомых признаков. Существенным недостатком метода является его полная достоверность только по отношению к изделию ЭКБ, подвергнутому разрушению. Однако существуют способы, позволяющие на этапе разработки разместить в изделии ЭКБ контрольные элементы, позволяющие выявлять наличие несанкционированных изменений при помощи электрических измерений.

Так в [9] с целью контроля отсутствия изменений в конструкции ИМС предложено на этапе разработки и проектирования разместить на неиспользуемой части кристалла ИМС элементы, позволяющие контролировать степень заполнения свободного пространства. Предложенные способы контроля позволяют методом электрического тестирования провести неразрушающий контроль, применить который можно в отношении каждого компонента из всей партии проверяемых ИМС.

В [10] описан метод косвенных признаков, позволяющий оценивать вероятность возможного наличия конструктивно-технологических изменений в ИМС по результатам сигнатурного анализа.

Учитывая растущее число заказных изделий ЭКБ, предложенные подходы представляются перспективными и требуют своего закрепления в нормативной документации. Нормативные документы, в том числе, должны определять порядок, правила и периодичность проведения подобного рода исследований.

Существующая нормативная база в части обеспечения ИБ и ФБ КВО отстает от требований программных документов. Необходимы формирование и корректировка понятийного (терминологического) аппарата в области ИБ, разработка нормативного обеспечения, направленного на решение проблемы технологической независимости России в области создания и использования отечественной электронной компонентой базы и микропрограммного обеспечения, доверенных информационных технологий, вычислительной техники, телекоммуникации и связи. Развитие нормативного обеспечения должно быть, в т.ч., направлено на предотвращение возможности включения в информационные технологии скрытых вредоносных функций, снижения опасности их применения.

Важной задачей является формирование *единого понятийного аппарата*, учитывающего изменения, обусловленные спецификой ФБ.

Следует сформировать понятие «функциональная безопасность», универсальное и применимое к различным системам, а также скорректировать множество угроз ФБ, включив в него угрозы информационной безопасности и угрозы, исходящие от применения недоверенных изделий ЭКБ.

[38]ГОСТ 2.103-2013 Межгосударственный стандарт Единая система конструкторской документации. Стадии разработки.

До настоящего времени отсутствует четкое определение понятия «доверенность» в отношении ЭКБ, хотя термин «доверенная компонентная база» употребляется часто [11] и вполне применим для оценки потенциального отсутствия несанкционированных КТИ изделия ЭКБ.

Предлагается определение «доверенное изделие ЭКБ», например, в следующей редакции: **доверенное изделие ЭКБ** – изделие ЭКБ, функционирующее в полном соответствии с техническим описанием производителя.

В таком виде определение учитывает необходимые признаки и, в то же время, является непротиворечивым в отношении условий эксплуатации и способов применения изделия ЭКБ, не соответствующих установленным производителем в техническом описании. В случае отличий условий эксплуатации от определенных производителем в техническом описании, доверенность пропадает.

Учитывая направленность документа, с целью более полного учета возможных угроз предлагается расширить требования п.11.а в Приказе ФСТЭК России от 25 декабря 2017 г. № 239[39]. В частности, вместо «угроз безопасности информации» в дальнейшем рассматривать угрозы «функциональной безопасности». Аналогичные изменения предлагается внести в п. 11.1, расширив его требования до ФБ. В частности, п. 11.1.б предлагается изложить в следующей редакции: «б) анализ возможных уязвимостей значимого объекта и его программных, аппаратных и программно-аппаратных средств».

Учет требования к защите технических средств со стороны аппаратной части требует внести изменения в Приказ ФСТЭК России от 14.03.2014 № 31, предусмотрев выявление, анализ и устранение (или предотвращение) уязвимостей аппаратного обеспечения АСУ, обусловленных возможным наличием КТИ изделий ЭКБ, на всех этапах жизненного цикла[40], а также контроль принимаемых мер по их выявлению, анализу, предотвращению и устранению.

Стандарт МЭК 61508-1 предполагает возможность использования для определения любой электрической и/или электронной и/или программируемой электронной системы в случае серьезных экономических последствий, вызванных отказами, что требует внести в группу стандартов МЭК 61508 изменения, отражающие существование несанкционированных опасных КТИ аппаратных и программно-аппаратных изделий ЭКБ на различных стадиях жизненного цикла систем. Выявление наличия КТИ изделий ЭКБ, приводящих к опасным событиям, необходимо производить на стадиях установки и ввода в эксплуатацию, подтверждения соответствия всей системы безопасности и ремонта, модификации системы безопасности.

Заключение

В статье поднята проблема отсутствия учета существующими нормативными документами аппаратных угроз, обусловленных потенциальным наличием опасных КТИ в недоверенных изделиях ЭКБ. Отмечена необходимость адаптации нормативной базы к современным условиям.

Анализ требований документов, определяющих стратегию национальной кибербезопасности национального уровня и законодательной базы, выявил наличие отставания нормативной базы в части учета угроз ИБ в современных условиях. Проблемы,

[39]Приказ ФСТЭК России от 25 декабря 2017 г. № 239 (в ред. приказов ФСТЭК России от 9 августа 2018 г. №138, от 26 марта 2019 г. № 60, от 20 февраля 2020 г. № 35) « Об утверждении требований по обеспечению безопасности объектов критической информационной инфраструктуры Российской Федерации».

[40]ГОСТ Р 57193-2016 Национальный стандарт Российской Федерации. Системная и программная инженерия. Процессы жизненного цикла систем.

обозначенные в стратегических документах, до настоящего времени не нашли своего отражения в нормативных документах.

Отсутствие нормативно-методического обеспечения, учитывающего угрозы потенциальных опасных КТИ в изделиях ЭКБ, не позволяет выявлять истинные причины отказов.

Анализ и практика применения терминов «функциональная безопасность», «информационная безопасность», «доверенность» выявил необходимость корректировки терминологического аппарата с целью обеспечения однозначного их определения.

Выявление наличия КТИ в изделиях недоверенной ЭКБ должно стать одним из направлений объективного контроля ФБ, направленного на предотвращение возможности включения в информационные технологии скрытых вредоносных функций, снижения опасности их применения. Развитие этого направления определяет необходимость разработки соответствующего нормативно-методического обеспечения.

СПИСОК ЛИТЕРАТУРЫ:

1. Федорец В.Н. Перспективные технологии защиты микросхем от обратного проектирования в контексте информационной безопасности, под ред. д-ра техн. наук В.Н. Федорца / Белов Е.Н., Балыбин С.В., Пономарев А.А., Семенов А.В., Федорец В.Н., Швыдя О.В. М.: «Техносфера», 2017. – 215 с.
2. Samuel T. King, Joseph Tucek, Anthony Cozzie, Chris Grier, Weihang Jiang, and Yuanyuan Zhou, Designing and implementing malicious hardware University of Illinois at Urbana Champaign, Urbana, IL 61801. URL: https://www.usenix.org/legacy/event/leet08/tech/full_papers/king/king.pdf (дата обращения: 16.05.2022).
3. Том Мини. Функциональная безопасность и индустрия 4.0. Часть 1. Пер.: М. Русских tau68@rambler.ru, no. 1 (91), 2021 CONTROL ENGINEERING РОССИЯ. URL: https://controleng.ru/wp-content/uploads/9162.pdf?ysclid=l37pqzh8of (дата обращения: 16.05.2022).
4. Thomas C. Reed. Над бездной. История холодной войны, рассказанная её участником (At the Abyss: An Insider’s History of the Cold War). 2004. ISBN 0891418210.; «Trans-Siberian Gas Pipeline Sabotage», Devin Myler, David Calderon-Guthe. URL: https://prezi.com/zzfjkvlmpr3w/trans-siberian-pipeline-sabotage-1982/ (дата обращения: 16.05.2022).
5. Скляр В.В. Функциональная безопасность, часть 7 из 7. Методы обеспечения информационной и функциональной безопасности. URL: https://habr.com/ru/post/327910/ (дата обращения: 16.05.2022).
6. Скляр В.В. Функциональная безопасность – старшая сестра информационной безопасности, часть 1 из 7. URL: https://habr.com/ru/post/308634/? (дата обращения: 16.05.2022).
7. Скляр В.В. Обеспечение безопасности АСУТП в соответствии с современными стандартами, изд. Инфра-Инженерия, 2018. – 384 с. ISBN:978-5-9729-0230-9.
8. Безродный Б.Ф. Особенности кибербезопасности АСУ ТП на железнодорожном транспорте. Декабрь 2020 – январь 2021, www.secuteck.ru. URL: https://www.secuteck.ru/articles/osobennosti-kiberbezopasnosti-asu-tp-na-zheleznodorozhnom-transporte (дата обращения: 16.05.2022).
9. Смирнов Д.О., Безродный Б.Ф., Беспалов А.В. Интегральные микросхемы. Проблема доверенности. Ж. «Наноиндустрия». 2021, т. 14, № S7 (107), с. 340–342. URL: https://www.elibrary.ru/item.asp?id=46704489 (дата обращения: 16.05.2022).
10. 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.
11. Дорохова И., Башкиров А., А.Новодережкин. РАСУ займется микроэлектроникой. URL: https://strana-rosatom.ru/2021/06/28/rasu-zajmetsya-mikroelektronikoj/?ysclid=l2f39a8gu0 (дата обращения: 16.05.2022).

REFERENCES:

[1] Fedorets V.N. Promising technologies of protection of microcircuits from reverse engineering in the context of information security, edited by Dr. of Technical Sciences V.N. Fedorets. Belov E.N., Balybin S.V., Ponomarev A.A., Semenov A.V., Fedorets V.N., Shvydya O.V. M.: "Technosphere", 2017. – 215 p. (in Russian).
[2] Samuel T. King, Joseph Tucek, Anthony Cozzie, Chris Grier, Weihang Jiang, and Yuanyuan Zhou, Designing and implementing malicious hardware University of Illinois at Urbana Champaign, Urbana, IL 61801.

URL: https://www.usenix.org/legacy/event/leet08/tech/full_papers/king/king.pdf (дата обращения: 16.05.2022).

[3] Tom Meany. Functional Security and Industry 4.0. Part 1. Trans.: Russian.M. Russkich. tau68@rambler.ru, no. 1 (91), 2021 technical control RUSSIA. URL: https://controleng.ru/wp-content/uploads/9162.pdf?ysclid=l37pqzh8of (accessed: 16.05.2022).

[4] Thomas C. Reed. Над бездной. История холодной войны, рассказанная её участником (At the Abyss: An Insider's History of the Cold War). 2004. ISBN 0891418210.; «Trans-Siberian Gas Pipeline Sabotage», Devin Myler, David Calderon-Guthe. URL: https://prezi.com/zzfjkvlmpr3w/trans-siberian-pipeline-sabotage-1982/ (accessed: 16.05.2022).

[5] Sklyar V.V. Functional security, part 7 of 7. Methods of ensuring information and functional security. URL: https://habr.com/ru/post/327910 / (accessed: 16.05.2022) (in Russian).

[6] Sklyar V.V. Functional security – the elder sister of information security, part 1 of 7. URL: https://habr.com/ru/post/308634 /? (accessed: 16.05.2022) (in Russian).

[7] Sklyar V.V. Ensuring the safety of automated process control systems in accordance with modern standards, ed. Infra-Engineering, 2018. – 384 p. ISBN:978-5-9729-0230-9 (in Russian).

[8] Bezrodny B.F. Features of cybersecurity of automated process control systems in railway transport. December 2020 – January 2021, www.secuteck.ru. URL: https://www.secuteck.ru/articles/osobennosti-kiberbezopasnosti-asu-tp-na-zheleznodorozhnom-transporte (accessed: 16.05.2022) (in Russian).

[9] Smirnov D.O., Bezrodny B.F., Bespalov A.V. The Problem of Trust. Mag. "Nanoindustry". 2021, vol. 14, no. S7 (107), p. 340–342. URL: https://www.elibrary.ru/item.asp?id=46704489 (accessed: 16.05.2022) (in Russian).

[10] Chuprinov, Anatoliy A.; Smirnov, Dmitry O. Indirect signs method for detecting hardware threats of technical means. IT Security (Russia), [S.l.], vol. 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 (in Russian).

[11] Dorokhova I., Bashkirov A., Novoderezhkin A. Rosatom Automated Control Systems will deal with microelectronics. URL: https://strana-rosatom.ru/2021/06/28/rasu-zajmetsya-mikroelektronikoj /?ysclid=l2f39a8gu0 (accessed 16.05.2022) (in Russian).

Поступила в редакцию – 12 мая 2022 г. Окончательный вариант – 05 июня 2022 г.
Received – May 12, 2022. The final version – June 05, 2022.