DOI: 10.58168/CISMP2024_40-43
УДК 004.9

ОРГАНИЗАЦИЯ РАБОТЫ ПО ПРОТИВОДЕЙСТВИЮ ДЕСТРУКТИВНОМУ ВОЗДЕЙСТВИЮ НА ЭТАПЕ ИСПЫТАНИЙ ОПЫТНОГО ОБРАЗЦА МИКРОСХЕМ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Ю.Ю. Громов[1], М.М. Репин[2], К.В. Стародубов[3]

[1]ФГБОУ ВО «Тамбовский государственный технический университет»
[2]ФГБОУ «Московский государственный технический университет имени Н.Э. Баумана»
[3]ФГБОУ ВО «МИРЭА - Российский технологический университет»

Аннотация. В статье приводятся результаты анализа существующих подходов к организации работ по противодействию деструктивному воздействию на этапе испытаний опытного образца микросхем специального назначения. Выделены ключевые особенности данных работ и предложен подход к организации мероприятий по противодействию деструктивному воздействию, позволяющий предотвратить обнаружение и определение характеристик образца микросхем специального назначения.

Ключевые слова: микросхемы специального назначения, жизненный цикл, противодействие, образец.

THE WORK TO COUNTER DESTRUCTIVE IMPACT AT THE TESTING STAGE OF A PRELIMINARY SPECIAL-PURPOSE MICROCIRCUITS

Yu.Yu. Gromov[1], M.M. Repin[2], K.V. Starodubov[3]

[1]Federal State Budgetary Educational Institution Tambov State Technical University
[2]Federal State Budgetary Educational Institution N.E. Bauman Moscow State Technical University
[3]Federal State Budgetary Educational Institution of Higher Education "MIREA - Russian Technological University

Abstract. The article presents the results of the analysis of existing approaches to the organization of work to counteract destructive influence at the stage of testing a prototype of special-purpose microcircuits. The key features of these works are highlighted and an approach to the organization of measures to counteract destructive influence is proposed, which allows preventing the detection and determination of the characteristics of a sample of special-purpose microcircuits.

Keywords: special-purpose microcircuits, life cycle, counteraction, sample.

Организация работ по противодействию деструктивному воздействию (ПДВ) на этапе испытаний опытного образца микросхем специального назначения (МСН) является важной частью работ по ПДВ, которые проводятся

на всех стадиях жизненного цикла образцов МСН. Данная тема частично освещена в ряде работ [1-3], где представлен ряд моделей развития технических разведок и угроз деструктивного воздействия, которые можно применять при проведении контроля эффективности ПДВ, а также частично отражены вопросы построения системы противодействия обнаружению и распознаванию характеристик образцов МСН.

Для того чтобы обеспечить оптимальный уровень противодействия и свести к минимуму вероятность обнаружения сигналов испытываемых образцов и определения параметров этих сигналов, необходимо применять комплексный подход к организации ПДВ.

На основе анализа представленных материалов была построена методика планирования и организации работ по ПДВ, позволяющая создать систему ПДВ, удовлетворяющую всем требованиям в каждом конкретном случае.

При разработке плана по организации ПДВ необходимо руководствоваться принципами, соблюдение которых обеспечивает наиболее эффективное решение поставленных задач. Эти принципы заключаются в том, что ПДВ, независимо от масштабов проводимых испытаний и конкретной обстановки, должна быть комплексной, нешаблонной и непрерывной. Под комплексностью подразумевается организация противодействия всем возможным угрозам и согласование всех мер защиты по цели, месту и времени. Нешаблонность организации ПДВ подразумевает под собой исключение применения одинакового подхода к построению систем противодействия различных образцов МСН, так как подобная практика может позволить предполагаемому противнику выработать эффективные методы обхода системы ПДВ. Непрерывность ПДВ подразумевает, что мероприятия по ПДВ должны выполняться постоянно на всех этапах проведения испытаний опытного образца МСН.

В соответствии с этими принципами на этапе проведения испытаний целесообразно проводить следующие виды работ по ПДВ от технических разведок (ТР):

Определение опасных видов ТР.

Определение опасных видов ТР проводится исходя из целей противодействия и имеющихся перечней сведений, подлежащих скрытию. Основное внимание должно уделяться защите характеристик испытываемого образца РТ. После анализа охраняемых сведений об образце необходимо определить возможные каналы утечки информации, а также методы и средства ТР.

Определение исходной защищенности от выбранных видов ТР.

Выделив на предыдущем этапе опасные виды ТР, необходимо оценить имеющиеся средства противодействия и применяемые организационные меры на достаточность для обеспечения защиты образца МСН на всех этапах проведения испытаний. Оценка проводится исходя из ценности охраняемых сведений и возможностей предполагаемого противника. Также на данном этапе необходимо разработать план проведения организационных и технических

мероприятий и план контроля эффективности ПДВ на последующих этапах проведения испытаний образца МСН.

Проведение организационных и технических мероприятий по ПДВ.

В соответствии с разработанным на предыдущем этапе планом, на данном этапе необходимо провести ряд организационных и технических мероприятий, которые позволят исключить или существенно затруднить обнаружение и определение характеристик образца МСН.

Контроль эффективности ПДВ во время проведения испытаний и выявление паразитных каналов утечки информации.

Контроль эффективности ПДВ подразделяется на организационный и технический. [4] Организационный контроль проводят при завершении определенного этапа испытаний образца, а технический контроль проводится при наличии реальных возможностей ведения ТР образца МСН, ее составных частей и комплектующих изделий.

В зависимости от способа получения информации о контролируемых параметрах образца МСН могут использоваться следующие методы:

- расчетный, заключающийся в определении контролируемых признаков образца с использованием математических моделей расчета и информации об исходных данных о значениях параметров объекта и условий контроля [5];
- инструментальный, заключающийся в непосредственном измерении контролируемых признаков с использованием средств контроля.

Подводя итог, при организационном контроле используются расчетный метод оценки, а при техническом инструментальный метод.

Проведение оценки выявленных паразитных сигналов на наличие охраняемых сведений об образце МСН.

В случае если при проведении контроля на этапах испытании были выявлены паразитные каналы утечки информации, необходимо провести анализ сигналов, фиксируемых в каналах утечки на наличие в них охраняемых сведений об образце МСН. Анализ проводится расчетным и инструментальным методами. Расчетный метод может быть построен на сравнении паразитного сигнала с эталонным и выделении в нем параметров образца. Инструментальный метод заключается в имитации действий ТР противника и оценке, с помощью специальных средств, возможности перехвата охраняемых параметров.

Защита образцов МСН от технических средств разведки на этапе проведения испытаний является важной частью общего плана по ПДВ на всех этапах жизненного цикла образца. Основное внимание должно уделяться характеристикам образца, раскрывающим новые технологии, использованные при создании образца, возможности образца, области применения и др. Использование предложенного подхода к организации мероприятий по ПДВ

позволит предотвратить обнаружение и определение характеристик образца МСН.

Список литературы

1. Меньшаков Ю.К. Основы защиты от технических разведок – Москва, 2011. – 478 с.
2. Модели технических разведок и угроз безопасности информации. Коллективная монография / под ред. Е.М. Сухарева. Кн. 3. – Москва, 2003. – 144 с.
3. Цветнов В.В., Демин В.П., Куприянов А.И. Радиоэлектронная борьба: радиомаскировка и помехозащита: Учебное пособие. – Москва, 1999. – 240 с.
4. Клименко, А. Н. Методы и средства контроля информационной безопасности в системах ПВО / А. Н. Клименко. — М.: Радиотехника, 2010. – 412 с.
5. Иванов, С. В. Принципы организации ПВО в современных условиях / С. В. Иванов // Военно-промышленный курьер. – 2018. – № 24. – С. 15-23.

References

1. Menshakov Yu.K. Fundamentals of protection against technical intelligence - Moscow, 2011. - 478 p.
2. Models of technical intelligence and threats to information security. Collective monograph / Ed. by E.M. Sukharev. Book. 3. - Moscow, 2003. - 144 p.
3. Tsvetnov V.V., Demin V.P., Kupriyanov A.I. Electronic warfare: radio masking and jamming: Textbook. - Moscow, 1999. - 240 p.
4. Klimenko, A. N. Metody i sredstva kontrolya informatsionnoy bezopasnosti v sistemakh PVO / A. N. Klimenko. – M.: Radiotekhnika, 2010. – 412 s.
5. Ivanov, S. V. Printsipy organizatsii PVO v sovremennykh usloviyakh / S. V. Ivanov // Voyenno-promyshlennyy kurer. – 2018. – No. 24. – S. 15-23