ISSN 2074-7128 (print), ISSN 2074-7136 (on-line)

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
(IT Security)

Периодический рецензируемый научный журнал «Безопасность информационных технологий», освещающий широкий спектр проблем обеспечения информационной безопасности, в том числе технологические, организационно-правовые и образовательные аспекты.

Журнал зарегистрирован в Государственном комитете Российской Федерации по печати.
Свидетельство № 017789.
Издается с 1994 г.

С момента основания и до настоящего времени учредителем журнала является федеральное государственное автономное образовательное учреждение высшего образования Национальный исследовательский ядерный университет «МИФИ» (НИЯУ МИФИ).

С 2007 г. и по настоящее время журнал входит в Перечень ВАК ведущих рецензируемых научных журналов и изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени доктора и кандидата наук по отраслям науки и группе специальностей научных работников 05.13.11 – Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей (технические науки), 05.13.19 – Методы и системы защиты информации, информационная безопасность (технические науки), по которым журнал входит в этот перечень.

Основные тематические направления журнала:

- *Концептуальные основы обеспечения информационной безопасности автоматизированных систем;*
- *Методические подходы к анализу и оценке рисков информационной безопасности, технологии поиска уязвимостей в программном обеспечении;*
- *Оценка уровня защищенности автоматизированных систем;*
- *Программно-технические способы и средства обеспечения информационной безопасности.*

Журналом приветствуются статьи на русском и английском языках.

IT Security (Russia)

IT Security is a periodic peer-reviewed scientific journal publishing papers on a wide range of information security topics, including technological, organizational, legal and educational problems.

Since its establishment in 1994 (registration certificate No. 017789 by the State Committee for Press of the Russian Federation), the journal has been publishing by the Federal Autonomous Educational Institution of Higher Education National Research Nuclear University, a.k.a. "MEPhI" (Moscow Engineering Physics Institute).

Papers in Russian and English are equally welcome.

Focus topics:

- *Fundamentals of information security of automated systems;*
- *Methodology of assessing the information security risks;*
- *Technology of detecting software vulnerabilities;*
- *Evaluation of the security level of automated systems;*
- *Soft- and hardware means of ensuring information security.*

СОДЕРЖАНИЕ

Ирина Г. Дровникова, Елена С. Овчинникова, Евгений А. Рогозин
ФОРМИРОВАНИЕ ОСНОВНЫХ ПОКАЗАТЕЛЕЙ ОПАСНОСТИ СЕТЕВЫХ АТАК
В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ОРГАНОВ ВНУТРЕННИХ ДЕЛ
6

Анатолий П. Дураковский, Леонид Н. Кессаринский, Алексей О. Ширин
МАРКИРОВКА И ПРОВЕРКА ПОДЛИННОСТИ ИЗДЕЛИЙ МИКРОЭЛЕКТРОНИКИ
НА ОСНОВЕ НЕКЛОНИРУЕМОСТИ РАДИАЦИОННОГО ПОВЕДЕНИЯ
18

Рустем В. Пенерджи, Григорий П. Гавдан
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ
26

Вячеслав А. Чепов, Иван И. Швецов-Шиловский, Сергей Б. Шмаков
АЛГОРИТМ СООТНЕСЕНИЯ ФИЗИЧЕСКОЙ И ЛОГИЧЕСКОЙ АДРЕСАЦИЙ
В МИКРОСХЕМАХ ПАМЯТИ С ПОМОЩЬЮ ИСТОЧНИКОВ
ЛАЗЕРНОГО ИЗЛУЧЕНИЯ
43

Сергей В. Дуга, Андрей И. Труфанов
СЕТЬ ЗНАНИЙ КАК КОНЦЕПЦИЯ СИСТЕМ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЯ
В ПРЕДВАРИТЕЛЬНОМ СЛЕДСТВИИ
54

Роман И. Гвоздев, Иван И. Швецов-Шиловский, Сергей Б. Шмаков.
АДАПТИРОВАННАЯ МЕТОДИКА КОНТРОЛЯ ФУНКЦИОНАЛЬНЫХ СБОЕВ
В NOR FLASH-ПАМЯТИ ПРИ ИСПЫТАНИЯХ НА СТОЙКОСТЬ
К ВОЗДЕЙСТВИЮ ТЯЖЁЛЫХ ЗАРЯЖЕННЫХ ЧАСТИЦ
66

Роман С. Торшин, Георгий С. Сорокоумов, Дмитрий В. Бобровский,
Александр А. Демидов, Анастасия В. Уланова
ИЗМЕРЕНИЕ КРИТЕРИАЛЬНЫХ ПАРАМЕТРОВ АНАЛОГО-ЦИФРОВЫХ
ПРЕОБРАЗОВАТЕЛЕЙ И КОНТРОЛЬ ИХ ИЗМЕНЕНИЯ ВО ВРЕМЯ
РАДИАЦИОННОГО ЭКСПЕРИМЕНТА
76

Дмитрий О. Титовец, Николай Д. Кравченко, Андрей Б. Каракозов,
Александр И. Чумаков, Дмитрий В. Бобровский
ИСПОЛЬЗОВАНИЕ ФУНКЦИИ ГЕНЕРАЦИИ ЗАРЯДА ПРИ ОЦЕНКЕ ПАРАМЕТРОВ
ЧУВСТВИТЕЛЬНОСТИ КМОП МИКРОСХЕМ
К ОДИНОЧНЫМ СБОЯМ ПРИ ВОЗДЕЙСТВИИ НЕЙТРОНОВ
89

Владислав Д. Калашников, Алексей Ю. Егоров, Армен В. Согоян,
Анастасия В. Уланова, Андрей Б. Каракозов, Павел А. Баламутов
ВЛИЯНИЕ ПОВЫШЕННОЙ ИНТЕНСИВНОСТИ НАБОРА ДОЗЫ ИОНИЗИРУЮЩЕГО
ИЗЛУЧЕНИЯ НА СТОЙКОСТЬ КМОП МИКРОСХЕМ
СИСТЕМ ПЕРЕДАЧИ ИНФОРМАЦИИ
98

CONTENT

Irina G. Drovnikova, Elena S. Ovchinnikova, Evgeni A. Rogozin
NETWORK ATTACKS MAIN DANGER INDICATORS FORMATION IN INTERNAL AFFAIRS BODIES AUTOMATED SYSTEMS
6

Anatoly P. Durakovskiy, Leonid N. Kessarinskiy, Alexey O. Shirin
THE USE OF MICROELECTRONICS RADIATION BEHAVIOR AS PHYSICAL UNCLONED FUNCTION TO FIND COUNTERFEIT
18

Rustem V. Penerdji, Grigory P. Gavdan
INFORMATION SECURITY OF STATE INFORMATION SYSTEMS
26

Viacheslav A. Chepov, Ivan I. Shvetsov-Shilovskiy, Sergey B. Shmakov
ALGORITHM FOR MATCHING PHYSICAL AND LOGICAL ADDRESSING IN MEMORY CHIPS USING LASER SOURCES
43

Sergey V. Duga, Andrey I. Trufanov
THE KNOWLEDGE GRAPH CONCEPT OF DECISION SUPPORT SYSTEM IN PRELIMINARY INVESTIGATION
54

Roman I. Gvozdev, Ivan I. Shvetsov-Shilovskiy, Sergey B. Shmakov
ADAPTED METHOD FOR MONITORING FUNCTIONAL FAILURES IN NOR FLASH-MEMORY DURING TESTS FOR RESISTANCE TO HEAVY CHARGED PARTICLES
66

Roman S. Torshin, Georgy S. Sorokoumov, Dmitry V. Bobrovsky, Alexander A. Demidov, Anastasya V. Ulanova
MEASUREMENT OF CRITERIA PARAMETERS OF ANALOG-TO-DIGITAL CONVERTERS AND MONITORING OF THEIR CHANGES DURING THE RADIATION EXPERIMENT
76

Dmitry O. Titovets, Nikolay D. Kravchenko, Andrey B. Karakozov, Alexander I. Chumakov, Dmitry V. Bobrovsky
USING THE BURST GENERATION RATE FUNCTION TO EVALUATE THE PARAMETERS OF CMOS CHIP SENSITIVITY TO SINGLE EVENT UPSETS WHEN EXPOSED TO NEUTRONS
89

Vladislav D. Kalashnikov, Alexey Yu. Egorov, Armen V. Sogoyan, Anastasia V. Ulanova, Andrey B. Karakozov, Pavel A. Balamutov
THE INFLUENCE OF HIGH IONIZING DOSE RATE ON CMOS IC RADIATION HARDNESS USED IN DATA TRANSMISSION ELEMENTS
98

Ирина Г. Дровникова[1], Елена С. Овчинникова[2], Евгений А. Рогозин[3]
[1,2,3]Воронежский институт министерства внутренних дел Российской федерации,
пр-т Патриотов, 53, Воронеж, 394065, Россия
[1]e-mail: idrovnikova@mail.ru, https://orcid.org/0000-0001-5265-5875
[2]e-mail: yelena_ovchinnikova1@mail.ru, https://orcid.org/0000-0003-4139-9524
[3]e-mail: evgenirogozin@yandex.ru, https://orcid.org/0000-0002-4455-7535

ФОРМИРОВАНИЕ ОСНОВНЫХ ПОКАЗАТЕЛЕЙ ОПАСНОСТИ СЕТЕВЫХ АТАК В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

DOI: http://dx.doi.org/10.26583/bit.2020.3.01

Аннотация. Целью статьи является анализ существующих показателей, используемых при оценивании опасности реализации угроз информационной безопасности в автоматизированных системах, для выявления их достоинств, недостатков и возможностей применения при проведении количественной оценки опасности реализации сетевых атак на автоматизированные системы, эксплуатируемые в защищенном исполнении на объектах информатизации органов внутренних дел. Для достижения поставленной цели применен метод системного анализа показателей опасности угроз на основе исследования открытых литературных источников, международных и отраслевых стандартов Российской Федерации по защите информации в автоматизированных системах, методических, руководящих документов и приказов Федеральной службы по техническому и экспертному контролю России по проблеме оценивания опасности реализации угроз несанкционированного доступа в автоматизированные системы, а также нормативной базы МВД России, регламентирующей эксплуатацию автоматизированных систем органов внутренних дел в защищенном исполнении. Для осуществления корректного выбора адекватных показателей при проведении количественного анализа риска нарушения информационной безопасности проанализирована риск-модель автоматизированной системы. Для проведения количественной оценки опасности реализации сетевых атак и исследования их в динамическом режиме предложены основные направления совершенствования выявленных показателей с учетом реально существующих особенностей и недостатков эксплуатации защищенных автоматизированных систем органов внутренних дел. Разработка динамического интегрального показателя опасности атак, отражающего реальные динамические свойства процесса реализации множества типовых сетевых атак на автоматизированную систему, и совершенствование существующего математического обеспечения оценки опасности сетевых атак путем определения вероятностно-временных характеристик множественных параллельно реализуемых типовых атак на основе имитационного моделирования позволит провести количественную оценку опасности и повысить реальную защищенность автоматизированных систем в процессе их эксплуатации на объектах информатизации органов внутренних дел.

Ключевые слова: автоматизированная система, сетевая атака, информационный риск, динамический интегральный показатель опасности, количественная оценка опасности.
Для цитирования: ДРОВНИКОВА, Ирина Г.; ОВЧИННИКОВА, Елена С.; РОГОЗИН, Евгений А. ФОРМИРОВАНИЕ ОСНОВНЫХ ПОКАЗАТЕЛЕЙ ОПАСНОСТИ СЕТЕВЫХ АТАК В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ОРГАНОВ ВНУТРЕННИХ ДЕЛ. Безопасность информационных технологий, [S.l.], v. 27, n. 3, p. 6–17, 2020. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1288>. Дата доступа: 02 sep. 2020. DOI: http://dx.doi.org/10.26583/bit.2020.3.01.

Irina G. Drovnikova[1], Elena S. Ovchinnikova[2], Evgeni A. Rogozin[3]
[1,2,3]Voronezh Institute of the Ministry of the Interior,
Prospect Patriotov, 53, Voronezh, 394065, Russia
[1]e-mail: idrovnikova@mail.ru, https://orcid.org/0000-0001-5265-5875
[2]e-mail: yelena_ovchinnikova1@mail.ru, https://orcid.org/0000-0003-4139-9524
[3]e-mail: evgenirogozin@yandex.ru, https://orcid.org/0000-0002-4455-7535

Network attacks main danger indicators formation in Internal Affairs Bodies automated systems

DOI: http://dx.doi.org/10.26583/bit.2020.3.01

Abstract. The purpose of this study is to analyze the existing indicators used in information security implementing threats risk assessing in automated systems. The goal is to identify its advantages, disadvantages and application possibilities, when conducting implementing danger network attacks quantitative assessment on automated systems operated in a secure execution at the Internal Affairs Bodies informatization objects. To achieve this goal we use the method of system analysis of threat hazard indicators based on research of open literature sources, international and industry standards of the Russian Federation for information protection in automated systems, methodological and guiding documents and orders of the Federal service for technical and expert control of Russia on the problem of assessing the risk of unauthorized access to automated systems, as well as the regulatory framework of the Ministry of internal Affairs of Russia, regulating the operation of automated systems of internal Affairs bodies in a protected version. The risk model of the automated system is analyzed to make a correct choice of adequate indicators when conducting a quantitative analysis of the risk of information security violations. To conduct network attacks danger quantitative assessment and study them in a dynamic mode, the main directions for improving the identified indicators are proposed, taking into account Internal Affairs Bodies protected automated systems operation actual features and disadvantages. Development of a dynamic integral attack hazard indicator that reflects the real dynamic properties of the process of implementing a set of typical network attacks on an automated system, and improvement of existing mathematical software for assessing the risk of network attacks by determining the probability-time characteristics of multiple parallel attacks implemented model-based simulation will allow to quantify risk and increase the real security of the automated systems in process of their operation on the objects of Informatization of Internal Affairs bodies.

Keywords: automated system, network attack, information risk, dynamic integral danger indicator, quantitative danger assessment.

For citation: DROVNIKOVA, Irina G.; OVCHINNIKOVA2, Elena S.; ROGOZIN, Evgeni A. Network attacks main danger indicators formation in Internal Affairs Bodies automated systems. IT Security (Russia), [S.l.], v. 27, n. 3, p. 6–17, 2020. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1288>. Date accessed: 02 sep. 2020. DOI: http://dx.doi.org/10.26583/bit.2020.3.01.

Введение

Оценивание опасности реализации угроз несанкционированного доступа (НСД), осуществляемых через удаленное взаимодействие с автоматизированной системой (АС) (сетевые атаки), является одним из ключевых моментов в процессе оценивания эффективности функционирования систем защиты информации (СЗИ) от НСД на этапе эксплуатации АС в защищенном исполнении на объектах информатизации органов внутренних дел (ОВД). Это, в свою очередь, необходимо для формирования требований по защите информации (ЗИ) в АС ОВД с целью разработки адекватных существующим атакам перспективных образцов СЗИ от НСД[1,2].

Обеспечение достаточной степени защищенности АС ОВД для их эффективного функционирования в условиях сетевых атак предполагает проведение процедуры оценивания опасности реализации атак как в процессе разработки СЗИ от НСД с целью формирования на этой основе частной модели актуальных атак для конкретной АС на объекте информатизации ОВД, так и при мониторинге и переоценке атак в ходе эксплуатации СЗИ от НСД, что приводит к необходимости разработки адекватных

[1]ISO/IEC 17000:2004. Conformity assessment. Dictionary and General principles.
[2]ГОСТ Р ИСО/МЭК 17021-2012. Национальный стандарт Российской Федерации. Оценка соответствия. Требования к органам, проводящим аудит и сертификацию систем менеджмента.

показателей опасности сетевых атак на защищаемые АС ОВД[3].

Необходимость разработки показателей опасности сетевых атак на АС, эксплуатируемые в защищенном исполнении на объектах информатизации ОВД, подтверждается требованиями приказа МВД России от 14.03.2012 № 169 «Об утверждении Концепции обеспечения информационной безопасности органов внутренних дел Российской Федерации до 2020 года», в котором определены цели, задачи, принципы и основные направления обеспечения информационной безопасности (ИБ) ОВД. В приказе отмечается, что одним из механизмов реализации Концепции является разработка критериев и методов оценки эффективности систем обеспечения ИБ ОВД, однако не рассматриваются конкретные критерии (показатели) опасности сетевых атак, необходимые для последующего формирования показателей и проведения количественной оценки эффективности функционирования СЗИ от НСД в АС ОВД. В то же время, данный документ во многом подтверждает актуальность проблемы разработки показателей опасности сетевых атак и определяет перспективные аспекты научных исследований в данной области применительно к объектам информатизации ОВД – АС, эксплуатируемым в защищенном исполнении.

1. Постановка задачи

В связи с недостаточностью научных исследований, посвященных разработке показателей опасности сетевых атак на АС ОВД, проанализируем показатели, используемые в настоящее время при оценивании опасности реализации угроз ИБ в АС с целью выявления их достоинств, недостатков и возможностей применения для проведения количественной оценки опасности реализации сетевых атак на защищенные АС, эксплуатируемые на объектах информатизации ОВД.

2. Теоретический анализ показателей опасности угроз информационной безопасности автоматизированных систем

Оценивание опасности реализации угрозы осуществляется по размеру информационного риска [1–3]. Анализ нормативной документации, раскрывающей понятие «риск», показал отсутствие единой трактовки данного термина[4,5,6,7]. Максимально соответствующим тому, что понимается под риском в большинстве публикаций, следует считать определение, согласно которому риск рассматривается как сочетание вероятности нанесения ущерба и тяжести этого ущерба[8].

С учетом выше изложенного под информационным риском будем понимать количественную величину, характеризующую возможность нанесения АС некоторого ущерба, а под показателем опасности угрозы – меру размера информационного риска от ее реализации.

---

[3]ГОСТ Р ИСО/МЭК 15408-2-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2: Функциональные компоненты безопасности.

[4]ГОСТ Р 53114-2008. Национальный стандарт Российской Федерации. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения.

[5]ГОСТ Р 51897-2011. Национальный стандарт Российской Федерации. Менеджмент риска. Термины и определения.

[6]О техническом регулировании: федеральный закон от 27.12.2002 № 184-ФЗ.

[7]ГОСТ Р 22.0.02-2016. Национальный стандарт Российской Федерации. Безопасность в чрезвычайных ситуациях. Термины и определения.

[8]ГОСТ Р 51898-2002. Национальный стандарт Российской Федерации. Аспекты безопасности. Правила включения в стандарты.

Таким образом, информационный риск в условиях сетевых атак следует рассматривать как сочетание двух характеристик: величины возможного ущерба от реализации атак и оценки возможности этой реализации (т.е. нанесения ущерба) [4].

Задачи анализа, обоснования и разработки показателей опасности угроз ИБ АС не являются новыми и решены в ряде методических документов Федеральной службы по техническому и экспертному контролю (ФСТЭК) России[9,10] и работах [4–9]. Представленные в [4] результаты анализа четырех наиболее популярных подходов, используемых в настоящее время при оценивании опасности реализации угроз ИБ в АС (экспертного, шкального, балльного, вероятностного), позволяют констатировать отсутствие среди авторов единства в выделении основных показателей опасности угроз (табл. 1).

Таблица 1. Представление показателей опасности угроз ИБ в АС

№ п/п	Название подхода	Показатели опасности угроз ИБ
1	Экспертный – основан на экспертном методе оценки, представленном в Методических документах ФСТЭК России	Уровень защищенности АС Потенциал нарушителя, необходимый для реализации угрозы ИБ в АС Максимальные размеры видов возможного ущерба[9]
		Коэффициент реализуемости угрозы Вербальный показатель опасности угрозы для АС[10]
2	Шкальный – основан на методе оппозиционных (полярных) шкал	Коэффициент опасности угрозы – свертка коэффициента опасности несанкционированного действия и вероятности реализации угрозы [7, 8]
3	Балльный – основан на балльном (табличном) методе оценки	Степень угрозы Степень уязвимости Показатель цены потери [9]
4	Вероятностный – основан на математическом моделировании процессов реализации угроз	Вероятность возникновения угрозы Вероятность реализации угрозы Вероятность нанесения ущерба реализацией угрозы Величина нанесенного ущерба [8]

Так в рамках экспертного подхода применяются следующие показатели опасности угрозы: уровень защищенности АС и потенциал нарушителя, необходимый для реализации данной угрозы ИБ в заданной АС (для оценивания возможности реализации угрозы); максимальные размеры каждого вида возможного ущерба, связанного с нарушением конфиденциальности, целостности или доступности каждого вида информации (для оценивания итоговой величины возможного ущерба)[9]. При оценивании опасности реализации угрозы персональным данным (ПДн) и определении актуальных угроз безопасности ПДн в АС ПДн предлагаются два показателя: коэффициент реализуемости угрозы и вербальный показатель опасности угрозы для рассматриваемой АС ПДн[10].

При использовании шкального подхода [7, 8] оценивание опасности реализации угрозы ИБ основывается на применении комплексного динамического показателя –

[9]ФСТЭК России. Методический документ. Методика определения угроз безопасности информации в информационных системах.

[10]ФСТЭК России. Методический документ. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

коэффициента опасности угрозы K_{thu}, который определяется в виде свертки коэффициента опасности несанкционированного действия K_g и вероятности реализации угрозы $P_{thu}(t)$:

$$K_{thu} = K_g \cdot P_{thu}(t), \quad (1)$$

где K_g представляет собой отношение максимального значения величины нанесенного ущерба к предельно допустимому его значению (применительно к общему объему информационного ресурса, для которого может быть реализовано данное несанкционированное действие)

$$K_g = \frac{\bar{u}}{u_{np}}. \quad (2)$$

При использовании балльного подхода для оценивания опасности реализации угроз ИБ в АС в [9] предлагаются три показателя опасности угрозы: степень (уровень) угрозы, степень (уровень) уязвимости, показатель цены потери (в зависимости от ценности ресурсов и вида возможного ущерба).

Очевидным недостатком показателей опасности угроз, выделенных в рамках изложенных подходов, применительно к оцениванию опасности реализации сетевых атак на АС ОВД является их недостаточная точность, обусловленная необходимостью экспертного участия в процессе оценивания.

Указанного недостатка лишен четвертый подход (вероятностный), используемый при оценивании опасности реализации угроз ИБ в АС, основанный на математическом моделировании (аналитическом, имитационном) процессов реализации угроз. Данный подход применяется для описания случайных событий, в частности, на основе определения их вероятностно-временных характеристик (ВВХ), что дает возможность проводить количественную оценку опасности реализации угроз обеспечения ИБ в АС и исследовать их в динамическом (временном) режиме [8, 10–13].

Модель риск-анализа АС, разрабатываемая в рамках вероятностного подхода, представляет собой математическую модель, учитывающую, во-первых, воздействие на систему всего множества типовых угроз и, во-вторых, применение различных средств и систем ЗИ. Выходным параметром рассматриваемой риск-модели является интегральный информационный риск для функционирующей в заданных условиях АС. Следовательно, вариация средств и систем ЗИ представляет собой способ регулирования рисков АС. Полученные значения риска для каждой исследуемой АС позволяют оптимизировать комплекс мер защиты.

Для осуществления корректного выбора адекватных параметров при проведении количественного анализа риска нарушения ИБ в [8] рассматривается схема воздействия угрозы на защищаемую АС, включающая следующие элементы:

1) *субъект угрозы* (ее источник) – активная составляющая процесса, способная посредством выполнения каких-либо действий оказывать влияние на другие составляющие;

2) *процесс реализации угрозы* – конкретный сценарий (операция), осуществляемый субъектом для достижения поставленной цели;

3) *объект угрозы* – пассивная составляющая процесса, подверженная влиянию субъекта;

4) *предмет угрозы* – цель действий субъекта (характеристика объекта или ее определенное значение, какое-либо свойство объекта).

Представленная схема рассмотрена в [4] применительно к воздействию сетевой атаки на защищаемую АС (рис. 1). Элементы схемы характеризуются четырьмя параметрами, составляющими основу риск-модели: $p_{\text{ви}}$, $p_{\text{ри}}$ – вероятности возникновения и реализации u-й атаки соответственно, $p_{\text{уи}j}$ – вероятность нанесения ущерба вида j реализацией u-й атаки, d_j – величина нанесенного ущерба вида j. Указанные параметры предлагаются в виде показателей опасности u-й атаки.

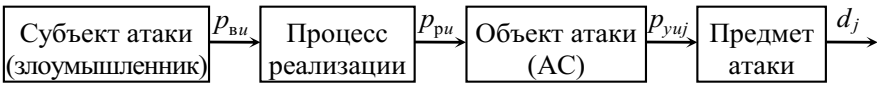


Рис. 1. Схема сетевой атаки на АС с параметрами, характеризующими ее элементы (Fig. 1. Scheme of network attack on the AS with parameters that characterize its elements)

Таким образом, величина интегрального информационного риска атакуемой АС определяется значением вероятности p нанесения общего ущерба реализацией множества типовых сетевых атак и количественным значением d этого ущерба.

При оценивании опасности реализации сетевых атак на АС вероятностный подход реализуется, как правило, в двух вариантах с использованием различных показателей опасности атаки (табл. 2).

Таблица 2. Взаимосвязь вариантов реализации вероятностного подхода с используемыми показателями опасности сетевой атаки на АС

№ п/п	Название варианта подхода	Показатели опасности сетевой атаки
1	Полностью вероятностный $(p \cdot p)$	$p_u(d)$ – вероятность нанесения ущерба *d* при реализации *u*-й атаки; $p_u(t)$ – вероятность реализации *u*-й атаки за время t
2	Частично вероятностный $(d \cdot p)$	$\overline{d_u}$ – средний размер возможного ущерба, наносимого в результате реализации *u*-й атаки; $p_u(t)$ – вероятность реализации *u*-й атаки за время t

Первый вариант – полностью вероятностный $(p \cdot p)$. Он сводится к проведению оценки риска R в виде нахождения произведения вероятности $p_u(d_{\min} < d < d_{\max})$ того, что при реализации конкретной u-й атаки будет нанесен ущерб d, размеры которого находятся в некотором заданном диапазоне $(d_{\min}, d_{\max})$ и вероятности $p_u(t)$ реализации такой атаки за заданное время t:

$$R(d_{\min}, d_{\max}, t) = p(d_{\min} < d \le d_{\max}) \cdot p_u(t). \quad (3)$$

Сложность использования такого варианта подхода заключается в том, что необходимо определить плотности распределения вероятностей $w(u)$ нанесения ущерба, по которой может быть рассчитана вероятность.

Для непрерывного закона распределения вероятностей эта вероятность рассчитывается по формуле

$$p(d_{\min} < d \le d_{\max}) = \int_{d_{\min}}^{d_{\max}} w(x)dx\,, \quad (4)$$

а для дискретного – по формуле

$$p(d_{\min} < d \le d_{\max}) = \sum_i d_i \cdot p(d_i) \quad (5)$$

для всех i, для которых $d_{\min} < d_i \leq d_{\max}$.

Однако, как непрерывное, так и дискретное распределение вероятностей нанесения ущерба в подавляющем большинстве случаев неизвестно и принимаются разные допущения относительно законов распределения возможного ущерба.

В связи с этим широкое применение нашел *второй вариант* – частично вероятностный $(d \cdot p)$, в котором используется оценка среднего размера $\overline{d_u}$ возможного ущерба, наносимого в результате реализации u-й атаки, и вероятность $p_u(t)$ реализации u-й атаки за заданное время t. При этом риск R оценивается как произведение:

$$R_u(t) = \overline{d_u} \cdot p_u(t)\,. \tag{6}$$

Для расчета должны быть известны (разработаны) модель оценки размеров ущерба и модель оценки вероятностей реализации сетевой атаки, в результате которой этот ущерб будет нанесен.

Для проведения количественной оценки размеров ущерба необходимо связать вид наносимого ущерба с предметом реализуемой на АС типовой сетевой атаки – нарушением конфиденциальности, целостности или доступности обрабатываемой в системе информации.

С теоретической точки зрения наилучшим для построения модели риск-анализа должен стать такой подход к оцениванию ущерба, в рамках которого к одинаковой единице измерения приводится любой ущерб, нанесенный АС реализацией сетевых атак различных типов. Однако в настоящее время вопрос оценивания ценности информации еще недостаточно изучен для возможности однозначного определения единого эквивалента ущерба нарушений ее конфиденциальности, целостности или доступности (например, финансового).

При расчете размеров ущерба необходимо учитывать важность каждого из предметов атаки для каждой конкретной АС, исходя из ее специфики и предназначения. Следовательно, за основу величины нанесенного ущерба при построении риск-модели АС целесообразно принять количество успешно реализованных сетевых атак определенного типа, рассчитывая отдельно риск для каждого из предметов этих атак.

Для адекватного оценивания рисков при реализации сетевых атак на АС необходимо проанализировать функционирование системы на некотором временном интервале $t_1 \leq t \leq t_2$. С точки зрения рисков для АС данный промежуток времени характеризуется количеством и типом атак, реализованных в течение указанного периода.

С учетом выше изложенного величина информационного риска от реализации множества сетевых атак, относящихся к типу m, может быть рассчитана по формуле

$$R_m(t) = N_m \cdot p_m(t), \tag{7}$$

где N_m – количество успешно реализованных атак типа m, приводящих за время t к нанесению ущерба АС, соответствующего предмету атаки; $p_m(t)$ – вероятность реализации атаки типа m.

В результате величина интегрального информационного риска атакуемой АС от параллельной реализации множества сетевых атак, приводящих за заданное время t к нанесению определенного вида ущерба АС, определится по формуле

$$R(t) = \sum_{m=1}^{K} N_m \cdot \prod_{m=1}^{K} p_m\,(t), \tag{8}$$

где K – количество типов успешно реализованных атак.

3. Основные аспекты совершенствования показателей опасности сетевых атак на защищенные автоматизированные системы органов внутренних дел

Рассмотренный частично вероятностный вариант реализации вероятностного подхода может быть использован при формировании основных показателей для оценивания опасности сетевых атак на АС ОВД при условии учета особенностей и недостатков эксплуатации данных систем в защищенном исполнении на объектах информатизации ОВД.

Особенности и реально существующие недостатки эксплуатации защищенных АС ОВД раскрыты в [10]. Выделим те их них, которые оказывают максимальное влияние на опасность реализации сетевых атак и, соответственно, должны быть учтены при выборе и обосновании основных показателей опасности сетевых атак на защищенные АС, эксплуатируемые на объектах информатизации ОВД.

Опыт эксплуатации современных АС в защищенном исполнении на объектах информатизации ОВД показал, что из указанных в [10] особенностей максимальное влияние на опасность реализации сетевых атак оказывают: территориальная распределенность АС, интеграция служебной информации АС в единый массив банков данных различного уровня конфиденциальности, хранение больших массивов данных. Следовательно, в АС ОВД осуществляется распределенная обработка больших объемов служебной информации различных уровней конфиденциальности, влекущая значительное количество параллельно реализуемых сетевых атак различных типов. Поэтому при расчете интегрального информационного риска от параллельной реализации множества сетевых атак на АС ОВД необходимо учесть их взаимовлияние в процессе реализации.

Из представленных в [10] недостатков эксплуатации защищенных АС на объектах информатизации ОВД максимальное влияние на эффективность функционирования их СЗИ от НСД оказывает непосредственная зависимость ресурсоемкости СЗИ от НСД от вычислительного ресурса АС (процессорного времени, оперативной памяти, дискового пространства).

Таким образом, в качестве основного показателя опасности сетевых атак на защищенные АС, эксплуатируемые на объектах информатизации ОВД, целесообразно использовать напрямую зависимый от времени динамический интегральный показатель опасности атак $V_{\text{иоп ат}}$, обратно пропорциональный показателю временной эффективности функционирования СЗИ от НСД АС $V_{\text{вэ СЗИ}}$ ($V_{\text{иоп ат}} = \frac{1}{V_{\text{вэ СЗИ}}}$) и выражающий, соответственно, меру размера интегрального информационного риска атакуемой АС ОВД от параллельной реализации множества типовых сетевых атак. При этом под временной эффективностью СЗИ от НСД понимается ее способность выполнять заданные действия в интервал времени, отвечающий заданным требованиям[11]. Следовательно, показатель $V_{\text{вэ СЗИ}}$ отражает спектр свойств СЗИ от НСД с учетом динамики ее функционирования в АС ОВД.

Взаимосвязь интегрального показателя опасности сетевых атак и выявленного недостатка эксплуатации АС в защищенном исполнении на объектах информатизации ОВД представлена в таблице 3.

Интегральный показатель опасности сетевых атак $V_{\text{иоп ат}}$ сводит за счет процедуры агрегирования в единый показатель частные показатели опасности атак $V_{\text{оп ат}\,m}$ различных типов $(m = 1, \dots, k)$, выражающие размеры информационного риска от их реализации в АС ОВД.

[11]ГОСТ 28195-89. Оценка качества программных средств. Общие положения.

Таблица 3. Связь интегрального показателя опасности сетевых атак с основным недостатком применения СЗИ от НСД в защищенных АС ОВД

Показатель	**Смысловое значение показателя**	**Недостаток**	**Смысловое значение недостатка**
$V_{\text{иоп ат}}$ – интегральный показатель опасности сетевых атак	Неспособность СЗИ от НСД соответствовать заявленным требованиям (с точки зрения временных параметров ее функционирования), а также находить эффективное решение (разумный компромисс), связанное с совместным функционированием СЗИ от НСД и защищенной АС ОВД по ее прямому назначению (обработка, хранение и передача конфиденциальной информации)	Непосредственная зависимость ресурсоемкости СЗИ от НСД от вычислительного ресурса АС ОВД	Выполнение СЗИ от НСД защитных функций осуществляется в процессе функционирования защищенной АС ОВД, что приводит к снижению производительности системы за счет использования процедурой защиты части вычислительного ресурса АС в ущерб реализации ее целевых функций. Ограниченность вычислительного ресурса АС ОВД влечет за собой увеличение времени реализации СЗИ от НСД защитных Ограниченность вычислительного ресурса АС ОВД влечет за собой увеличение времени реализации СЗИ от НСД защитных функций и, как следствие, наблюдается несоответствие используемой СЗИ предъявляемым к ней требованиям по ЗИ

Задачу оценивания $V_{\text{иоп ат}}$ в математическом виде можно представить как нахождение отображения $F: V_{\text{иоп ат}} \to \{0,1\}$, где F определяет правила, реализуемые соответствующими моделями и алгоритмами.

Поскольку реализация сетевых атак на защищенные АС на объектах информатизации ОВД представляет собой сложный динамический процесс для его формального описания в настоящее время широко применяются модели, построенные на сетях Петри-Маркова (основанные на теории сетей Петри и марковских (полумарковских) процессах) [14-16], что позволяет определять ВВХ при исследовании реализации параллельных процессов с целью формирования показателей для проведения количественной оценки опасности реализации сетевых атак на информационный ресурс

защищенных АС ОВД [8, 10, 12].

Заключение

Анализ методической и научно-технической литературы по проблеме оценивания опасности реализации угроз НСД в АС, а также нормативной базы МВД России, регламентирующей эксплуатацию АС ОВД в защищенном исполнении, выявил ряд вопросов, требующих безотлагательного решения применительно к формированию основных показателей опасности сетевых атак на АС с целью повышения реальной защищенности данных систем при их эксплуатации на объектах информатизации ОВД:

1) существующие показатели опасности угроз ИБ, как правило, недостаточно адекватно отражают реальные свойства угроз удаленного доступа, реализуемых посредством сетевых атак на информационный ресурс защищенных АС на объектах информатизации ОВД, а, следовательно, не позволяют исследовать их в динамическом режиме и проводить количественную оценку опасности реализации угроз;

2) существующие показатели опасности сетевых атак не отражают особенности и реально существующие недостатки эксплуатации АС в защищенном исполнении на объектах информатизации ОВД, а, следовательно, не могут быть использованы при проведении количественной оценки опасности реализации сетевых атак на данные системы;

3) для проведения количественной оценки опасности реализации сетевых на защищенные АС ОВД и исследования их в динамическом режиме требуются: разработка динамического интегрального показателя опасности атак, отражающего реальные динамические свойства процесса реализации множества типовых сетевых атак на АС, эксплуатируемые в защищенном исполнении на объектах информатизации ОВД; совершенствование существующего математического обеспечения оценки опасности сетевых атак путем определения вероятностно-временных характеристик множественных параллельно реализуемых типовых атак на основе имитационного моделирования.

СПИСОК ЛИТЕРАТУРЫ:

1. Язов Ю.К. Защита информации в информационных системах от несанкционированного доступа / Ю.К. Язов, С.В. Соловьев. Воронеж: Кварта, 2015. – 440 с.
2. Anisimov V.G. A risk-oriented approach to the control arrangement of security protection subsystems of information systems / V.G. Anisimov, P.D. Zegzhda, E.G. Anisimov, D.A. Bazhin // Automatic Control and Computer Sciences. 2016. Vol. 50. №. 8. P. 717–721. DOI: https://doi.org/10.3103/S0146411616080289.
3. Giannopoulos G. Risk assessment methodologies for Critical Infrastructure Protection / G. Giannopoulos, R. Filippini, M. Schimmer // European Commission Joint Research Centre Institute for the Protection and Security of the Citizen. Part I: A state of the art. Luxembourg: Publications Office of the European Union, 2017. – 45 p. URL: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/docs/pdf/ra_ver2_en.pdf (дата обращения: 19.01.2020).
4. Дровникова И.Г. Анализ существующих способов и процедур оценки опасности реализации сетевых атак в автоматизированных системах органов внутренних дел и аспекты их совершенствования / И.Г. Дровникова, Е.С. Овчинникова, Е.А. Рогозин // Вестник Воронеж. ин-та МВД России. 2019. № 4. С. 51–63. URL: https://ви.мвд.рф/upload/site132/document_journal/Vestnik_4_2019.pdf (дата обращения: 19.01.2020).
5. Al Hadidi, Mazin & Al Azzeh, Jamil & Akhmetov, Berik & Korchenko, O. & Kazmirchuk, Svitlana & Zhekambayeva, M. (2016). Methods of Risk Assessment for Information Security Management. International Review on Computers and Software (IRECOS). DOI: https://doi.org/10.15866/irecos.v11i2.8233.
6. Lippmann R.P. Threat-based risk assessment for enterprise networks / R.P. Lippmann, J.F. Riordan // Lincoln Laboratory Journal. 2016. Vol. 22. № 1. P. 33–45. URL:https://www.ll.mit.edu/sites/default/files/publication/doc/threat-based-risk-assessment-enterprise-networks-lippmann-108609.pdf (дата обращения: 20.01.2020).
7. Язов Ю.К. Организация защиты информации в информационных системах от несанкционированного доступа: монография / Ю.К. Язов, С.В. Соловьев. Воронеж: Кварта, 2018. – 588 с. URL: https://rusneb.ru/catalog/000200_000018_RU_NLR_BIBL_A_012090330/ (дата обращения: 18.01.2020).

8. Радько Н.М. Проникновения в операционную среду компьютера: модели злоумышленного удаленного доступа / Н.М. Радько, Ю.К. Язов, Н.Н. Корнеева. Воронеж: Воронеж. гос. тех. ун-т, 2013. – 265 с. URL: https://search.rsl.ru/ru/record/01007533232 (дата обращения: 18.01.2020).
9. Петренко С.А. Управление информационными рисками. Экономически оправданная безопасность / С.А. Петренко, С.В. Симонов. М.: Компания АйТи; ДМК Пресс, 2016. – 384 с. URL: https://upravlenie-informaciodisus.ru/knigi/172587-1-petrenko-a-nnimi-riskami-ekonomicheski-opravdannaya-bezopasnost-petrenko-a-simonov-v-m-kompaniya.php (дата обращения: 22.01.2020).
10. Попов А.Д. Модели и алгоритмы оценки эффективности систем защиты информации от несанкционированного доступа с учетом их временных характеристик в автоматизированных системах органов внутренних дел: дис. канд. техн. наук: 05.13.19, Попов Антон Дмитриевич. Воронеж, 2018. – 163 с. URL:https://ви.мвд.рф/Nauka/Dissovety/sostojavshiesja_zashhiti_dissertacij (дата обращения: 22.01.2020).
11. Разработка моделей и алгоритмов оценки эффективности подсистемы защиты конфиденциальных сведений при ее проектировании в системах электронного документооборота ОВД: монография / Дровникова И.Г. и др. Воронеж: Воронеж. ин-т МВД России, 2019. – 116 с. URL:https://catalog.inforeg.ru/ Inet/GetEzineByID/325482 (дата обращения: 21.01.2020).
12. Радько Н.М. Риск-модели информационно-телекоммуникационных систем при реализации угроз удаленного и непосредственного доступа / Н.М. Радько, И.О. Скобелев. М: РадиоСофт, 2015. – 232 с. URL:http://www.sozvezdie.su/science/izdaniya/riskmodeli_informatsionnotelekommunikatsionnih/ (дата обращения: 24.01.2020).
13. Бокова, О.И., Дровникова, И.Г., Етепнев, А.С., Рогозин, Е.А., & Хвостов, В.А. (2019). Методики оценивания надежности систем защиты информации от несанкционированного доступа в автоматизированных системах. Труды СПИИРАН, 18(6), 1301–1332. DOI: https://doi.org/10.15622/sp.2019.18.6.1301-1332.
14. M. El Hassan Charaf and S. Azzouzi, "A colored Petri-net model for control execution of distributed systems," 2017 4th International Conference on Control, Decision and Information Technologies (CoDIT), Barcelona, 2017. P. 0277–0282. DOI: https://doi.org/10.1109/CoDIT.2017.8102604.
15. L. Yao, P. Dong, T. Zheng, H. Zhang, X. Du and M. Guizani, "Network security analyzing and modeling based on Petri net and Attack tree for SDN," 2016 International Conference on Computing, Networking and Communications (ICNC), Kauai, HI, 2016. P. 1–5. DOI: https://doi.org/10.1109/ICCNC.2016.7440631.
16. Дровникова И.Г. Создание модели информационного конфликта «нарушитель – система защиты» на основе сети Петри-Маркова / Вестник Воронеж. ин-та МВД России. 2019. № 2. С. 93–100. URL:https://ви.мвд.рф/upload/site132/document_journal/Vestnik_2_ 2019.pdf (дата обращения: 20.01.2020).

REFERENCES:

[1] Yazov Yu.K. Protection of information in information systems from unauthorized access Yu.K. Yazov, S.V. Solovyov. Voronezh: Quarter, 2015. – 440 p. (in Russian).
[2] Anisimov V.G. A risk-oriented approach to the control arrangement of security protection subsystems of information systems V.G. Anisimov, P.D. Zegzhda, E.G. Anisimov, D.A. Bazhin. Automatic Control and Computer Sciences. 2016. Vol. 50. №. 8. P. 717–721. DOI: https://doi.org/10.3103/S0146411616080289.
[3] Giannopoulos G. Risk assessment methodologies for Critical Infrastructure Protection G. Giannopoulos, R. Filippini, M. Schimmer. European Commission Joint Research Centre Institute for the Protection and Security of the Citizen. Part I: A state of the art. Luxembourg: Publications Office of the European Union, 2017. – 45 p. URL: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/docs/pdf/ra_ver2_en.pdf (accessed: 19.01.2020).
[4] Drovnikova I.G. Analysis of existing methods and procedures for assessing the risk of network attacks in automated systems of internal Affairs bodies and aspects of their improvement I.G. Drovnikova, E.S. Ovchinnikova, E.A. Rogozin. Vestnik of the Voronezh Institute of the Ministry of internal Affairs of Russia. 2019. № 4. P. 51–63. URL: https://ви.мвд.рф/upload/site132/document_journal/Vestnik_4_2019.pdf (accessed: 19.01.2020) (in Russian).
[5] Al Hadidi, Mazin & Al Azzeh, Jamil & Akhmetov, Berik & Korchenko, O. & Kazmirchuk, Svitlana & Zhekambayeva, M. (2016). Methods of Risk Assessment for Information Security Management. International Review on Computers and Software (IRECOS). DOI: https://doi.org/10.15866/irecos.v11i2.8233.
[6] Lippmann R.P. Threat-based risk assessment for enterprise networks R.P. Lippmann, J.F. Riordan. Lincoln Laboratory Journal. 2016. Vol. 22. № 1. P. 33–45. URL: https://www.ll.mit.edu/sites/default/files/publication/doc/threat-based-risk-assessment-enterprise-networks-lippmann-108609.pdf (accessed: 20.01.2020).
[7] Yazov Yu.K. Organization of information protection in information systems from unauthorized access: monograph Yu.K. Yazov, S.V. Solovyov. Voronezh: Kvarta, 2018. – 588 p. URL: https://rusneb.ru/catalog/

000200_000018_ RU_NLR_BIBL_A_012090330/ (accessed: 18.01.2020) (in Russian).

[8] Radko N.M. Penetration into the computer operating environment: models of malicious remote access N.M. Radko, Yu.K. Yazov, N.N. Korneeva. Voronezh: Voronezh state technical University, 2013. – 265 p. URL: https://search.rsl.ru/ru/record/01007533232 (accessed: 18.01.2020) (in Russian).

[9] Petrenko S.A. Information risk management. Economically justified security S.A. Petrenko, S.V. Simonov. M: AiTi Company; DMK Press, 2016. – 384 p. URL: https://upravlenie-informaciodisus.ru/knigi/172587-1-petrenko-a-nnimi-riskami-ekonomicheski-opravdannaya-bezopasnost-petrenko-a-simonov-v-m-kompaniya.php (accessed: 22.01.2020) (in Russian).

[10] Popov A.D. Models and algorithms for evaluating the effectiveness of information protection systems against unauthorized access taking into account their time characteristics in automated systems of internal Affairs bodies: dis. cand. techn. sciences: 05.13.19, Popov Anton Dmitrievich. Voronezh, 2018. – 163 p. URL:https:// ви.мвд.рф/Nauka/Dissovety/sostojavshiesja_zashhiti_dissertacij (accessed: 22.01.2020) (in Russian).

[11] Development of models and algorithms for evaluating the effectiveness of the subsystem for protecting confidential information in its design in the electronic document management systems of ATS: monograph Drovnikova I.G. etc. Voronezh: Voronezh. in-t of the Ministry of internal Affairs of Russia, 2019. – 116 p. URL:https:// catalog.inforeg.ru/ Inet/GetEzineByID/325482 (accessed: 21.01.2020) (in Russian).

[12] Radko N.M. Risk models of information and telecommunication systems in the implementation of remote and direct access threats N.M. Radko, I.O. Skobelev. M: Radiosoft, 2015. – 232 p. URL:http://www.sozvezdie.su/science/izdaniya/riskmodeli_informatsionnotelekommunikatsionnih/ (accessed: 24.01.2020) (in Russian).

[13] Bokova, O. I., Drovnikova, I. G., Etepnev, A. S., Rogozin, E. A., & Khvostov, V. A. (2019). Methods of Estimating Reliability of Information Security Systems which Protect from Unauthorized Access in Automated Systems. SPIIRAS Proceedings, 18(6), 1301–1332. DOI: https://doi.org/10.15622/sp.2019.18.6.1301-1332 (in Russian).

[14] M. El Hassan Charaf and S. Azzouzi, "A colored Petri-net model for control execution of distributed systems," 2017 4th International Conference on Control, Decision and Information Technologies (CoDIT), Barcelona, 2017. P. 0277–0282. DOI: https://doi.org/10.1109/CoDIT.2017.8102604.

[15] L. Yao, P. Dong, T. Zheng, H. Zhang, X. Du and M. Guizani, "Network security analyzing and modeling based on Petri net and Attack tree for SDN," 2016 International Conference on Computing, Networking and Communications (ICNC), Kauai, HI, 2016. P. 1–5. DOI: https://doi.org/10.1109/ICCNC.2016.7440631.

[16] Drovnikova I.G. Creating a model of information conflict «violator – protection system» based on the Petri-Markov network I.G. Drovnikova, M.S. Solomatin, E.A. Rogozin. Vestnik of the Voronezh Institute of the Ministry of internal Affairs of Russia. 2019. № 2. P. 93-100. URL:https://ви.мвд.рф/upload/site132/document_journal/Vestnik_2_2019.pdf (accessed: 20.01.2020) (in Russian).

Поступила в редакцию – 14 февраля 2020 г. Окончательный вариант – 17 августа 2020 г.
Received – February 14, 2020. The final version – August 17, 2020.

Анатолий П. Дураковский[1], Леонид Н. Кессаринский[2], Алексей О. Ширин[3]
[1,2,3]Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, Москва, 115409, Россия
[1]e-mail: APDurakovskiy@mephi.ru, https://orcid.org/0000-0002-8311-7735
[2]e-mail: LNKessarinskiy@mephi.ru, https://orcid.org/0000-0001-7756-6166
[3]e-mail: Aoshir@spels.ru, https://orcid.org/0000-0001-9121-0529

МАРКИРОВКА И ПРОВЕРКА ПОДЛИННОСТИ ИЗДЕЛИЙ МИКРОЭЛЕКТРОНИКИ НА ОСНОВЕ НЕКЛОНИРУЕМОСТИ РАДИАЦИОННОГО ПОВЕДЕНИЯ

DOI: http://dx.doi.org/10.26583/bit.2020.3.02

Аннотация. Статья посвящена проблеме подделки электронных устройств. Постоянно растущие требования к характеристикам и функциональным возможностям изделий электронной компонентной базы (ЭКБ), применяющимся в ответственной аппаратуре (космических аппаратах, технике двойного и специального назначения, транспорте и т.д.), приводят к применению продукции коммерческой категории качества иностранного производства. Таким образом, возникает риск применения ЭКБ контрафактного происхождения, что определяет необходимость проводить испытания и исследования, подтверждающие аутентичность изделий. Но даже применение всего арсенала методов исследований не гарантирует 100% достоверности результата, подтверждающего аутентичность изделия. Кроме того, глобальная тенденция заключается в том, что количество поддельных микросхем (и не только микросхем) увеличивается, но эффективность методов обнаружения падает. Одним из методов борьбы с контрафакцией является маркировка подлинных компонентов. И самый безопасный для маркировки метод, основанный на физически неклонируемых функциях (ФНФ) т.е. таких свойств изделия, которые невозможно воспроизвести в следствие естественного разброса характеристик паразитных структур, неопределенности результатов случайных процессов технологии производства. Распределение амплитуд ионизационных откликов и радиационная деградация параметров по мере накопления поглощенной дозы является одной из таких ФНФ т.к. обладает нужными свойствами: невозможностью воспроизведения с одной стороны, и однородностью результатов в рамках одной партии микросхем или транзисторов с другой стороны. Поэтому предлагается использовать различные признаки ухудшения радиационного поведения в качестве ФНФ. Несколько примеров такого использования представлены в статье.

Ключевые слова: электроника, подделка, контрафакт, радиация, чипы, физически неклонируемая функция.

Для цитирования: ДУРАКОВСКИЙ, Анатолий П.; КЕССАРИНСКИЙ, Леонид Н.; ШИРИН, Алексей О. МАРКИРОВКА И ПРОВЕРКА ПОДЛИННОСТИ ИЗДЕЛИЙ МИКРОЭЛЕКТРОНИКИ НА ОСНОВЕ НЕКЛОНИРУЕМОСТИ РАДИАЦИОННОГО ПОВЕДЕНИЯ. Безопасность информационных технологий, [S.l.], v. 27, n. 3, p. 18–25, 2020. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1289>. Дата доступа: 08 sep. 2020. DOI: http://dx.doi.org/10.26583/bit.2020.3.02.

Anatoly P. Durakovskiy[1], Leonid N. Kessarinskiy[2], Alexey O. Shirin[3]
[1,2]National Research Nuclear University MEPhI
Kashirskoye shosse, 31, Moscow, 115409, Russia
[1]e-mail: APDurakovskiy@mephi.ru, https://orcid.org/0000-0002-8311-7735
[2]e-mail: LNKessarinskiy@mephi.ru, https://orcid.org/0000-0001-7756-6166
[3]e-mail: Aoshir@spels.ru, https://orcid.org/0000-0001-9121-0529

The use of microelectronics radiation behavior as physical uncloned function to find counterfeit

DOI: http://dx.doi.org/10.26583/bit.2020.3.02

Abstract. The study is devoted to the problem of counterfeiting electronic devices. The constantly increasing requirements for the characteristics and functionality of electronic components for critical equipment (spacecraft, dual-purpose and special-purpose equipment, transport, etc.) lead to the use of foreign-made commercial products. Thus, there is a risk of using counterfeit electronic components, which determines the need to provide tests to the authenticity confirmation. But even the use of the entire arsenal of research methods does not guarantee 100% authenticity of the product. In addition, the global trend is that the number of counterfeit microcircuits (and not only ICs) is increasing, but the effectiveness of detection methods is falling. One of the methods used to combat counterfeiting is the marking of genuine components. And the safest method for marking is based on physical unclonable functions (PUF) i.e. such properties of the product that cannot be reproduced due to the natural spread of the characteristics of parasitic structures, and the uncertainty of the results of random processes of production technology. The distribution of the amplitudes of ionization responses and the radiation degradation of parameters with the accumulation of the absorbed dose is one of such PUFs because possesses the necessary properties: the impossibility of reproduction on the one hand, and uniformity of results within one batch of microcircuits or transistors on the other hand. Therefore, it is proposed to use various signatures of deterioration of radiation behavior as PUF. Several examples of this use are presented in the paper.
Keywords: electronics, counterfeit, radiation, chips, physical uncloned function.
For citation: DURAKOVSKIY, Anatoly P.; KESSARINSKIY, Leonid N.; SHIRIN, Alexey O. The use of microelectronics radiation behavior asphysical uncloned function to find counterfeit. IT Security (Russia), [S.l.], v. 27, n. 3, p. 18-25, 2020. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1289>. Date accessed: 08 sep. 2020. DOI: http://dx.doi.org/10.26583/bit.2020.3.02.

Введение

Как известно, вся микроэлектроника делится на 4 основных класса: коммерческая, промышленная, военная и космическая. В соответствии с назначением, большинство техники ответственного применения традиционно комплектуется изделиями соответствующего класса. Однако общая тенденция к усложнению аппаратуры, расширению функциональных возможностей, рост требований к различным показателям эффективности (энергопотребление и энергосохранение, КПД, плотность мощности и др.) привела к массовому использованию в военной и космической технике ЭКБ промышленного или даже коммерческого класса качества. С другой стороны, географическое разделение центров разработки и производства изделий ЭКБ с переносом производственных и утилизационных мощностей в страны Азии стало дополнительной причиной резкого обострения проблемы контрафакта [1–4].

Рост доли контрафактной микроэлектроники за последние годы стал мировой проблемой. Созданы международные технические комитеты и группы исследователей по разработке общей стратегии по борьбе с контрафактом, воплотившихся в стандарты AS5553, AS6171, AS6081 и др. Стратегия борьбы с контрафактом сводится к доверенным путям поставки ЭКБ и проверке на наличие признаков контрафакта в испытательных лабораториях. Несмотря ни на что доля контрафактных микросхем растет, качество подделок постоянно увеличивается, что усложняет процесс их выявления. Согласно версии AS6171A (2018 г.) вероятность выявления некоторых типов контрафакта (например, клонирования) составляет всего несколько процентов, даже при использовании всех известных методов проверок (более 30) [5–10]. Что делать? Одной из эффективных стратегий решения этой проблемы является маркировать изделия ЭКБ на основе так называемых физически неклонируемых функций.

1. Физически неклонируемые функции

Несмотря на строгость правил технологического процесса изготовления серийной микроэлектроники, естественный разброс параметров, характеристики паразитных

структур, неконтролируемые параметры внешней среды создают уникальные элементы конструкции изделия ЭКБ, которые невозможно подделать. Принцип маркировки ЭКБ для последующей идентификации на основе таких элементов называется принципом аутентификации на основе ФНФ. Существует несколько идей и реализаций процесса аутентификации на основе ФНФ. Все их объединяет выполнение нескольких правил:

1. Реализация элемента с ФНФ не должна влиять на основное функционирование изделия. Лучше всего, если такие элементы будут «сами собой» существовать в любом изделии без приложения дополнительных усилий проектировщиков.
2. Проверяемые характеристики элемента с ФНФ нельзя подделать или воспроизвести. Они должны быть основаны на случайных процессах.
3. Результаты проверки (измерения) характеристик элементов с ФНФ должны иметь свойство воспроизводиться независимо от лаборатории или производителя измерительного оборудования.
4. Результаты проверки (измерения) характеристик элементов с ФНФ должны иметь возможность дать однозначный ответ: подлинное изделие или контрафактное. Не важно на основе сравнения с прогнозируемым результатом, эталонными значениям или результатом сравнения с эталонным образцом.

Одной из таких ФНФ является радиационное поведение изделия ЭКБ. Реализация такой ФНФ внутри микросхем или мощных дискретных приборов не требует создания специальных блоков. Радиационное поведение для современных технологических процессов определяется деградацией характеристик, связанных с паразитными структурами и связанными с ними параметрами ЭКБ [11–12].

2. Радиационное поведение как физически неклонируемая функция

Примеры применения радиационного поведения в качестве характеристик ФНФ приведены ниже. Недостатком использования радиационного поведения в качестве ФНФ для аутентификации является то, что это разрушающее испытаний и придется жертвовать образцом. Однако, примерно половина методов выявления контрафакта, перечисленных в AS6171 также являются разрушающими (например, проверка перемаркировки), что не мешает их комбинировать и проводить на одних и тех же образцах.

Приведем примеры использования радиационного поведения в качестве ФНФ для определения неоднородных образцов в выборке.

Мощные МОП транзисторы (МОПТ) IRFNG50 фирмы International Rectifier. Две партии производства: 0842 Мексика и 1038 США. С точки зрения функционирования и параметры образцов МОПТ соответствуют нормам из datasheet. Реализация ФНФ заключается в измерении деградации порогового напряжения отпирания транзистора в зависимости от накопленной дозы. Графики зависимостей приведены на рис. 1 и 2. Горизонтальной чертой на графике показано предельное значение параметра (не менее 2В), которое допускается документацией, а пересечение ее является критерием параметрического отказа образца [13].

Результаты измерения деградации порогового напряжения от поглощенной дозы в ходе радиационного воздействия позволяет сделать два вывода: для одной партии различий между образцами нет, для любых образцов из разных партий – различия существенные и позволяют однозначно отнести их к нужной партии.

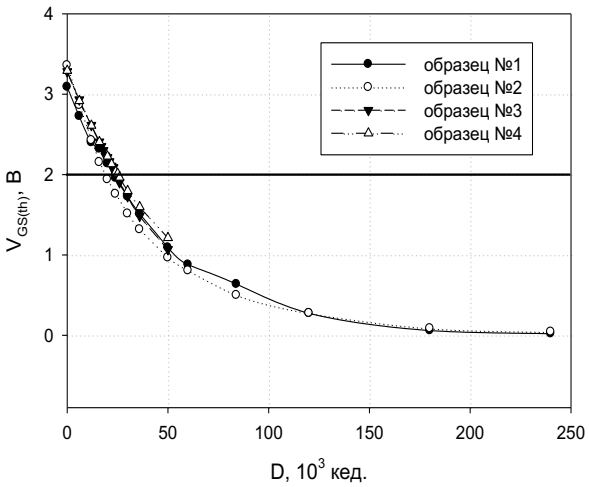


Рис. 1. Зависимость порогового напряжения транзисторов IRFNG50 партии 0842 (Мексика) от уровня поглощенной дозы

Fig. 1. Dependence of threshold voltage of IRFNG50 transistors batch 0842 (Mexico) on the level of absorbed dose

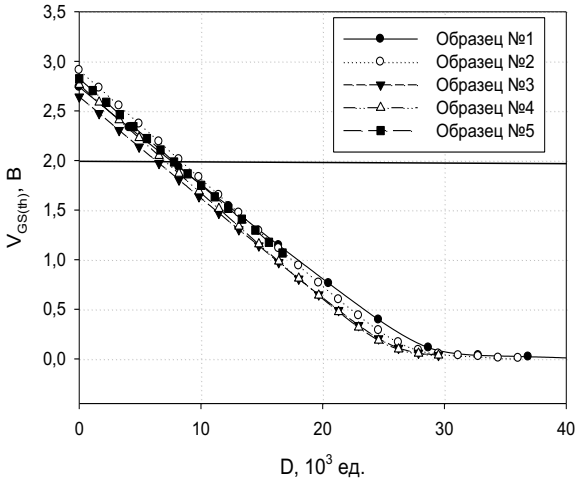
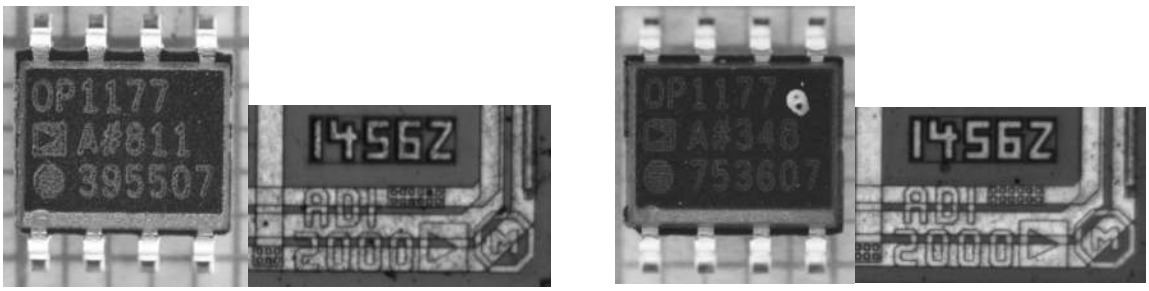


Рис. 2. Зависимость порогового напряжения транзисторов IRFNG50 партии 1038 (США) от уровня поглощенной дозы.

Fig. 2. Dependence of threshold voltage of IRFNG50 transistors batch 1038 (USA) on the level of absorbed dose

Операционный усилитель OP1177ARZ фирмы Analog Devices. Были исследованы 4 партии разных лет производства: 2008, 2010, 2012, 2013. За исключением даты производства, внешне образцы выглядят одинаковыми по внешнему виду, по характеристикам и по меткам на кристаллах [14]. На рис. 3 приведены примеры для двух партий 2008 и 2013 годы.

Реализация ФНФ заключалась в снятии карт ионизационного отклика кристаллов микросхем. Процедура выполняется следующим образом. Сначала выполняется проверка параметров образцов, чтобы убедиться в их годности. Затем часть пластикового корпуса над кристаллом химически стравливается. Открытый кристалл начинает подвергаться сканирующему воздействию сфокусированного (диаметр 10 мкм, длительность 10 пс, длина волны 1,06 мкм) лазерного луча одновременно с фиксацией всплеска тока по цепям питания микросхемы.



п.395507 п.753607

Рис. 3. Внешний вид корпусов и маркировка кристаллов OP1177ARZ

Fig. 3. Appearance of cases and marking of OP1177ARZ crystals

Объединение данных о месте выстрела лазером и амплитудой отклика составляет карту ионизационного отклика, которая фактически показывает взаимосвязь нескольких физических процессов и их характеристик: (а) локальной области кристалла (на которое

происходит воздействие сфокусированного излучения), (б) механизмом и особенностями сбора сгенерированного избыточного заряда (с учетом локального профиля легирования кремния, геометрии и топологии областей, переотражения лазерного излучения от слоев металлизации, первичной рекомбинации и т.д.), (в) движением этого заряд от места генерации до исследуемых выводов микросхемы (с учетом потерь по мере движения, рекомбинацией, перезарядом паразитных реактивностей). С учетом огромного количества непредсказуемых внутренних факторов (в том числе паразитных элементов), влияющих на итоговую форму отклика на выводах микросхемы, карту ионизационного отклика можно считать еще одной реализацией физически неклонируемой функции.

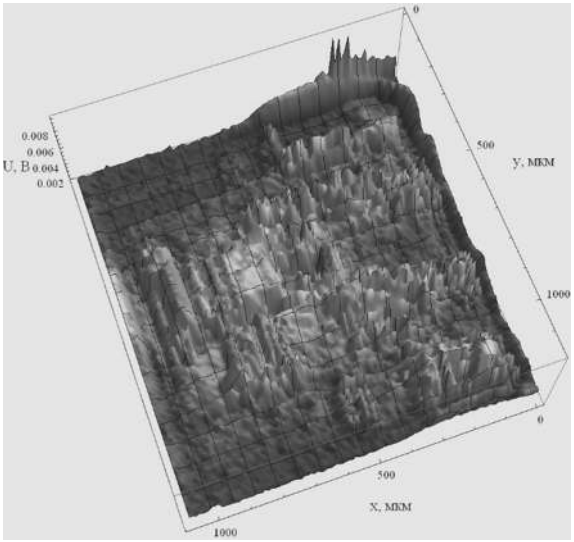


Рис. 4. 3D-карта ионизационного отклика n.395507
Fig. 4. 3D map of the ionization response b. 395507

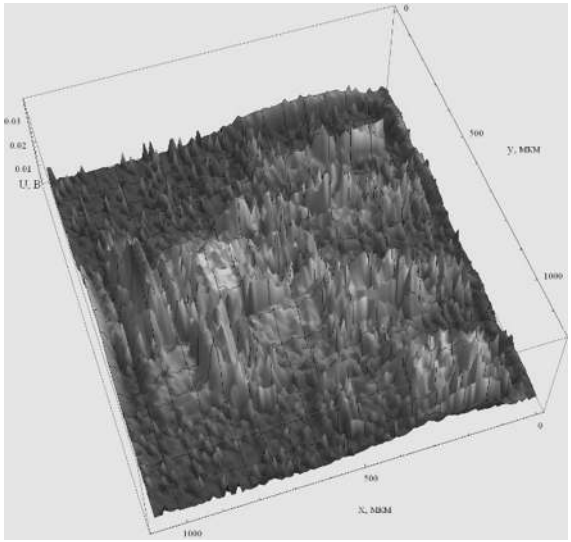


Рис. 5. 3D-карта ионизационного отклика n. 753607
Fig. 5. 3D map of the ionization response b. 753607

На рис. 4 и 5 приведены карты отклика для разных партий микросхем OP1177ARZ. После проведенных исследований не остается сомнений в отличии топологии и технологии изготовления партии 395507 от партии 753607, как на поверхности, так и внутри кристалла (см. рис. 6.). Это в дальнейшем было подтверждено детальным анализом топологии кристаллов в месте наиболее значимого различия карт отклика.

a) b)

Рис. 6. Фотография кристалла OP1177ARZ. a) область 1 партии 395507; b) область 1 партии 753607
Fig. 6. Photo of OP1177ARZ crystal. a) area of 1st batch 395507; b) area of 1st batch 753607

Таким образом, карта ионизационного отклика – вариант реализации ФНФ в ходе полностью автоматического сканирования независимо от функционального назначения изделия. Его преимущество по сравнению с послойным травлением и сравнением металлизации с эталоном в том, что ионизационный отклик формируется одновременно и картой металлизации (определяет долю лазерного излучения, доходящую до кремниевых областей), и топологией самих кремниевых областей кристалла (анализ которых обычно ограничен для визуального сравнения топологии).

Заключение

Испытания изделий микроэлектроники на выявление признаков является одним из составляющих стратегии противостоянию контрафакту. Но, к сожалению, даже применение всех методов выявления не обеспечивает 100% гарантию того, что проверенное изделие является подлинным.

Выходом из такой ситуации служит аутентификация образцов на основе физически неклонируемых функций.

В статье изложены примеры реализации аутентификации образцов ЭКБ на основе ФНФ – радиационного поведения изделий. В качестве примеров приведены данные для мощных полупроводниковых приборов, аналоговых микросхем низкой степени интеграции.

Поскольку радиационные испытания являются одним из обязательных видов испытаний ЭКБ, для проверки соответствия условиям работы аппаратуры в условиях, например, космической радиации – использование полученных данных о радиационном поведении изделий для аутентификации является дополнительным результатом проводимых исследований.

СПИСОК ЛИТЕРАТУРЫ:

1. Jo Vann, Supplier anti-counterfeit requirements, report of IEC TC107 WG3. March 2018. URL:https://www.caa.co.uk/uploadedFiles/CAA/Content/Standard_Content/Commercial_industry/Aircraft/Airworthiness/Seminars/Production_Organisations_28th_March_2018/IECQ%20Anti-Counterfeit%20Standards%20-%20Jo%20Vann.pdf (дата обращения: 15.08.2020).
2. U.S. Dept. of Comm., Defense Industrial Base Assessment: Counterfeit Electronics (2010). P. 179. URL: https://docplayer.net/398759-Defense-industrial-base-assessment-counterfeit-electronics.html (дата обращения: 15.08.2020).
3. Farinaz Koushanfar, Saverio Fazzari, Carl McCants, William Bryson, Matthew Sale, Peilin Song, and Miodrag Potkonjak. 2012. Can EDA combat the rise of electronic counterfeiting? In Proceedings of the 49th Annual Design Automation Conference (DAC '12). Association for Computing Machinery, New York, NY, USA, 133–138. DOI: https://doi.org/10.1145/2228360.2228386
4. Alkabani Y., Koushanfar F., Kiyavash N., Potkonjak M. (2008) Trusted Integrated Circuits: A Nondestructive Hidden Characteristics Extraction Approach. In: Solanki K., Sullivan K., Madhow U. (eds) Information Hiding. IH 2008. Lecture Notes in Computer Science. Vol 5284. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/978-3-540-88961-8_8.
5. Gassend, B., Lim, D., Clarke, D., Van Dijk, M., & Devadas, S. (2004). Identification and authentication of integrated circuits. Concurrency Computation Practice and Experience, 16(11), 1077–1098. DOI: https://doi.org/10.1002/cpe.805.
6. S. Pope, "Trusted Integrated Circuit Strategy," in IEEE Transactions on Components and Packaging Technologies. Vol. 31, no. 1. P. 230–234, March 2008. DOI: https://doi.org/10.1109/TCAPT.2008.918319.
7. Дураковский А.П., Кессаринский Л.Н, Ширин А.О., Артамонов А.С., Бойченко Д.В., Тайибов Ф.Ф. Идентификация элементной компонентной базы с целью исключения контрафакта и анализа результатов радиационных испытаний. Актуальные направления развития систем охраны, специальной связи и информации для нужд органов государственной власти Российской Федерации: XI Всероссийская межведомственная научная конференция: материалы и доклады (Орёл, 5–6 февраля 2019 года). В 10 ч. Ч. 5 / под общ. ред. П. Л. Малышева. – Орёл: Академия ФСО России, 2019. С. 65–67

8. Кессаринский, Леонид Н. и др. Идентификация элементной компонентной базы киберфизических систем. Безопасность информационных технологий, [S.l.], № 3. С. 67–78, 2018. ISSN 2074-7136. URL: (дата обращения: 12.02.2019). doi:http://dx.doi.org/10.26583/bit.2018.3.07.
9. Кессаринский, Леонид Н. и др. Выявление признаков контрафакта в изделиях электронной компонентной базы в аспекте обеспечения промышленной кибербезопасности. Безопасность информационных технологий, [S.2.], № 2. С. 117–128, 2019. ISSN 2074-7136. URL: (дата обращения: 01.11.2019).
10. Дураковский А.П., Кессаринский Л.Н, Ширин А.О. Развитие терминологии нормативной базы испытаний на выявление признаков контрафакта в изделиях электронной компонентной базы аппаратуры объектов критической информационной инфраструктуры. Безопасность информационных технологий, [S.1.], № 1. С. 19–27, 2020. ISSN 2074-7136. URL: (дата обращения: 02.12.2019)
11. A.Y. Nikiforov et al., "Basic trends in electronic components product range development: Radiation hardness aspects," 2017 IEEE 30th International Conference on Microelectronics (MIEL), Nis, 2017. P. 45–48. DOI: https://doi.org/10.1109/MIEL.2017.8190066.
12. A. Borisov, M. Belova, L. Kessarinskiy, D. Boychenko, and A. Nikiforov “Analysis of total dose effects in modern analog ICs”, RAD Conference Proceedings vol. 2015-June. P. 427–431, 2015. URL:http://apps.webofknowledge.com/InboundService.do?product=WOS&Func=Frame&SrcApp=Alerting&SrcAuth=Alerting&secure=false&locale=en_US&SID=D43b5tW6hoBz151lRqN&customersID=Alerting&mode=FullRecord&IsProductCode=Yes&Init=Yes&Alias=WOK5&action=retrieve&UT=WOS%3A000387979700088 (дата обращения: 15.08.2020).
13. N.E. Aristova, A.Y. Borisov, A.S. Tararaksin, L.N. Kessarinskiy and A.V. Yanenko, "Automatic test complex for parametric control of power NMOS and PMOS transistors," 2015 International Siberian Conference on Control and Communications (SIBCON), Omsk, 2015. P. 1–4. DOI: https://doi.org/10.1109/SIBCON.2015.7146984.
14. A. Demidova, A. Pechenkin, A. Borisov, L. Kessarinskiy, D. Boychenko, and A. Yanenko “Identification of IC chips by ionization response comparison on the example of OP1177”, RAD Conference Proceedings vol. 2015-June. P. 409–411, 2015. URL:http://apps.webofknowledge.com/InboundService.do?customersID=Alerting&mode=FullRecord&IsProductCode=Yes&product=WOS&Init=Yes&Func=Frame&DestFail=http%3A%2F%2Fwww.webofknowledge.com&action=retrieve&SrcApp=Alerting&SrcAuth=Alerting&SID=D43b5tW6hoBz151lRqN&UT=WOS%3A000387979700084 (дата обращения: 15.08.2020).

REFERENCES:

[1] Jo Vann, Supplier anti-counterfeit requirements, report of IEC TC107 WG3. March 2018. URL:https://www.caa.co.uk/uploadedFiles/CAA/Content/Standard_Content/Commercial_industry/Aircraft/Airworthiness/Seminars/Production_Organisations_28th_March_2018/IECQ%20Anti-Counterfeit%20Standards%20-%20Jo%20Vann.pdf (accessed: 15.08.2020).
[2] U.S. Dept. of Comm., Defense Industrial Base Assessment: Counterfeit Electronics (2010). P. 179. URL: https://docplayer.net/398759-Defense-industrial-base-assessment-counterfeit-electronics.html (accessed: 15.08.2020).
[3] Farinaz Koushanfar, Saverio Fazzari, Carl McCants, William Bryson, Matthew Sale, Peilin Song, and Miodrag Potkonjak. 2012. Can EDA combat the rise of electronic counterfeiting? In Proceedings of the 49th Annual Design Automation Conference (DAC '12). Association for Computing Machinery, New York, NY, USA, 133–138. DOI: https://doi.org/10.1145/2228360.2228386
[4] Alkabani Y., Koushanfar F., Kiyavash N., Potkonjak M. (2008) Trusted Integrated Circuits: A Nondestructive Hidden Characteristics Extraction Approach. In: Solanki K., Sullivan K., Madhow U. (eds) Information Hiding. IH 2008. Lecture Notes in Computer Science. Vol 5284. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/978-3-540-88961-8_8.
[5] Gassend, B., Lim, D., Clarke, D., Van Dijk, M., & Devadas, S. (2004). Identification and authentication of integrated circuits. Concurrency Computation Practice and Experience, 16(11), 1077–1098. DOI: https://doi.org/10.1002/cpe.805.
[6] S. Pope, "Trusted Integrated Circuit Strategy," in IEEE Transactions on Components and Packaging Technologies. Vol. 31, no. 1. P. 230–234, March 2008. DOI: https://doi.org/10.1109/TCAPT.2008.918319.
[7] Durakovskiy A.P., Kessarinskiy L.N, Shirin A.O., Artamonov A.S., Boychenko D.V., Tayibov F.F. Identification of the element component base in order to eliminate counterfeit and analyze the results of radiation tests. Aktual'nyye napravleniya razvitiya sistem okhrany, spetsial'noy svyazi i informatsii dlya nuzhd organov

gosudarstvennoy vlasti Rossiyskoy Federatsii: XI Vserossiyskaya mezhvedomstvennaya nauchnaya konferentsiya: materialy i doklady (Orel, February 5–6, 2019). V 10 ch. Ch. 5 pod obshch. red. P.L. Malysheva. – Orel: Akademiya FSO Rossii, 2019. P. 65–67 (in Russian).

[8] Kessarinskiy, Leonid N. et al. Authentication of electronics components for cyber-physical systems. IT Security (Russia), [S.l.], n. 3. P. 67–78, 2018. ISSN 2074-7136. URL: <https://bit.mephi.ru/index.php/bit/article/view/1141> (accessed: 12.02.2019). doi:http://dx.doi.org/10.26583/bit.2018.3.07 (in Russian).

[9] Kessarinskiy, Leonid N. et al. Counterfeit electronic components identifying methods in terms of industrial cyber security IT Security (Russia), [S.2.], n. 2. P. 117–128, 2018. ISSN 2074-7136. URL: <https://bit.mephi.ru/index.php/bit/article/view/1204> (accessed: 01.11.2019).

[10] Durakovskiy A.P., Kessarinskiy L.N, Shirin A.O. Terms and definitions base development for counterfeit electronics test for critical information infrastructure object**sю** IT Security (Russia), [S.1.], n. 1. P. 19-27, 2020. ISSN 2074-7136. URL: <https://bit.mephi.ru/index.php/bit/article/view/1249> (accessed: 02.12.2019).

[11] A.Y. Nikiforov et al., "Basic trends in electronic components product range development: Radiation hardness aspects," 2017 IEEE 30th International Conference on Microelectronics (MIEL), Nis, 2017. P. 45–48. DOI: https://doi.org/10.1109/MIEL.2017.8190066.

[12] A. Borisov, M. Belova, L. Kessarinskiy, D. Boychenko, and A. Nikiforov “Analysis of total dose effects in modern analog ICs”, RAD Conference Proceedings vol. 2015-June. P. 427–431, 2015. URL:http://apps.webofknowledge.com/InboundService.do?product=WOS&Func=Frame&SrcApp=Alerting&SrcAuth=Alerting&secure=false&locale=en_US&SID=D43b5tW6hoBz151lRqN&customersID=Alerting&mode=FullRecord&IsProductCode=Yes&Init=Yes&Alias=WOK5&action=retrieve&UT=WOS%3A000387979700088 (accessed: 15.08.2020).

[13] N.E. Aristova, A.Y. Borisov, A.S. Tararaksin, L.N. Kessarinskiy and A.V. Yanenko, "Automatic test complex for parametric control of power NMOS and PMOS transistors," 2015 International Siberian Conference on Control and Communications (SIBCON), Omsk, 2015. P. 1–4. DOI: https://doi.org/10.1109/SIBCON.2015.7146984.

[14] A. Demidova, A. Pechenkin, A. Borisov, L. Kessarinskiy, D. Boychenko, and A. Yanenko “Identification of IC chips by ionization response comparison on the example of OP1177”, RAD Conference Proceedings vol. 2015-June. P.409–411, 2015. URL:http://apps.webofknowledge.com/InboundService.do?customersID=Alerting&mode=FullRecord&IsProductCode=Yes&product=WOS&Init=Yes&Func=Frame&DestFail=http%3A%2F%2Fwww.webofknowledge.com&action=retrieve&SrcApp=Alerting&SrcAuth=Alerting&SID=D43b5tW6hoBz151lRqN&UT=WOS%3A000387979700084 (accessed: 15.08.2020).

Поступила в редакцию - 9 июля 2020 г. Окончательный вариант - 21 августа 2020 г.
Received - July 09, 2020. The final version - August 21, 2020.

Рустем В. Пенерджи[1], Григорий П. Гавдан[2]
[1,2]Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, Москва, 115409, Россия
[1]e-mail: Prv0@yandex.ru, https://orcid.org/0000-0003-4105-2221
[2]e-mail: GPGavdan@mephi.ru, https://orcid.org/0000-0003-3185-3076

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

DOI: http://dx.doi.org/10.26583/bit.2020.3.03

Аннотация. Целью статьи является рассмотрение вопросов связанных с обеспечением безопасности государственных информационных систем в Российской Федерации. Актуальность этих вопросов обусловлена в первую очередь тем, что с каждым годом в России не уменьшается число кибератак (наносящих значительный ущерб государству) на различные сферы её экономики, в том числе, на её государственные информационные системы. Несколько лет назад начала реализацию национальная инициатива в области кибербезопасности – NICE (*«The National Initiative for Cybersecurity Education»*), что не обойдено вниманием российских и других специалистов в области информационной безопасности. К основным направлениям защиты информационной собственности отнесены: охрана (государственной, служебной, коммерческой, банковской, налоговой, страхования, персональных данных и др.) тайн и интеллектуальная собственность. Государственные информационные системы (ГИС) включают информационно-технологические средства и системы, при создании которых опираются на передовые научные изыскания, такие как знания, передовые технологии (ноу-хау) и др. и являются неотъемлемой частью и достаточно сложной системы государственного управления. Предметом исследования являются ГИС, как основа управления государственных органов. В работе первоочередное внимание уделено современным тенденциям в области обеспечения защиты информации ГИС, краткому обзору законодательства в области ГИС и критической информационной инфраструктуре.
Ключевые слова: государственная информационная система, государственное управление, информационная система, информационная собственность, критическая информационная инфраструктура.
Для цитирования: ПЕНЕРДЖИ, Рустем В.; ГАВДАН, Григорий П. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ. Безопасность информационных технологий, [S.l.], v. 27, n. 3, p. 26–42, 2020. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1290>. Дата доступа: 01 sep. 2020. DOI: http://dx.doi.org/10.26583/bit.2020.3.03.

Rustem V. Penerdji[1], Grigory P. Gavdan[2]
[1,2]National Nuclear Research University MEPHI (Moscow Engineering Physics Institute),
Kashirskoe sh., 31, Moscow, 115409, Russia
[1]e-mail: Prv0@yandex.ru, https://orcid.org/0000-0003-4105-2221
[2]e-mail: GPGavdan@mephi.ru, https://orcid.org/0000-0003-3185-3076

Information security of state information systems

DOI: http://dx.doi.org/10.26583/bit.2020.3.03

Abstract. The purpose of the paper is to consider issues related to the security of state information systems in the Russian Federation. The relevance of these issues is primarily due to the fact that the number of cyber-attacks (causing significant damage to the state) on various areas of its economy, including its state information systems, is increasing every year in Russia. For example, the national initiative for Cybersecurity Education (NICE) was launched in the United States several years ago. This event has not escaped the attention of Russian and other experts in the field of information security (is). The main areas of information property protection include: protection (state, official, commercial, banking, tax, insurance, personal data (PD), etc.) of secrets and intellectual property. State information systems include information technology tools and systems that rely on advanced scientific research, such as knowledge, advanced

technologies (know-how), etc. Today, state information systems are an integral part of a fairly complex system of public administration. It is also important to recall the role of the Russian FSTEC regulator in ensuring information security. The subject of the research is SIS as the basis of management of state bodies. The paper focuses on current trends in the field of SIS information security, a brief overview of SIS legislation, and the critical information infrastructure (CII) of Russia's main geopolitical opponent. The main arguments for the importance of the chosen direction of work are discussed. Further research is expected to be conducted in the field of SIS security in an uncertain environment.
Keywords: state information system, public administration, information system, information property, critical information system.
For citation: PENERDJI, Rustem V.; GAVDAN, Grigory P. Information security of state information systems. IT Security (Russia), [S.l.], v. 27, n. 3, p. 26–42, 2020. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1290>. Date accessed: 01 sep. 2020. DOI: http://dx.doi.org/10.26583/bit.2020.3.03.

Введение

Тенденции развития мирового сообщества и происходящие в мире процессы геополитического характера действительно не являются случайными. Ведущие мировые державы (такие, например, как США, Великобритания, Евросоюз, Китай, Россия и др.) и «закулисная мировая элита», оказывают существенное влияние на их формирование. Между этими оппонентами (игроками) существует геополитическое противоборство, в том числе и информационное. От этого всем этим сторонам никуда не уйти, как бы этого всем не хотелось бы. Государственные информационные системы (ст.14)[1] создаются в целях реализации полномочий государственных органов и обеспечения обмена информацией между этими органами, а также в иных установленных федеральными законами целях. ГИС являются неотъемлемой частью сложной системы управления государства, которая способна обеспечить свою бесперебойную работу и должное её функционирование.

Практически каждое ведомство или министерство Российской Федерации ведут свои реестры и собирают информацию по своему профилю в рамках обозначенной деятельности. Например, Федеральная налоговая служба автоматизировала процедуру сбора налоговой отчетности и фискальных проверок и др. в режиме он-лайн; автоматизирована процедура закупок для государственных нужд посредством ведения всеми участниками единых ИС. Системы постоянно модифицируются и обновляются. Например, Государственные (Пенсионный, социального страхования, медицинского страхования и др.) фонды также ведут свои БД и соответствующие реестры и т.д. [1].

Государственные органы (ГО), организующие должное функционирование ГИС, в свою очередь обязаны предоставить необходимый доступ к информации (обеспечить её достоверность, доступность, целостность, аутентичность, актуальность и др.) в порядке, предусмотренном законодательством РФ и обеспечить требуемую защиту (информации ограниченного доступа) от модифицирования, уничтожения, неправомерного доступа, блокирования, копирования и иных неправомерных действий [2]. ГИС и др. ИС, где компрометация информационных систем может иметь весьма тяжёлые последствия является тому подтверждением и не может не привлекать к себе внимание.

К основным направлениям защиты информационной собственности относят: охрану (государственной, служебной, коммерческой, банковской, медицинской, персональных и др.) тайн и интеллектуальную собственность. Ситуации, когда, по словам секретаря Совета безопасности Российской Федерации Патрушева Н.П., основными целями иностранных спецслужб по-прежнему остаются объекты КИИ РФ (критической информационной

[1]Федеральный Закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» в редакции от 18 марта 2019 г.

инфраструктуры) [3], компрометация подобных информационных систем может иметь весьма тяжёлые последствия.

Затруднения, возникающие при обеспечении ИБ современных информационных систем, во многом связаны, с:

– задержкой внесения изменений (например, в ходе обнаружения новых факторов риска) при включении их в нормативно-правовые акты (НПА) в области обеспечения безопасности информации и отсутствием соответствия между этими НПА;

– субъективностью экспертных оценок, возникающей при формировании модели угроз безопасности ИС и увеличивающейся при этом степенью неопределённости модели угроз;

– частым обнаружением новых уязвимостей и угроз в программном и аппаратном обеспечении ИС.

В соответствии с базовым законом[1] в области информатизации, информационных технологий (ИТ) и защите информации (ЗИ), информация, содержащаяся в ГИС, а также иные имеющиеся в распоряжении ГО сведения и документы являются национальными (государственными) информационными ресурсами [2]. Например, в РФ только в органах государственной власти (ОГВ) федерального и регионального уровней накоплен значительный объем информационных фондов (ИФ), объединяющих десятки тысяч баз данных (БД) [2], которые в области их защиты также требуют к себе должного внимания.

Остановимся на государственных информационных системах. Рассмотрим современные тенденции в сфере обеспечения безопасности информации и проведем их анализ.

1. Анализ современных тенденций в сфере обеспечения безопасности информации

Существующие проблемы обеспечения информационной безопасности информационных систем в РФ (в том числе и ГИС) подтверждаются:

проводимыми исследованиями (например, минимизация рисков ИБ [4], оценка рисков на основе графов атак для систем управления ИБ [5], оценка угроз безопасности ИС персональных данных (ПД) [6], обеспечение требуемой защищенности информационно-телекоммуникационных узлов [7], многофакторная классификация угроз информационной безопасности киберфизических систем [8]);

выступлениями (видеоконференции, конференции, форумы и т.д.) представителей государственных и коммерческих организаций (структур), работающих в области защиты информации и ИБ.

Программой «Цифровая экономика РФ»[2] предусматривается развитие не только в рамках совершенствования ИТ, но и в более широком смысле.

Развитие цифровой экономики охватывает восемь ключевых направлений [2], следуя логике Давосского проекта. Поэтому в настоящее время требуется не только внимание к «цифровизации общества», но и к принятию на уровне государства должных мер защиты.

1.1 Техническая проблематика

Различные отчёты отечественных и зарубежных компаний, связанные с вопросами ЗИ (ГИС, промышленные ИС и др.), подтверждают тот факт то, что за последнее время не снижается уровень компьютерных инцидентов.

Представленная на рис. 1 диаграмма распределения числа утечек по отраслям в 2017 году [9] показывает, что третье – четвертое места занимают силовые структуры и

[2]Программа «Цифровая экономика Российской Федерации», утверждена Распоряжением Правительства РФ от 28 июля 2017 г. № 1632-р.

государственные органы.

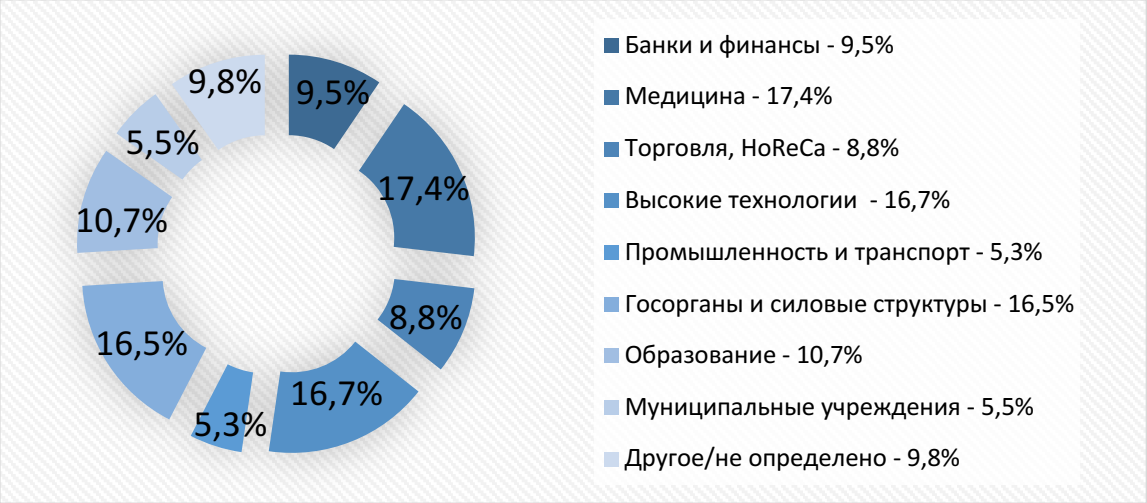


Рис. 1. Распределение числа утечек по отраслям, 2017 г.
(Fig. 1. Distribution of the number of leaks by industry, 2017)

Аналогичный отчёт за 2018 год для ГИС показывает также третье-четвертое место [10]. Диаграмма распределения числа утечек по отраслям в 2018 году [10] представлена на рис. 2.

Прогнозы по видоизменению угроз также предполагают увеличение компьютерных инцидентов с ИС. Так, например, по данным [11] основными проблемами в 2019 году были:

1) увеличение атак на промышленные ИС – за счет увеличения доступных к воздействию элементов;

2) возрастание интереса как киберпреступников, так и кибервойск;

3) недооценка общего уровня угроз: проблемы ИБ, как правило, не на слуху у широкой публики. У сотрудников же самих компаний господствует вера в непогрешимость систем аварийной защиты;

4) непонимание специфики угроз безопасности, характерных для промышленных систем и др. Этот факт подтверждается в [12].

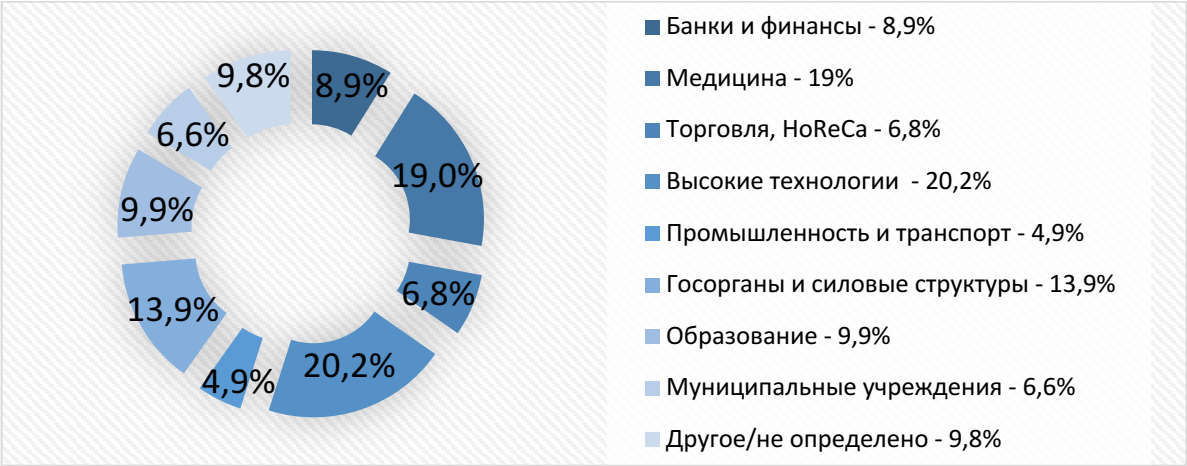


Рис. 2. Распределение числа утечек по отраслям, 2018 г.
(Fig. 2. Distribution of the number of leaks by industry, 2018)

Наиболее важными выводами являются:

1) непрекращающаяся тенденция увеличения числа уязвимостей в компонентах автоматизированных систем управления технологическими процессами (АСУ ТП) [12] (Рис. 3);

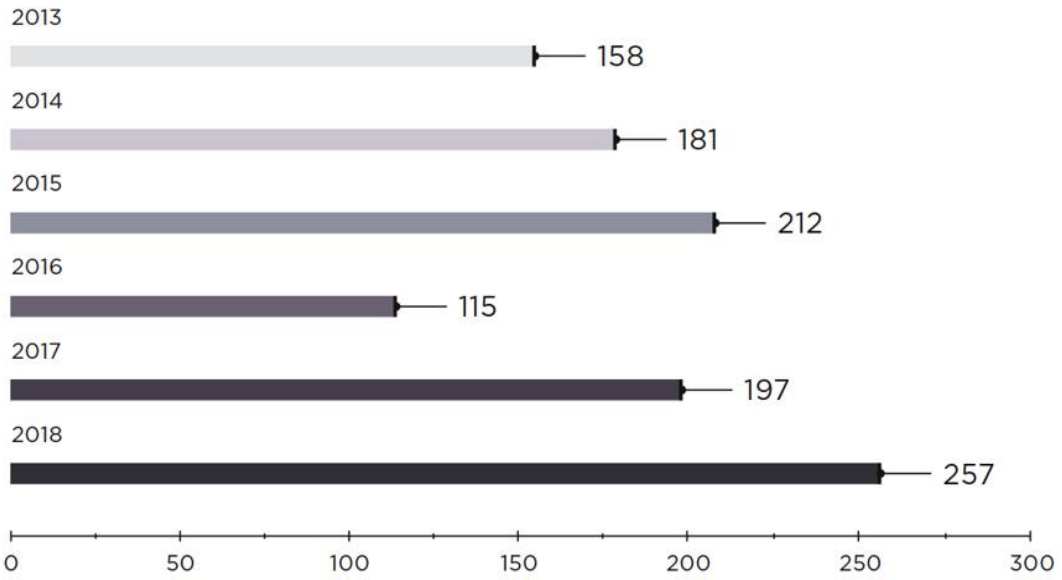


Рис. 3. Статистика обнаружения уязвимостей в компонентах АСУ ТП
(Fig. 3. The statistics of vulnerabilities in the components of the ACS of TP)

2) значительная доля уязвимостей критической и высокой степеней риска. Число уязвимостей, относящихся, в соответствии с оценкой стандарта Common Vulnerability Scoring System версии 3, к критическим и высоким степеням риска составили по итогам 2018 года, соответственно, 25% и 53% от общего числа обнаруженных уязвимостей. Соответствующая диаграмма степени риска обнаруженных уязвимостей приведена на рис. 4 [12].

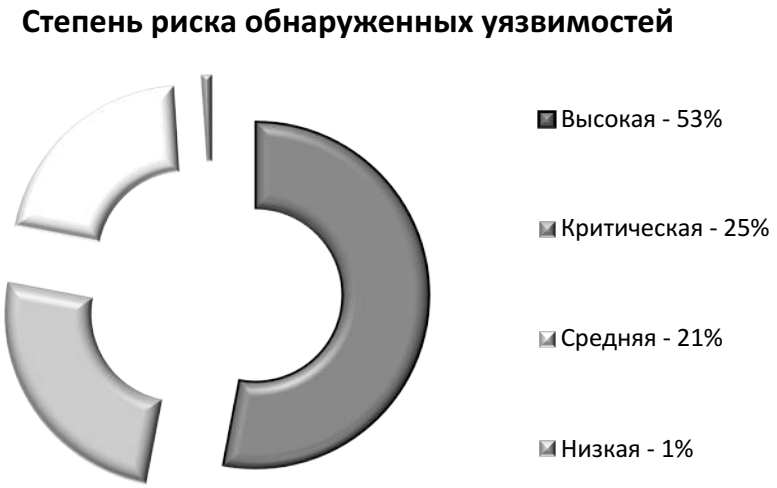


Рис. 4. Степени риска обнаруженных уязвимостей
(Fig. 4. Risk levels of detected vulnerabilities

1.2 Геополитическая составляющая

Важной тенденцией в ЗИ является милитаризация киберпространства. Весьма существенным подтверждением данного факта является то, что в настоящее время официально признано существование кибервойск двадцатью странами мира [14].

В Российской Федерации (РФ) об этом объявлено в 2013 году. В табл.1 приведены сводные данные по странам, имеющим кибервойска и оцениваемым их потенциалом, определяющимся из уровня их финансирования и ориентировочной численности [14].

В табл. 1 представлены 19 стран. Согласно этих же источников, 20-й страной является Россия. Так, специалисты компании Zecurion Analytics [15], входящей в крупную отечественную IT-компанию Zecurion, заявляют, что Россия может входить в ТОП-5 государств, обладающих развитыми кибервойсками. Подавляющее число стран, указанных в табл. 1 либо не имеют дружеских отношений с РФ, либо входят в военно-политические блоки, противостоящие РФ.

Помимо развития кибервойск, в мире уделяется внимание уровню образования широких кругов населения в области защиты информации. Например, в США несколько лет назад начала реализовываться национальная инициатива в области кибербезопасности – NICE (*«The National Initiative for Cybersecurity Education»*) [16].

По результатам исследования, приведенным в [17], национальная инициатива «ориентирована на рост общего числа работников, подготовленных для защиты национальных интересов от существующих и будущих угроз».

2. Обзор законодательства по ГИС и критической информационной инфраструктуре основного геополитического оппонента

Основным геополитическим противником РФ являются Соединённые Штаты Америки. Содержание актуальной редакции (2017 года) Стратегии Национальной Безопасности США [18]: «Китай и Россия бросают вызов американской власти, влиянию и интересам, пытаясь подорвать американскую безопасность и процветание» является тому подтверждением. В том же источнике Россия обвиняется в проведении информационных атак против т.н. «свободного мира»: «Россия использует информационные операции как часть своих (наступательных) киберусилий по влиянию на общественное мнение по всему миру. Её кампании влияния сочетают тайные разведывательные операции и ложные онлайн-персонажи с государственными средствами массовой информации, сторонними посредниками и платными пользователями социальных сетей или «троллями» [18].

Современные отрасли экономики активно внедряют новейшие цифровые решения с помощью различных объектов информационной инфраструктуры, таких например как: ИС, АСУ ТП и ИТС с целью повышения их конкурентоспособности и модернизации, с целью ускорения своего инновационного развития [19].

Согласно отчету Kaspersky ICS-CERT, в мире количество компьютерных атак с попытками внедрения вредоносных объектов на компьютеры АСУ в первом полугодии 2019 г. по сравнению с первым полугодием 2018 г. выросли незначительно, однако все равно находятся на высоких отметках.

Следует отметить о важности в РФ организации подготовки и проведения регулярных учений по киберзащите (КЗ), так же как это, например, организовано у наших оппонентов. Учения по киберзащите в настоящее время играют достаточно важную роль: в подготовке специалистов, например, разработка и внедрение систем оценки доступности для учений по киберзащите [20] в области ЗИ наравне с подготовкой кадров страны. Практическая работа и выполнение специальных упражнений повысит квалификацию, готовность и осведомленность, как специалистов, так и экспертов.

Таблица 1. Потенциал кибервойск стран мира

№	Страна	Финансирование, млн. $, в год	Число военнослужащих
1	США	7000	9000
2	Китай	1500	20000
3	Великобритания	450	2000
4	Германия	250	1000
5	Северная Корея	200	4000
6	Франция	220	800
7	Южная Корея	400	700
8	Израиль	150	1000
9	Польша	50	400
10	Япония	250	500
11	Австралия	125	300
12	Эстония	7	100
13	Иран	25	250
14	Италия	70	250
15	Нидерланды	15	150
16	Чехия	18,5	150
17	Турция	10	100
18	Канада	20	100
19	Дания	15	150

Киберпространство, как оперативная область [21], признается организацией североатлантического альянса, *North Atlantic Treaty Organization* (НАТО), наряду с сушей, морем, воздухом и космосом.

В настоящее время эксперты НАТО одобряют развитие, как оборонительного, так и оперативно кибернетического потенциала [22]. США существенно раньше озаботились защитой информации, как в ГИС, так и критической информационной инфраструктуры. В табл. 2 представлен перечень основных нормативно-правовых актов США.

Составной частью Федеральной ГИС (ФГИС) Росстандарта является Федеральный информационный фонд (ФИФ) по обеспечению единства измерений, созданный в соответствии с положениями Федерального закона № 102-ФЗ[3] и принадлежащий Федеральному агентству по техническому регулированию и метрологии (Росстандарт). В соответствии со статьей 20, сведения, содержащиеся в ФИФ, используются при оказании государственных услуг.

[3]Федеральный закон от 26.06.2008 № 102-ФЗ (ред. от 18.03.2019) «Об обеспечении единства измерений» // URL: http://www.consultant.ru/document/cons_doc_LAW_77904/ (дата обращения: 02.03.2020).

Таблица 2. Основные законодательные акты США в области ГИС и КИИ

№ п/п	Наименование НПА	Краткое описание
1	Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection 2003	Определяет национальную политику федеральных министерств и ведомств по выявлению и приоритезации важнейших объектов инфраструктуры и их защите от нападений.
2	FIPS PUB 199 Standards for Security Categorization of Federal Information and Information Systems 2004	Устанавливает категории безопасности, как для информации, так и для информационных систем. Категории безопасности основаны на потенциальном воздействии на организацию в случае возникновения определенных событий, которые ставят под угрозу информацию и информационные системы, необходимые организации для выполнения возложенной на нее миссии, защиты ее активов, выполнения ее юридических обязанностей, поддержания ее повседневных функций и защиты физических лиц. Категории безопасности должны использоваться в сочетании с информацией об уязвимости и угрозах при оценке риска для организации.
3	FIPS PUB 200 Minimum Security Requirements for Federal Information and Information Systems 2006	Стандарт устанавливает минимальные требования безопасности для федеральных ИС в семнадцати областях, связанных с безопасностью. Федеральные органы должны соблюдать минимальные требования безопасности, определенные в настоящем документе, путем использования средств контроля безопасности в соответствии с NIST SP800-53.
4	NIST SP800-53, Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations 2013	Целью документа является предоставление рекомендаций по выбору и конкретизации средств контроля безопасности для организаций и информационных систем, поддерживающих органы исполнительной власти федерального правительства в соответствии с требованиями публикации FIPS 200
5	NIST SP800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations 2011	Цель этого руководства – помощь организациям в разработке стратегии ISCM и реализации программы, которая обеспечивает осведомленность об угрозах и уязвимостях, видимость активов и эффективность развернутых средств контроля безопасности. Стратегия и программа ISCM поддерживают постоянную уверенность в том, что запланированные и реализованные средства контроля приведены в соответствие с допуском организационных рисков, а также способностью своевременно предоставлять информацию, необходимую для реагирования на риск.
6	Presidential Policy Directive 21: Critical Infrastructure Security and Resilience (PPD-21) 2013	Защита и обеспечение устойчивости критической инфраструктуры является законом Соединенных Штатов, который направлен на укрепление и обеспечение безопасности критической инфраструктуры страны. Президент Барак Обама выпустил PPD-21 в 2013 году для содействия большей интеграции и сотрудничеству между государственными и частными организациями. Целью директивы является снижение уязвимости, выявление и устранение угроз, минимизация последствий и ускорение усилий по реагированию и восстановлению, связанных с критической инфраструктурой.

Отметим, что областью деятельности Росстандарта в соответствии с постановлением[4] является, в том числе и область транспортных средств. Следовательно,

[4]Постановление Правительства РФ от 17 июня 2004 г. N 294 «О Федеральном агентстве по техническому регулированию и метрологии» // URL: https://base.garant.ru/12135835/ (дата обращения: 04.01.2020).

можно утверждать, что Федеральная ГИС Росстандарта является объектом КИИ, функционирующим в сфере транспорта. Одновременно можно отметить, что объектом критической информационной инфраструктуры могут являться ГИС, чему во ФСТЭК России имеются неоднократные подтверждения.

3. Модель угроз государственной информационной системы

3.1 Отличительные признаки государственных информационных систем

В соответствии со ст. 14 Федерального закона N 149-ФЗ[1] информационные системы, относящиеся к ГИС должны отвечать следующим критериям:

– в ГИС возможно размещение открытых данных (п. 4);

– создаются в целях реализации полномочий государственных органов и обеспечения обмена информацией между этими органами (п. 1);

– информация для создания и эксплуатации ГИС предоставляется как физическими лицами и организациями, так и государственными органами и органами местного самоуправления» (п. 3);

– доступ к части информации, циркулирующей в ГИС, может быть предоставлен только после авторизации в Единой системе идентификации и аутентификации (п. 4.1);

– технические средства, предназначенные для обработки информации, содержащейся в ГИС, в том числе программно-технические средства и СЗИ, должны соответствовать требованиям законодательства Российской Федерации о техническом регулировании (п. 8);

– информация, содержащаяся в государственных информационных системах, является государственными информационными ресурсами (п. 9);

– ответственными за обеспечение безопасности информации ГИС являются государственные органы (п. 9).

Для нахождения отличительных черт федеральных ГИС и определения критериев и показателей отнесения ГИС к федеральным ГИС предложено использовать «Реестр федеральных государственных информационных систем» (далее – Реестр), созданный в соответствии с Постановлением Правительства РФ №723[5] и в настоящее время размещенный на Сервере органов государственной власти Российской Федерации. Кроме того, для поиска введённых в эксплуатацию ГИС необходимо проанализировать все нормативные акты государственных органов и федеральных органов исполнительной власти, начиная с сентября 2009 года.

3.2 Анализ информационных систем

На момент прекращения актуализации в Реестре было зарегистрировано 339 федеральных ГИС, внесённых с 1988 г. по 2016 г. В табл. 3 представлен перечень некоторых «официальных» ГИС РФ.

Анализ ФГИС, входящих в Реестр проводился по критериям, представленным далее.

3.2.1 Общие особенности ФГИС

Анализ общих особенностей ФГИС проводился по следующим критериям:

– функционирование ФГИС в настоящее время: показатель бинарный, соответственно, значения – функционирует или не функционирует;

[5]Постановление Правительства РФ № 723 от 10 сентября 2009 г. «О порядке ввода в эксплуатацию отдельных государственных информационных систем» // URL: https://base.garant.ru/12169521/ (дата обращения 04.05.2020).

– представление ФГИС в сети Интернет: показатель бинарный, соответственно, значения – есть или нет.

3.2.2 Особенности ФГИС по доступу к информации

Анализ особенностей ФГИС, относящихся к доступу к циркулирующей в ней информации проводился по следующим критериям:

– наличие во ФГИС закрытого контура, для доступа к которому необходимо пройти какую-либо авторизацию: показатель бинарный, соответственно, значения – есть или нет;

– через Единую систему идентификации и аутентификации;

– через собственную систему авторизации;

– наличие во ФГИС открытого контура, для доступа к которому нет необходимости проходить какую-либо авторизацию: показатель бинарный, соответственно, значения – есть или нет;

– тип авторизации при доступе к закрытому контуру ФГИС: показатель неизвестен, возможные значения будут сформированы по результатам анализа.

3.2.3 Особенности ФГИС по вводу информации

Анализ особенностей ФГИС, относящихся к вводу информации проводился по следующим критериям:

– способ ввода информации во ФГИС в настоящее время: показатель неизвестен.

Предположительно, возможны следующие значения:

– через закрытый контур ФГИС;

– через взаимодействие с другими ИС;

– способ известен только Оператору.

3.2.4 Особенности ФГИС по организации взаимодействия с другими ИС

Анализ особенностей ФГИС, относящихся к их взаимодействию с другими информационными системами проводился по следующим критериям:

– наличие взаимодействия: показатель бинарный – взаимодействует или не взаимодействует;

– способ взаимодействия.

Предположительно, возможны следующие значения:

– с помощью собственного протокола обмена;

– с помощью утверждённого для взаимодействия ИС в РФ протокола обмена;

– протокол известен только Оператору.

3.2.5 Результаты анализа ФГИС, входящих в Реестр

По результатам анализа ФГИС, входящих в Реестр ФГИС, сформирована для дальнейшего исследования табл. 4. При анализе ФГИС, входящих в Реестр о значении конкретного показателя на основе косвенных данных, например, о способе ввода информации, взаимодействию с другими ИС и способе взаимодействия с другими ИС.

Косвенные данные подразумевают упоминание о значении показателя в сети Интернет. Оценка достоверности проводилась экспертным путём эксперта выступили исследователи.

3.3 Формирование критериев принадлежности ГИС к ФГИС

По результатам анализа принадлежности ГИС к ФГИС можно сделать следующие выводы:

– авторизация в закрытом контуре ФГИС происходит с помощью Единой системы идентификации и аутентификации, которая сама является ФГИС;

– взаимодействие ФГИС с другими информационными системами происходит по протоколам «Системы межведомственного электронного взаимодействия, СМЭВ[1]», которая сама является федеральной государственной информационной системой; введены в действие 20 февраля 2012 г. и созданной на основании п. 19 ст. 2[4].

Таблица 3. Перечень «официальных» ГИС Российской Федерации

№ п.п	Реест-ровый номер	Наименование ФГИС	Наименование оператора ФГИС	Дата ввода в эксплуа-тацию	Адрес официального сайта	Номер и дата выдачи электронного паспорта
1	1	ЕИС Роскомнадзора	Роскомнадзор	01.01.2010	www.rkn.gov.ru	ФС-77100001 от 31.03.2010
2	2	АИС ГВР	Росводресурсы	01.01.2008	voda.mnr.gov.ru	ФС-77100002 от 12.04.2010
3	5	ИТКС Контроль	Счетная палата Российской Федерации	25.12.2006	www.ach.gov.ru	ФС-77100005 от 23.04.2010
4	6	АИС РФС АПК	Минсельхоз России	01.09.2009	www.mcx.ru	ФС-77100006 от 28.04.2010
5	8	ЕИАС ФСТ России	ФСТ России	15.12.2006	www.fstrf.ru	ФС-77100008 от 12.05.2010
6	10	ИС ВПВ МИД России	МИД России	28.09.2001	www.mid.ru	ФС-77100010 от 27.05.2010
7	13	ЕБД	ФСКН России	01.01.2007	www.fskn.gov.ru	ФС-77100013 от 08.06.2010
8	14	ЕГАИС	Росалкоголь-регулирование	05.11.2008	www.fsrar.ru	ФС-77100014 от 09.06.2010
9	16	АИС Финансы	Минфин России	14.12.1999	www.minfin.ru	ФС-77100016 от 16.06.2010
10	17	АС ОПИГ МИД России	МИД России	29.12.2003	www.mid.ru	ФС-77100017 от 12.07.2010
11	18	АДИС-МВД	МВД России	22.12.2006	www.mvd.ru	ФС-77100018 от 14.07.2010
12	19	АИС «Консул ЗУ»	МИД России	23.02.2000	www.mid.ru	ФС-77100019 от 21.07.2010
13	24	ЭРПАС	Минкультуры России	06.12.2005	www.mkrf.ru	ФС-77100024 от 05.08.2010
14	25	АИС «Гражданство МИД»	МИД России	27.12.2006	www.mid.ru	ФС-77100025 от 20.08.2010
15	26	Электронный реестр судов	ФГУП Морсвязьспутник	01.03.2008	www.morflot.ru	ФС-77100026 от 06.09.2010
16	27	АИС «Загранпаспорт МИД»	МИД России	17.01.2007	www.mid.ru	ФС-77100027 от 08.09.2010
17	28	АИС УНРО	Минюст России	02.07.2007	www.minjust.ru	ФС-77100028 от 24.09.2010
18	30	АИС ЯРБ	Ростехнадзор	26.05.2009	www.gosnadzor.ru	ФС-77100030 от 06.10.2010
19	31	Инспектор	Ростехнадзор	25.02.2010	www.gosnadzor.ru	ФС-77100031 от 12.10.2010
20	32	Энергосистема-Зима	Ростехнадзор	25.02.2010	www.gosnadzor.ru	ФС-77100032 от 12.10.2010
21	33	Система каталогизации промышленной продукции для федеральных гос. нужд	ФГБУ РосНИИ ИТ и АП	28.12.2005	минобрнаки.рф	ФС-77100033 от 14.10.2010

Продолжение таблицы 3

22	34	ИСДМ-Рослесхоз	ФБУ Центральная база авиационной охраны лесов Авиалесоохрана	08.12.2005	www.rosleshoz.gov.ru	ФС-77100034 от 21.10.2010
23	35	ИАС ЕСУГИ	Росимущество	19.08.2009	www.rosim.ru	ФС-77100035 от 22.10.2010
24	37	Правовая информационная система Федерального агентства по рыболовству	Росрыболовство	15.12.2005	www.fishcom.ru	ФС-77100037 от 29.10.2010
25	38	Реестр лицензий	Росалкогольрегулирование	18.06.2009	www.fsrar.ru	ФС-77100038 от 01.11.2010
26	41	АИС «Служебный выезд»	МИД России	14.09.2007	www.mid.ru	ФС-77100041 от 11.11.2010
27	42	АИС ХБ ФМБА России	ФМБА России	01.12.2010	www.fmbaros.ru	ФС-77100042 от 22.11.2010
28	43	АИС Росздравнадзора	Росздравнадзор	31.03.2006	www.roszdravnadzor.ru	ФС-77100043 от 29.11.2010
29	45	АСВЗ	Росреестр	25.12.2010	www.rosreestr.ru	ФС-77100045 от 09.12.2010
30	48	База данных деклараций	Росалкогольрегулирование	11.11.2009	www.fsrar.ru	ФС-77100048 от 24.12.2010
31	51	ПК ИС ЕГРП	Росреестр	12.01.2015	www.rosreestr.ru	ФС-77110051 от 21.01.2011
32	52	АИС «Юстиция»	Росреестр	12.01.2015	www.rosreestr.ru	ФС-77110052 от 21.01.2011
33	53	Программное обеспечение по центральным выплатам получателям ЕДК в возмещении вреда здоровью гражданам, подвергшимся воздействию радиации вследствие радиационных аварий	Роструд	17.04.2007	www.rostrud.ru	ФС-77110053 от 31.01.2011
34	54	ЕФРСБ	Минэкономразвития России	29.12.2010	www.economy.gov.ru	ФС-77110054 от 01.02.2011
35	55	АИС РПУ	Роструд	01.01.2009	www.rostrud.ru	ФС-77110055 от 02.02.2011
36	56	АИС УП	Минэкономразвития России	22.10.2010	www.economy.gov.ru	ФС-77110056 от 08.02.2011
37	58	АИС АГС	Роструд	20.12.2006	www.rostrud.ru	ФС-77110058 от 14.02.2011
38	59	Система ФАИП	Минэкономразвития России	01.01.2011	www.economy.gov.ru	ФС-77110059 от 15.02.2011
39	60	ИС ФЦП	Минэкономразвития России	01.01.2011	www.economy.gov.ru	ФС-77110060 от 15.02.2011
40	62	Web-представительство информационно-аналитической системы «Трудовая миграция» (ИАС ТМ) «Работа в России»	Роструд	14.11.2008	www.rostrud.ru	ФС-77110062 от 15.02.2011

Таблица 4. Результаты исследования ФГИС, входящих в Реестр ФГИС

Функционирование ФГИС	Представительство ФГИС в сети Интернет	Наличие открытого контура	Наличие закрытого контура	Авторизация в закрытом контуре		
				ЕСИА	Своя СА	Н/Д
286	286	247	246	95	36	115

Продолжение Таблицы 4

Способ ввода информации			Взаимодействие ФГИС с другими ИС	Способ взаимодействия с другими ИС		
Через закрытый контур	Через взаимодействие с другими ИС	Н/Д		Через собственный протокол обмена	Через утверждённый протокол обмена	Н/Д
20	24	202	31	0	22	264

3.4 Анализ состояния баз данных угроз и уязвимостей

Для определения возможных угроз исследуемой ГИС необходимо провести анализ актуальных баз данных угроз и уязвимостей.

В этой части анализируются существующие в настоящее время БД уязвимостей с целью выбора наиболее подходящей для анализа наличия возможных уязвимостей и угроз безопасности информации объекта исследования.

3.4.1 Банк данных угроз безопасности ФСТЭК России

Банк данных угроз безопасности ФСТЭК России (БДУ ФСТЭК)[6] содержит сведения об основных угрозах безопасности информации и уязвимостях. Особое внимание уделяется угрозам, которые применимы к ГИС и АСУ производственными и технологическими процессами критически важных объектов. Ведётся данный банк, ФСТЭК России и ФАУ «ГНИИИ ПТЗИ ФСТЭК России».

В БДУ ФСТЭК содержатся как данные об угрозах безопасности информации, так и данные об уязвимостях в программном и программно-аппаратном обеспечении.

В настоящее время в БДУ ФСТЭК содержатся данные о двухсот тринадцати угрозах безопасности информации и о двадцати одной тысяче четырехстах тринадцати уязвимостях программного обеспечения. При этом, как правило, существует соответствие между уязвимостями БДУ ФСТЭК и в NVD.

Об использовании настоящего источника можно указать наличие в его реестре уязвимостей системного и общего программного обеспечения, входящего в [17].

3.4.2 База данных уязвимостей National Vulnerability Database (NVD) Национального института стандартов и технологий Министерства торговли США.

Данная база данных NVD ведётся с 1998 года и в настоящее время насчитывает более девяноста восьми тысяч уязвимостей. Нужно отметить, что не всегда имеются данные об уязвимостях в программном обеспечении российского производства.

Данная БД совместима с разработанным корпорацией MITRE Corporation (США) реестром уязвимостей CVE List (https://cve.mitre.org/cve/), ведением которого занимаются более 80 организаций, в т.ч. ведущие разработчики программного обеспечения и средств защиты информации, например, «Лаборатория Касперского».

Данный факт обуславливает, в отличие от БДУ ФСТЭК, очень быстрое пополнение реестра известных уязвимостей. В пользу принятия решения об использовании настоящего источника можно указать:

[6]Постановление Правительства РФ № 697 от 8 сентября 2010 г. «О единой системе межведомственного электронного взаимодействия» // URL: https://base.garant.ru/199319/ (дата обращения: 04.05.2019).

– большой объём накопленных данных об уязвимостях;

– продолжающееся, при разработке ГИС, использование системного и общего программного обеспечения, не входящего в «Единый реестр российских программ для электронных вычислительных машин и баз данных» [18].

3.4.3 Прочие база данных уязвимостей

Для полноты были проанализированы следующие базы данных уязвимостей.

3.4.3.1 Secunia Advisory and Vulnerability Database

Ведётся с 2003 года исследовательской компанией Secunia Research (всемирная компания с филиалами в США и Европе). Не в полной мере совместима с NVD и не совместима с БДУ ФСТЭК. Содержит свыше семидесяти тысяч записей о различных уязвимостях. Бесплатный доступ к Secunia Advisories and Vulnerability Database возможен только при некоммерческом использовании. Доступна по адресу: https://secuniaresearch.flexerasoftware.com/community/advisories/.

3.4.3.2 Open Sourced Vulnerability Database

Ведение БД было начато в 2004 году как свободно доступный проект. В 2016 году с закрытием трансформировалась в коммерческий проект – БД уязвимостей VulnDB (https://vulndb.cyberriskanalytics.com/). В настоящее время содержит свыше ста семидесяти тысяч записей.

3.4.3.3 Vulnerability Notes Database

VND (Vulnerability Notes Database, https://www.kb.cert.org/vuls). Ведётся CERT Coordination Center при университете Carnegie Mellon (США). Является агрегатором. Обновления крайне редки. По состоянию на настоящее время насчитывает не более пяти тысяч записей.

3.4.4 Итоги отбора БДУ

Исходя из анализа БД уязвимостей и угроз, по критериям соответствия среде используемого в РФ программного обеспечения, полноты содержания описаний уязвимостей и их связями с угрозами и вида доступа к информации, принято решение использовать в качестве источников информации об уязвимостях и угрозах БДУ ФСТЭК России.

3.5 Математические методы, применимые при построении модели угроз

Набор исходных данных, представляют собой конечные множества данных, для которых можно использовать математическую модель на основе теории множеств.

Построение характеристической функции, принимающей одно из двух бинарных значений «1» – «Принадлежит, истина, входит, …» или «0» – «Не принадлежит, ложно, не входит, …» становится затруднительным. Например, можно указать наличие в составе ФГИС определённой версии некоего ПО, имеющего уязвимости по данным NVD, но отсутствующем в БДУ ФСТЭК России. Иными словами, существенную часть решений будет приниматься экспертами на основании своих знаний и опыта.

Заключение

Анализ текущего состояния информационных фондов ОГВ РФ (федеральных министерств и ведомств РФ, ОГВ субъектов РФ) выявил наиболее характерные тенденции, имеющие распространение и на информационные ресурсы, и на ГИС. В работе выявлены отличительные признаки и разработаны критерии отбора федеральных ГИС.

Исходя из анализа баз и банков данных уязвимостей и угроз, проведенного по критериям соответствия среде используемого в РФ программного обеспечения, полноты содержания описаний уязвимостей и их связями с угрозами и вида доступа к информации,

принято решение использовать в качестве источников информации об уязвимостях и угрозах БДУ ФСТЭК России и в нормативно-правовых актах.

В результате проведенных исследований подтверждены: возрастающая значимость защиты государственных информационных систем; актуальность выбранной темы и принадлежность (важность отнесения) рассматриваемого объекта исследования к государственной информационной системы и критической информационной инфраструктуре.

Полученные данные предполагается в дальнейшем использовать в ходе разработки методики оценки угроз безопасности информации в государственных информационных системах.

СПИСОК ЛИТЕРАТУРЫ:

1. Горлатых, Андрей В.; Запечников, Сергей В. Построение защищенной системы управления многомерными структурами данных. Безопасность информационных технологий, [S.l.]. Т. 25, № 3. С. 16–25, сен. 2018. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1136 (дата обращения: 19.08.2020). DOI: http://dx.doi.org/10.26583/bit.2018.3.022.
2. Малюк, Анатолий А.; Гавдан, Григорий П. Формирование и использование национальных информационных ресурсов – основа развития цифровой экономики. Безопасность информационных технологий, [S.l.]. Т. 26, № 2. С. 67–85, июнь 2019. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1200/1145. (дата обращения: 20.07.2020). DOI:http://dx.doi.org/10.26583/bit.2019.2.05.
3. О выездном совещании Секретаря Совета Безопасности России Николая Патрушева с главами регионов, входящих в состав Сибирского федерального округа. Официальные сайты органов государственной власти Российской Федерации // URL: http://www.scrf.gov.ru/news/allnews/2665/ (дата обращения 02.07.2020).
4. Баранкова И.И., Михайлова У.В., Афанасьева М.В. «Минимизация рисков информационной безопасности на основе моделирования угроз безопасности» // Динамика систем, механизмов и машин. 2019. № 4. С. 60–66. DOI: https://doi.org/10.25206/2310-9793-7-4-60-66.
5. Дойникова Е.В., Котенко И.В. «Методики и программный компонент оценки рисков на основе графов атак для систем управления информацией и событиями безопасности» // Информационно-управляющие системы. 2016. №5. С. 56–67. DOI: https://doi.org/10.15217/issn1684-8853.2016.5.54.
6. Шабуров А.С., Юшкова С.А., Бодерко А.В. «Моделирование оценки угроз безопасности информационных систем персональных данных» // Вестник ПНИПУ. Серия «Электротехника, информационные технологии, системы управления». 2013. № 7 (1). С. 149–159. УДК: 004.056.5-047.58.
7. Шинкаренко А.Ф. Методика оценивания защищенности информационно-телекоммуникационных узлов // Интеллектуальные технологии на транспорте. 2016. №1. URL: https://cyberleninka.ru/article/n/metodika-otsenivaniya-zaschischennosti-informatsionno-telekommunikatsionnyh-uzlov (дата обращения: 07.07.2020).
8. Казарин О.В., Шаряпов Р.А., Ященко В.В. Многофакторная классификация угроз информационной безопасности киберфизических систем // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2018. № 1 (1). С. 39–55. УДК 004.056.
9. Глобальное исследование утечек конфиденциальной информации в 2017 году, InfoWatch // URL: https://www.infowatch.ru/sites/default/files/report/analytics/russ/InfoWatch_Global_Report_2017_year.pdf?rel=1 (дата обращения: 07.05.2020).
10. Глобальное исследование утечек конфиденциальной информации в 2018 году, InfoWatch // URL: https://www.infowatch.ru/sites/default/files/report/analytics/russ/InfoWatch_Global_Report_2018_year.pdf?rel=1 (дата обращения: 07.05.2019).
11. Kaspersky Security Bulletin: Прогнозы по развитию угроз в сфере промышленной безопасности на 2019 год. АО «Лаборатория Касперского» // URL: https://securelist.ru/ksb-threat-predictions-for-industrial-security-in-2019/92848/ (дата обращения: 07.05.2020).
12. Уязвимости в АСУ ТП: итоги 2018 года. «Positive Technologies» // URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/ICS-vulnerabilities-2019-rus.pdf (дата обращения: 07.05.2020).
13. Рябова В. Китай признал существование кибервойск. D-Russir.ru // URL: https://d-russia.ru/kitaj-priznal-sushhestvovanie-kibervojsk.html (дата обращения: 07.07.2020).

14. Zecurion Analytics «Кибервойны 2017: Баланс сил в мире». Аналитический центр Zecurion // URL: https://www.zecurion.ru/upload/iblock/cb8/cyberarmy_research_2017_fin.pdf (дата обращения: 07.05.2020).
15. Аналитики назвали Россию в числе пяти стран с лучшими кибервойсками. Лента новостей. РБК // URL: https://www.rbc.ru/politics/10/01/2017/58747b439a7947526d203417 (дата обращения: 07.07.2020).
16. National initiative for cybersecurity education (NICE) // URL: https://www.nist.gov/itl/applied-cybersecurity/nice (дата обращения: 02.05.2020).
17. Мельников, Дмитрий А.; Гавдан, Григорий П.; Корсаков, Иван А. К вопросу о цели и задачах национальной образовательной инициативы США в области кибербезопасности. Безопасность информационных технологий, [S.l.]. Т. 25, № 2. С. 23–37, май 2018. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1107. (дата обращения: 05.06.2020). DOI: http://dx.DOI.org/10.26583/bit.2018.2.02.
18. NATIONAL SECURITY STRATEGY of the United States of America DECEMBER 2017 // URL: https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf (дата обращения: 04.05.2020).
19. Салкуцан, Алексей А.; Гавдан, Григорий П.; Полуянов, Андрей А. Методика определения критических процессов на объектах информационной инфраструктуры. Безопасность информационных технологий, [S.l.]. Т. 27, № 2. С. 18–34, июнь 2020. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1268/1187. DOI: http://dx.doi.org/10.26583/bit.2020.2.02 (дата обращения: 26.07.2020).
20. Банк данных угроз безопасности информации Федеральной службы по таможенному и экспортному контролю Российской Федерации // URL: https://bdu.fstec.ru (дата обращения: 04.05.2020).
21. Mauno Pihelgas. Design and Implementation of an Availability Scoring System for Cyber Defence Exercises. (This paper was accepted to the 14th International Conference on Cyber Warfare and Security: ICCWS 2019 and the final version of the paper is included in the Conference Proceedings. ISBN: 978-1- 912764-11-2; ISSN: 2048-9870).URL:https://ccdcoe.org/uploads/2020/02/M_Pihelgas-Design_and_Implementation_of_an_Availability_Scoring_System_for_Cyber_Defence_Exercises.pdf (дата обращения: 02.05.2020).
22. 12th International Conference on Cyber Conflict 20/20 VISION: THE NEXT DECADE Copyright © 2020 by NATO CCDCOE Publications. All rights reserved. URL: https://ccdcoe.org/uploads/2020/05/CyCon_2020_book.pdf (дата обращения: 02.05.2020).

REFERENCES:

[1] Andrey V. Gorlatyh, Sergey V. Zapechnikov. Building secure multidimensional data management system. IT Security (Russia), [S.l.]. V. 25, n. 3. P. 16–25, sep. 2018. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1136. (accessed: 19.08.2020). DOI: http://dx.doi.org/10.26583/bit.2018.3.02 (in Russian).
[2] MALYUK, Anatoly A.; GAVDAN, Grigory P. Development and use of national information resources as the basis for digital economy development. IT Security (Russia), [S.l.]. V. 26, n. 2. P. 67–85, june 2019. ISSN 2074-7136. URL: <https://bit.mephi.ru/index.php/bit/article/view/1200 (accessed: 20.07.2020). DOI: http://dx.doi.org/10.26583/bit.2019.2.05 (in Russian).
[3] About the visiting meeting of the Secretary of the Security Council of Russia Nikolai Patrushev with the heads of the regions that make up the Siberian Federal district. Official websites of state authorities of the Russian Federation. Available on: URL: http://www.scrf.gov.ru/news/allnews/2665/ (accessed: 02.07.2020) (in Russian).
[4] Barankova I.I., Mikhailova U.V., Afanasyeva M.V. Minimization of information security risks based on modeling security threats. Dynamics of Systems, Mechanisms and Machines (Dynamics). 2019. № 4. P. 60–66. DOI: https://doi.org/10.25206/2310-9793-7-4-60-66 (in Russian).
[5] Dojnikova E.V., Kotenko I.V. TECHNIQUES AND SOFTWARE TOOL FOR RISK ASSESSMENT ON THE BASE OF ATTACK GRAPHS IN INFORMATION AND SECURITY EVENT MANAGEMENT SYSTEMS. Saint-Petersburg Institute for Informatics and Automation of the RAS. 2016. №5. P. 56–67. DOI: https://doi.org/10.15217/issn1684-8853.2016.5.54 (in Russian).
[6] Shaburov A.S., Yushkova S.A., Boderko A.V. Modelling of evaluation of security threat for informational systems dealing with personal data. Vestnik PNIPU. Seriya «Elektrotekhnika, informacionnye tekhnologii, sistemy upravleniya». 2013. № 7 (1). S. 149–159. UDC: 004.056.5-047.58 (in Russian).
[7] Shinkarenko A.F. The method of estimation of the security of information and telecommunication. Intellectual Technologies on Transport. 2016. №1. URL: https://cyberleninka.ru/article/n/metodika-otsenivaniya-zaschischennosti-informatsionno-telekommunikatsionnyh-uzlov (in Russian).

[8] Kazarin O.V., Sharyapov R.A., Yashchenko V.V. Multifactorial classification of threats to information security of cyber-physical systems. Vestnik RGGU. Seriya «Informatika. Informacionnaya bezopasnost'. Matematika». 2018. № 1 (1). S. 39–55. UDC 004.056 (in Russian).
[9] Global study of confidential information leaks in 2017, InfoWatch. URL:https://www.infowatch.ru/sites/default/files/report/analytics/russ/InfoWatch_Global_Report_2017_year.pdf?rel=1 (accessed: 07.05.2020) (in Russian).
[10] Global study of confidential information leaks in 2018, InfoWatch. URL:https://www.infowatch.ru/sites/default/files/report/analytics/russ/InfoWatch_Global_Report_2018_year.pdf?rel=1 (accessed: 07.05.2019) (in Russian).
[11] «Kaspersky Security Bulletin: Kaspersky Security Bulletin: Forecasts for the development of threats in the field of industrial security for 2019. «Kaspersky Lab». URL: https://securelist.ru/ksb-threat-predictions-for-industrial-security-in-2019/92848/ (accessed: 07.05.2020) (in Russian).
[12] Vulnerabilities in automated process control systems: 2018 results. «Positive Technologies» // URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/ICS-vulnerabilities-2019-rus.pdf (accessed: 07.05.2020) (in Russian).
[13] Ryabova V. China has recognized the existence of cyber warfare. D-Russir.ru. URL: https://d-russia.ru/kitaj-priznal-sushhestvovanie-kibervojsk.html (accessed: 07.07.2020) (in Russian).
[14] Zecurion Analytics: Cyberwar 2017: Balance of power in the world. Analytical center Zecurion. URL: https://www.zecurion.ru/upload/iblock/cb8/cyberarmy_research_2017_fin.pdf (accessed: 07.05.2020) (in Russian).
[15] Analysts named Russia among the five countries with the best cyber forces. News feed.. RBC.RU. URL: https://www.rbc.ru/politics/10/01/2017/58747b439a7947526d203417 (accessed: 07.07.2020) (in Russian).
[16] National initiative for cybersecurity education (NICE) Workforce Framework Cybersecurity. NICCS. URL: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-181.pdf (accessed: 02.05.2020).
[17] Melnikov, Dmitriy A.; Gavdan, Grigory P.; Korsakov, Ivan A. To the issue about the purpose and objectives the USA National initiative for cybersecurity education. IT Security (Russia), [S.l.]. V. 25, n. 2. P. 23–37, may 2018. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1107 (accessed: 05.06.2020). DOI: http://dx.doi.org/10.26583/bit.2018.2.02 (in Russian).
[18] NATIONAL SECURITY STRATEGY of the United States of America DECEMBER 2017. URL: https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf (accessed: 04.05.2020).
[19] Salkutsan Alexei A., Gavdan Grigory P., Poluyanov Andrey A. The method of identifying critical processes at information infrastructure facilities. IT Security (Russia), [S.l.]. V. 27, n. 2. P. 18–34, june 2020. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1268/1187.
DOI: http://dx.doi.org/10.26583/bit.2020.2.02 (accessed: 26.07.2020).
[20] Data Bank of information security threats of the Federal service for customs and export control of the Russian Federation. URL: https://bdu.fstec.ru (accessed: 04.05.2020).
[21] Mauno Pihelgas. Design and Implementation of an Availability Scoring System for Cyber Defence Exercises. (This paper was accepted to the 14th International Conference on Cyber Warfare and Security: ICCWS 2019 and the final version of the paper is included in the Conference Proceedings. ISBN: 978-1- 912764-11-2; ISSN: 2048-9870). URL: https://ccdcoe.org/uploads/2020/02/M_Pihelgas_-_Design_and_Implementation_of_an_Availability_Scoring_System_for_Cyber_Defence_Exercises.pdf. (accessed: 02.05.2020).
[22] 12th International Conference on Cyber Conflict 20/20 VISION: THE NEXT DECADE Copyright © 2020 by NATO CCDCOE Publications. All rights reserved. URL: https://ccdcoe.org/uploads/2020/05/CyCon_2020_book.pdf (accessed: 02.05.2020).

Поступила в редакцию - 16 июля 2020 г. Окончательный вариант - 20 августа 2020 г.
Received - July 16, 2020. The final version - August 20, 2020.

Вячеслав А. Чепов[1], Иван И. Швецов-Шиловский[2], Сергей Б. Шмаков[3]
[1,2,3]Национальный исследовательский ядерный университет «МИФИ,
Каширское ш., 31, Москва, 115409, Россия
[1,2,3]Акционерное общество «Экспериментальное научно-производственное объединение
СПЕЦИАЛИЗИРОВАННЫЕ ЭЛЕКТРОННЫЕ СИСТЕМЫ»,
Каширское ш., 31, Москва, 115409, Россия
[1]e-mail: vache@spels.ru, http://orcid.org/0000-0002-5401-7102
[2]e-mail: iish@spels.ru, http://orcid.org/0000-0002-8161-9926
[3]e-mail: sbshmak@spels.ru, http://orcid.org/0000-0002-4692-9355

АЛГОРИТМ СООТНЕСЕНИЯ ФИЗИЧЕСКОЙ И ЛОГИЧЕСКОЙ АДРЕСАЦИЙ В МИКРОСХЕМАХ ПАМЯТИ С ПОМОЩЬЮ ИСТОЧНИКОВ ЛАЗЕРНОГО ИЗЛУЧЕНИЯ

DOI: http://dx.doi.org/10.26583/bit.2020.3.04

Аннотация. В статье представлен разработанный алгоритм соотнесения физической и логической адресаций в микросхемах памяти с помощью источников лазерного излучения для определения характера сбоев при испытаниях на стойкость к ионизирующему излучению (ИИ). Предложен вариант аппаратно-программной реализации алгоритма, приведены ключевые программные инструменты. Алгоритм апробирован на источнике сфокусированного лазерного излучения с возможностью воздействия на отдельную ячейку памяти. Найдены закономерности расположения ячеек в блоке памяти, достаточные для построения полной карты соотнесения физической и логической адресации. Продемонстрированы основные результаты экспериментальной апробации алгоритма, которые подтверждают возможность разработки инструмента визуализации карты сбоев с точностью до одного бита информации. Показан пример применения данного инструмента для анализа стойкости микросхемы статического оперативного запоминающего устройства (СОЗУ) при воздействии импульсного ИИ.

Ключевые слова: ионизирующее излучение, физическая адресация памяти, логическая адресация памяти.

Для цитирования: ЧЕПОВ, Вячеслав А.; ШВЕЦОВ-ШИЛОВСКИЙ, Иван И.; ШМАКОВ, Сергей Б. АЛГОРИТМ СООТНЕСЕНИЯ ФИЗИЧЕСКОЙ И ЛОГИЧЕСКОЙ АДРЕСАЦИЙ В МИКРОСХЕМАХ ПАМЯТИ С ПОМОЩЬЮ ИСТОЧНИКОВ ЛАЗЕРНОГО ИЗЛУЧЕНИЯ. Безопасность информационных технологий, [S.l.], v. 27, n. 3, p. 43–53, 2020. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1291>. Дата доступа: 02 sep. 2020. DOI: http://dx.doi.org/10.26583/bit.2020.3.04.

Viacheslav A. Chepov[1], Ivan I. Shvetsov-Shilovskiy[2], Sergey B. Shmakov[3]
[1,2,3]National Nuclear Research University MEPHI (Moscow Engineering Physics Institute),
Kashirskoe sh., 31, Moscow, 115409, Russia
[1,2,3]Joint Stock Company "Experimental Research and Production Association
SPECIAL ELECTRONIC SYSTEM",
Kashirskoe sh., 31, Moscow, 115409, Russia
[1]e-mail: vache@spels.ru, http://orcid.org/0000-0002-5401-7102
[2]e-mail: iish@spels.ru, http://orcid.org/0000-0002-8161-9926
[3]e-mail: sbshmak@spels.ru, http://orcid.org/0000-0002-4692-9355

Algorithm for matching physical and logical addressing in memory chips using laser sources

DOI: http://dx.doi.org/10.26583/bit.2020.3.04

Abstract. The paper presents the developed algorithm for correlating the physical and logical addressing in memory chips using laser radiation sources to determine the nature of failures in radiation tests. A variant

of the hardware-software implementation of the algorithm is proposed, key software tools are presented. The algorithm was tested using the focused laser facility with the ability to irradiate a separate memory cell. The patterns of location of the memory cells in single memory block were obtained, necessary to compose the full correlation between the physical and logical addressing. The main experimental results of the algorithm approbation are shown, which confirm the possibility of developing the tool for visualizing the map of failures with one-bit precision. The adaptation of the tool for analyzing the hardness of a static random-access memory (SRAM) IC under pulsed ionizing radiation is presented.

Keywords: ionizing radiation, physical memory addressing, logical memory addressing.

For citation: CHEPOV, Viacheslav A.; SHVETSOV-SHILOVSKIY, Ivan I.; SHMAKOV, Sergey B. Algorithm for matching physical and logical addressing in memory chips using laser sources. IT Security (Russia), [S.l.], v. 27, n. 3, p. 43–53, 2020. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1291>. Date accessed: 02 sep. 2020. DOI: http://dx.doi.org/10.26583/bit.2020.3.04.

Введение

В настоящее время существует проблема возникновения сбоев в микросхемах памяти при воздействии ионизирующего излучения [1, 2]. Данная проблема существенно сказывается на сохранности информации: происходит потеря информации в ячейках памяти.

Соотнесение физической и логической адресаций в микросхемах памяти необходимо для построения пространственной карты распределения сбившихся ячеек, что дает возможность наглядно проанализировать характер сбоев, которые могут возникать при воздействии ионизирующего излучения. Визуализация сбившихся ячеек позволяет определять области на кристалле наименее стойкие к воздействию ИИ [3]. Результаты работы могут быть применимы в таких исследованиях как моделирование эффекта «просадки питания на внутренних шинах» (Rail-Span Collapse) [4, 5] в микросхемах, подверженных воздействию импульсного ИИ [6].

Знание взаимного расположения ячеек памяти между собой полезно, если стоит задача определения характера сбоев при воздействии отдельных заряженных частиц (ОЯЧ) [7]. В [8] представлена методика регистрации многократных сбоев (МС) в ячейках, относящихся к одному логическому блоку. Визуализация многократных физических сбоев позволит разработчику микросхем избегать многократные логические сбои путём выбора минимального расстояния между битами в слове (по одному адресу) [9, 10].

Одним из способов получения топологии является использование источника лазерного излучения. При заданных диаметре пятна и шаге сканирования лазерная установка имеет возможность регистрировать координаты ячеек памяти в месте воздействия лазерного излучения. После сканирования есть возможность построить карту, демонстрирующую соответствие координат и адресов сбившихся ячеек памяти. Однако для микросхем памяти с большой ёмкостью данный метод может занять большой промежуток времени (по расчётам для микросхемы СОЗУ ёмкостью 4 Мбит с проектными нормами 180 нм время сканирования заняло бы около 49 дней) [11].

В статье описан подход со значительным снижением временных затрат (до двух дней), при котором удается определить координаты каждой ячейки памяти, при воздействии только в часть накопителя без потери точности соотнесения физической и логической адресаций.

1. Алгоритм соотнесения физической и логической адресаций

Разработка алгоритма сопровождалась проведением эксперимента на сфокусированном источнике лазерного излучения. Данная установка облучает площадки микросхемы памяти при заданных диаметре пятна и шаге сканирования. При сканировании

микросхемы регистрируются координаты в месте воздействия лазерного излучения. Таким образом, есть возможность построить карту, демонстрирующую соответствие координат и адресов сбившихся ячеек памяти.

У предлагаемого способа есть ряд ограничений:

- необходимость вскрытия микросхемы со стороны подложки для исключения влияния металлизации на равномерность облучения;
- необходимость наличия сбоя при выстреле в ячейку памяти.

Современные микросхемы памяти имеют достаточно большую ёмкость, поэтому облучение ячеек по всему размеру микросхемы представляется долгим процессом, вплоть до нескольких недель.

Принято решение производить воздействие лазерного излучения на микросхему следующим образом: выбирается размер пятна 3 микрометра, ячейки, подвергающиеся воздействию ИИ, расположены друг от друга на 100 микрометров вдоль осей абсцисс и ординат. В общем случае данные значения могут быть отличными от представленных. Диаметр пятна должен быть меньше расчётного размера ячейки памяти (n на рис. 1). Размер шага (m на рис. 1) выбирается при условии наличия нескольких сбоев вдоль осей абсцисс и ординат в пределах одного блока памяти. Остальные координаты ячеек с учётом симметрии блоков памяти достраиваются на карте сбоев, разработанной с помощью среды разработки NI LabVIEW 2018. Таким образом, нет необходимости сбивать все ячейки памяти в кристалле.

Сканирование проводится «змейкой»: после каждого воздействия ИИ на ячейку памяти лазер перемещается вдоль оси абсцисс с шагом m, пока не достигнет предела строки, после чего он с шагом n перемещается вниз. В каждой новой строке ячейки, подвергающиеся воздействию ИИ, смещаются вправо с шагом n. В итоге формируется последовательность, представляющая собой диагональные полосы сбившихся ячеек памяти по всему размеру кристалла. Данная последовательность позволяет сбить ячейки памяти вдоль осей абсцисс и ординат в пределах блока памяти, а значит является достаточным условием для анализа всего размера микросхемы памяти, что существенно сокращает время сканирования на сфокусированной лазерной установке.

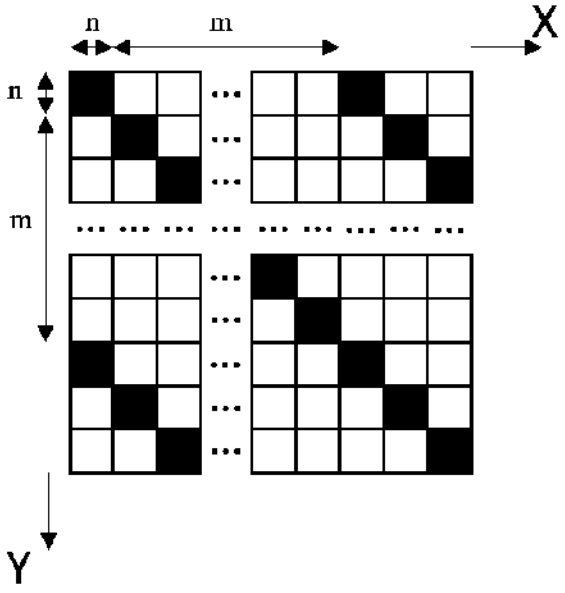


Рис. 1. Схематическое изображение заданной последовательности облучения ячеек памяти (Fig. 1. Schematic representation of the given sequence of irradiation of memory cells)

Алгоритм соотнесения физической и логической адресаций:

1. Предварительный анализ
    1.1. Анализ технической документации
        1.1.1. Количество бит в строке/столбце
    1.2. Визуальный анализ
        1.2.1. Размер кристалла
        1.2.2. Количество и объём банков памяти
        1.2.3. Площадь одной ячейки
2. Выбор необходимой точности соотнесения. Выбор размеров пятна и шага сканирования при условии наличия хотя бы одного сбоя в пределах одного шага
3. Сканирование памяти на установке сфокусированного лазерного излучения. Получение карты сбоев (массив: координаты – адреса, по которым наблюдаются сбои)
4. Изменение разрядов адреса, определение, какие его разряды отвечают за:
    4.1. Банк – при изменении адреса группа сбоев изменяет координату скачком
    4.2. Строка – при фиксации разряда адреса и переборе его значений на карте наблюдается горизонтальная линия из сбоев, при изменении адреса эта линия смещается по вертикали
    4.3. Столбец – при фиксации разряда адреса и переборе его значений на карте наблюдается вертикальная линия из сбоев, при изменении адреса эта линия смещается по горизонтали
5. Определение координат сбоев по адресам
    5.1. Каждой комбинации адресов, отвечающих за столбцы, присвоить координату X
    5.2. Каждой комбинации адресов, отвечающих за строки, присвоить координату Y
6. Дополнение адресной карты по выявленным закономерностям, если это необходимо
7. Если в строке/столбце/банке не было сбоя, то в результате анализа карты сбоев установить закономерности расположения строк/столбцов/банков и рассчитать координаты по адресам, где сбои не зафиксированы.

2. Описание аппаратно-программного комплекса

Блок-схема стенда для воздействия лазерного излучения на микросхему памяти приведена на рис. 2. Стенд содержит персональный компьютер, аппаратный комплекс фирмы National Instruments, сфокусированную лазерную установку ПИКО-3, лазерную установку РАДОН-8 [12, 13].

Аппаратный комплекс NI включает:

- PXI-4110 – 3-канальный программируемый источник питания
- PXI-7951R – ПЛИС (FPGA)
- PXI-6581 – 54-канальный несимметричный цифровой модуль адаптера ввода-вывода.

Задание необходимого уровня питания производится при помощи программируемого источника питания PXI-4110. С помощью ПЛИС PXI-7951R и цифрового адаптера ввода/вывода PXI-6581 проводится проверка сохранности информации. Обработка информации, полученной с аппаратного комплекса, и вывод результатов на экран монитора организуется посредством персонального компьютера. Воздействие лазерного излучения на микросхему памяти осуществляется с помощью сфокусированной лазерной установки ПИКО-3 или лазерной установки РАДОН-8.

Разработка ПО проводилась с помощью среды разработки NI LabVIEW 2018. Блок-схема ПО приведена на рис. 3. Основной частью разработанного ПО является программа, отвечающая за управление всеми PXI-модулями, входящими в состав стенда.

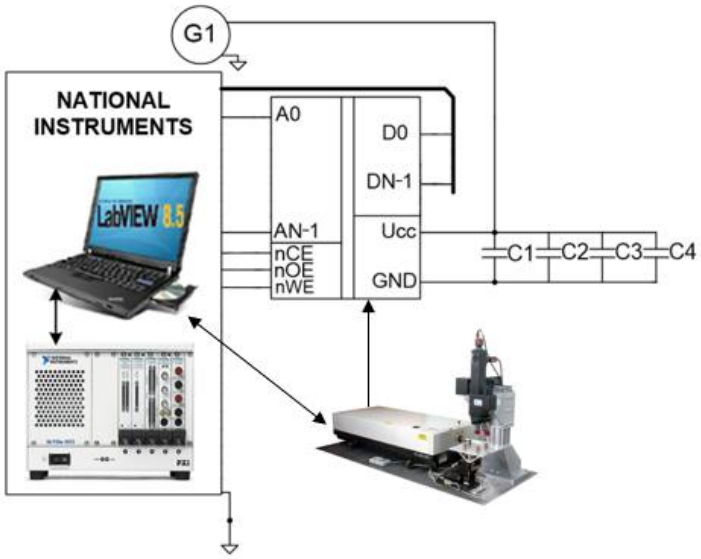


Рис. 2. Блок-схема стенда
(Fig. 2. Block diagram of the test setup)

Рис. 3. Блок-схема ПО, иллюстрирующая ключевые функциональные блоки
(Fig. 3. Software block diagram illustrating key functional blocks)

3. Программа формирования карты сбоев

В данной программе предусмотрена возможность интерактивно взаимодействовать с каждым разрядом адреса памяти. Для этого добавлены управляющие элементы, число которых равно количеству разрядов адреса памяти (для исследуемой памяти с объёмом

4 Мбит их число равно 22). Также в программу добавлена адресная строка, предоставляющая возможность вводить интересующий адрес в виде двоичного кода.

Переключение управляющих элементов в активное состояние интересующих разрядов адреса фиксирует данные разряды. В результате этого формируется пара масок. Фиксированные разряды адреса строго демонстрируют те значения, которые указаны в адресной строке. Оставшаяся часть разрядов принимает значения, соответствующие типу маски (для Mask1 – единицы, для Mask0 – нули).

Программа проводит проверку соответствия масок с каждым адресом памяти. При фиксировании управляющими элементами интересующих разрядов адреса на карте сбоев отобразятся только те координаты ячеек памяти, которые соответствуют указанным значениям разрядов в адресной строке. Множество координат ячеек памяти, разряды адреса которых не были зафиксированы управляющими элементами, отображаются на карте сбоев в полном объеме.

Иными словами, на карте сбоев отображаются координаты ячеек памяти, которые удовлетворяют условию:

(Маска единиц | Адрес = Маска единиц) & (Маска нулей & Адрес = Маска нулей),

где Маска единиц – адрес, все разряды которого равны единице кроме фиксированных;

Маска нулей – адрес, все разряды которого равны нулю кроме фиксированных;

Адрес – адрес облученной ячейки памяти, подающийся на сравнение с масками;

|, & – логические операторы.

4. Программа вывода изображения

Программа вывода изображения иллюстрирует аналитически заданную последовательность булевых констант, где константы со значением ИСТИНА показывают расположения сбившихся ячеек памяти. Разработка программы проводилась при помощи анализа карты сбоев, описанной выше.

Изображение формируется путём конвертирования из двумерного массива. Таким образом, основная идея задания необходимой аналитической последовательности состоит в том, чтобы при изменении значения определённых разрядов адреса выделить закономерности изменения расположения координат облученных ячеек памяти относительно оси абсцисс и ординат.

Анализ карты сбоев позволил разделить разряды адреса на группы: блоки памяти, строки, столбцы, биты данных. Данное разделение объясняется различием характера закономерности каждой группы. С учетом полученных в ходе анализа закономерностей значения адресов образуют массивы данных для каждой группы.

Элементы каждого образованного массива проходят проверку соответствия с адресом, у которого зафиксированы разряды, соответствующие определённой группе. Таким образом образуется пара масок (маска единиц и маска нулей). Маски сравниваются со значением адреса, пришедшего на вход программы согласно условию, описанному выше:

(Маска единиц | Адрес = Маска единиц) & (Маска нулей & Адрес = Маска нулей).

После завершения данных операций проводится поиск значения, которое удовлетворяет условиям для всех групп, которые соответствуют изменению координат относительно оси абсцисс, и выносится его индекс. Такая же процедура предусмотрена для групп, соответствующих изменению координат относительно оси ординат. В блок замены массива заносятся найденные индексы строк и столбцов. Таким образом, в двумерном массиве появляется булева константа ИСТИНА, иллюстрирующая расположение координаты сбившейся ячейки памяти. Результатом перебора всего

множества адресов, пришедших на вход программы, является двумерный массив булевых констант, значения ИСТИНА которого демонстрируют координаты сбившихся ячеек памяти.

5. Основные результаты апробации алгоритма

С помощью лазерной установки ПИКО-3 проведено облучение кристалла по заданным размерам пятна и шага сканирования. Результаты облучения занесены в лог-файл, в каждом абзаце которого располагаются адреса облученных частей кристалла и координаты точек, в которых эти части были получены. Кроме того, в программном обеспечении на лазерной установке проиллюстрировано изображение координат сбившихся ячеек памяти (рис. 4).

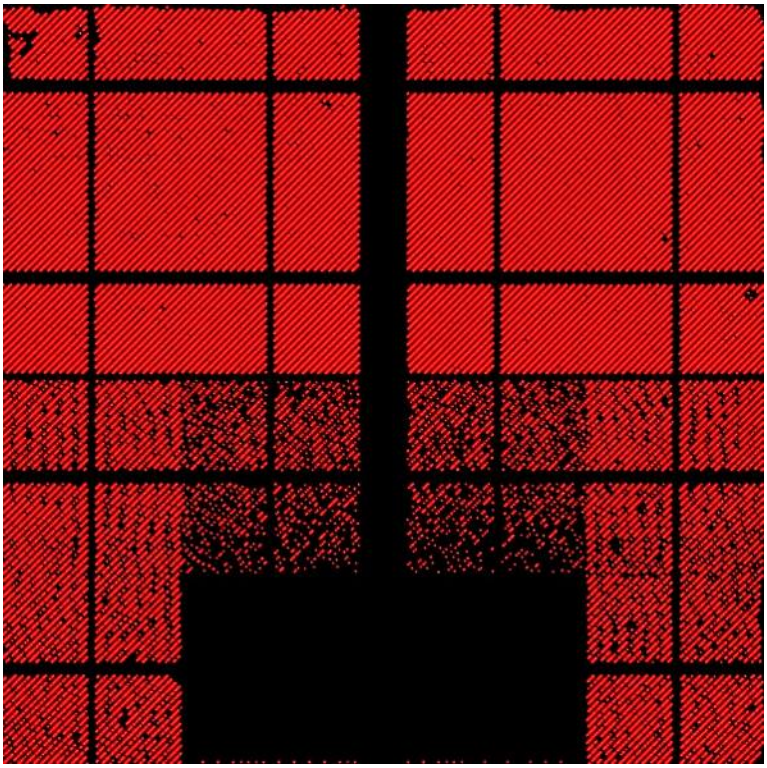


Рис. 4. Изображение координат сбившихся ячеек памяти, полученное в ПО на сфокусированной лазерной установке
(Fig. 4. Image of the coordinates of upsets in memory cells obtained by software on a focused laser system)

На рис. 4 видно, что в нижней области нет отображения некоторых координат (чёрный прямоугольник). Связано это с нехваткой энергии при лазерном облучении данного участка памяти.

Занесенные в лог-файл адреса облученных частей кристалла и соответствующие им координаты были поданы на вход программы формирования карты сбоев. Полученные данные дали возможность построить карту сбоев, представленную на рис. 5. Карта в точности иллюстрирует изображение, полученное на сфокусированной лазерной установке.

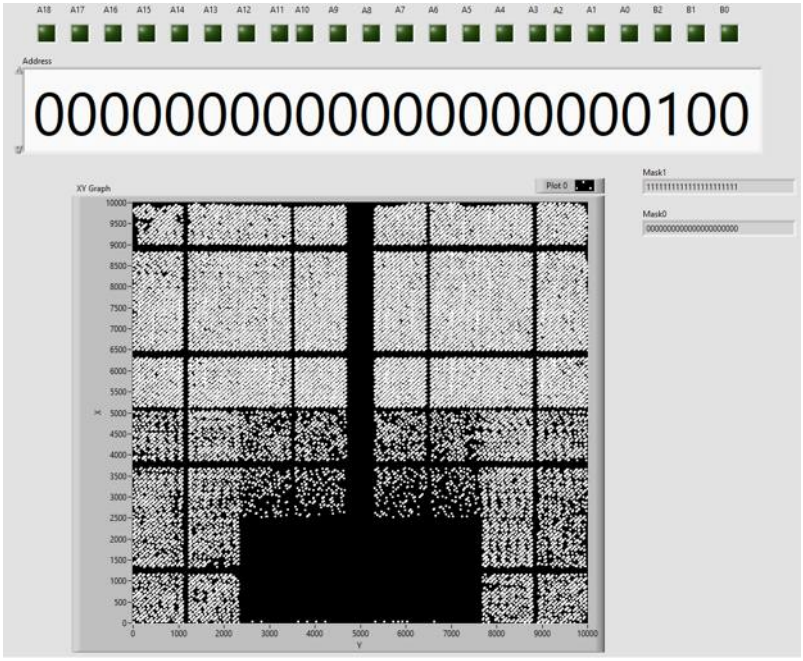


Рис. 5. График координат облученных ячеек памяти
(Fig. 5. The plot of the coordinates of the irradiated memory cells)

Анализ полученной карты проводился с помощью программы формирования карты сбоев и привёл к следующим выводам:

- При переборе значений трех старших разрядов адреса наблюдается разделение микросхемы на 8 пар равных блоков памяти симметричных относительно оси ординат (B0–B7 на рис. 6).
- При переборе значений трех старших и трех младших разрядов наблюдается разделение микросхемы на 64 равных сегмента памяти размером 128x512 бит.
- При переборе значений разрядов A0–A6 наблюдается перемещение координат относительно оси ординат.
- При переборе значений разрядов A7–A15 наблюдается перемещение координат относительно оси абсцисс.

Схематическое изображение полученных закономерностей представлено на рис. 6.

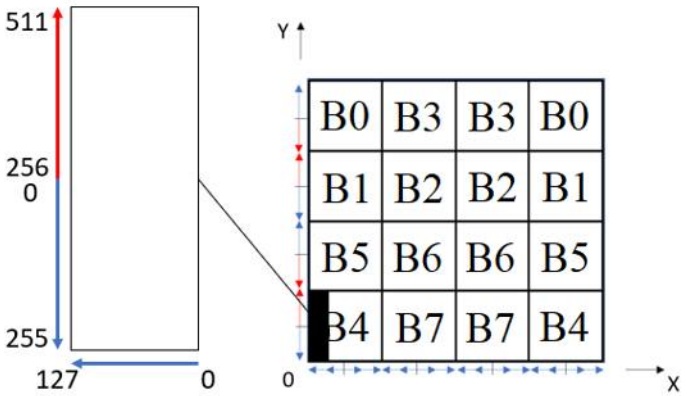


Рис. 6. Схематическое изображение полученных закономерностей расположения ячеек памяти
(Fig. 6. Schematic representation of the obtained patterns of the locations of memory cells)

Стрелки вдоль осей абсцисс и ординат показывают, в каком направлении происходит смещение координат при увеличении значения адреса. Таким образом, учитывая симметрию расположения блоков и сегментов памяти, можно однозначно устанавливать расположение ячеек памяти с точностью до 1-го бита информации.

Результаты, полученные в ходе анализа, при сравнении с данными от изготовителя подтвердились.

6. Применение алгоритма для анализа результатов при воздействии импульсного ИИ

Воздействие проводилось на источнике лазерного излучения РАДОН-8, предназначенного для моделирования эффектов мощности дозы ионизирующего излучения на интегральные схемы. В ходе эксперимента контролировалась сохранность информации микросхемы памяти. Воздействие проводилось на весь кристалл со стороны приборного слоя.

Результат, полученный при помощи программы вывода изображения в ходе эксперимента, представлен на рис. 7 (ячейки памяти, подвергшиеся воздействию импульсного ИИ выделены красным цветом, остальные ячейки – зеленым). Видно, что при одинаковом уровне воздействия на всю площадь кристалла, подавляющее большинство сбившихся ячеек памяти приходится на его центр. Отсюда вывод, что ячейки памяти, находящиеся ближе к центру, сбиваются при меньшем уровне воздействия чем те, которые находятся на периферии. Данный результат может быть полезен при исследованиях эффекта «просадки питания на внутренних шинах» (Rail span collapse) [4, 5].

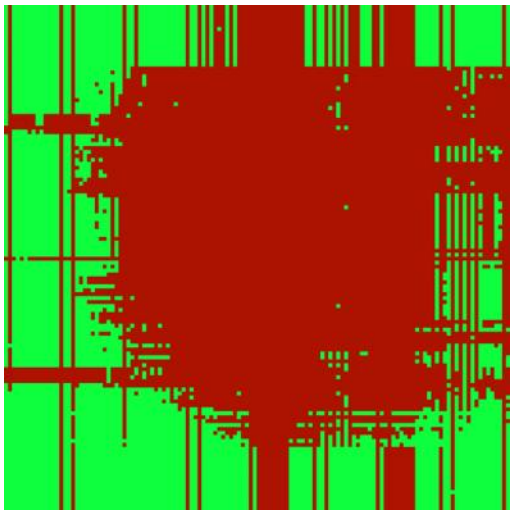


Рис. 7. Результат воздействия импульсного ИИ на микросхему СОЗУ
(Fig. 7. The result of the impact of pulsed ionizing radiation on the SRAM chip)

Заключение

В статье продемонстрирован разработанный алгоритм соотнесения физической и логической адресаций в микросхемах памяти с помощью источников лазерного излучения, а также представлен аппаратно-программный комплекс для его реализации. Разработан инструмент визуализации карты сбоев для возможности оперативного анализа на карте логической и физической адресаций.

Проведена апробация алгоритма на сфокусированной лазерной установке при заданных диаметре пятна 3 мкм и шаге сканирования 100 мкм в микросхеме СОЗУ

ёмкостью 4 Мбит с проектными нормами 180 нм. Результаты апробации выведены на карту сбоев.

Проведён анализ особенностей топологии исследуемого объекта при помощи данных на карте сбоев, полученных на сфокусированной лазерной установке. Результаты анализа подтвердили возможность разработки системы с точностью до 1 бита информации.

Представлено применение инструмента визуализации карты сбоев на примере исследования стойкости микросхемы СОЗУ к воздействию импульсного ИИ на источнике лазерного излучения РАДОН-8.

СПИСОК ЛИТЕРАТУРЫ:

1. Чумаков, А.И. Радиационная стойкость изделий ЭКБ [Текст] / А.И. Чумаков // Общая характеристика ионизирующих излучений: сб. статей. – М.: НИЯУ МИФИ, 2015. – 512 с.
2. Барбашов, В.М.; Трушкин, Н.С. Оценка надежности цифровых ис при воздействии радиации. Безопасность информационных технологий, [S.l.]. Т. 23, № 3. С. 11–19, oct. 2016. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/13 (дата обращения: 15.08.2020).
3. Романова И.К. Современные методы визуализации многомерных данных: анализ, классификация, реализация, приложения в технических системах [Текст] / И.К. Романов – М.:, Наука и Образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2016. № 03. С. 133–167. URL: https://cyberleninka.ru/article/n/sovremennye-metody-vizualizatsii-mnogomernyh-dannyh-analiz-klassifikatsiya-realizatsiya-prilozheniya-v-tehnicheskih-sistemah (дата обращения: 15.08.2020).
4. A.B. Boruzdina et al., "Temperature Dependence of MCU Sensitivity in 65 nm CMOS SRAM," in IEEE Transactions on Nuclear Science. Vol. 62, no. 6. P. 2860–2866, Dec. 2015. DOI: https://doi.org/10.1109/TNS.2015.2499120.
5. D.G. Mavis, D.R. Alexander and G.L. Dinger, "A chip-level modeling approach for rail span collapse and survivability analyses," in IEEE Transactions on Nuclear Science. Vol. 36, no. 6. P. 2239–2246, Dec. 1989. DOI: https://doi.org/10.1109/23.45430.
6. Согоян А.В., Чумаков А.И. Диффузионная модель ионизационной реакции элементов БИС при воздействии ТЗЧ, «Микроэлектроника». // Микроэлектроника. 2017. Т. 46. № 4. С. 305–312. DOI: https://doi.org/10.7868/S0544126917040081.
7. P.K. Skorobogatov, G.G. Davydov, A.A. Pechenkin, D.V. Boychenko. Behavior of modern integrated circuits after latch-up parrying. RAD Conference Proceedings. Vol. 2. P. 159–162, 2017. DOI: https://doi.org/10.21175/RadProc.2017.32.
8. Боруздина А.Б. Методики экспериментальных исследований многократных сбоев в КМОП микросхемах статических оперативных запоминающих устройств при возведении отдельных ядерных частиц [Текст]: автореферат диссертации на соиск. учен. степ. канд. техн. наук (05.13.05) / Боруздина Анна Борисовна; НИЯУ «МИФИ». – Москва, 2015. – 25 с.
9. J.N. Bradford, "Geometric Analysis of Soft Errors and Oxide Damage Produced by Heavy Cosmic Rays and Alpha Particles," in IEEE Transactions on Nuclear Science. Vol. 27, no. 1. P. 941–947, Feb. 1980. DOI: https://doi.org/10.1109/TNS.1980.4330955.
10. D. Giot, P. Roche, G. Gasiot, J. Autran and R. Harboe-Sorensen, "Heavy Ion Testing and 3-D Simulations of Multiple Cell Upset in 65 nm Standard SRAMs," in IEEE Transactions on Nuclear Science. Vol. 55, no. 4. P. 2048–2054, Aug. 2008. DOI: https://doi.org/10.1109/TNS.2008.916063.
11. Чумаков, Александр И. Возможности и ограничения лазерных методов при оценке параметров чувствительности бис к эффектам воздействия тяжелых заряженных частиц. Безопасность информационных технологий, [S.l.]. Т. 26, № 3. С. 58–67, сен. 2019. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1217 (дата обращения: 15.08.2020). DOI: http://dx.doi.org/10.26583/bit.2019.3.05.
12. Лазерная установка ПИКО-3. URL: http://www.spels.ru/index.php?option=com_content&view=article&id=344:2017-04-20-09-07-42&catid=43:ntk&Itemid=54. (дата обращения: 15.08.2020).
13. Лазерная установка РАДОН-8. URL: http://www.spels.ru/index.php?option=com_content&view=article&id=346:2017-04-20-09-07-42&catid=43:ntk&Itemid=54 (обращения: 15.08.2020).

REFERENCES:

[1] Chumakov A.I. Radiation resistance of electronic component base products. General characteristics of ionizing radiation: collection of articles., Moscow: National research nuclear University MEPhI, 2015. – 512 p. (in Russian).

[2] Barbashov, V.M.; Trushkin, N.S. The digital ics reliability assessment under the influence of radiation. IT Security (Russia), [S.l.]. V. 23, no. 3. P. 11–19, oct. 2016. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/13 (accessed: 15.08.2020) (in Russian).

[3] Romanova I.K. Modern Methods of Multidimensional Data Visualization: Analysis, Classification, Implementation, and Applications in Technical Systems. Science and Education of the Bauman MSTU, 2016, no. 03. P. 133–167. URL: https://cyberleninka.ru/article/n/sovremennye-metody-vizualizatsii-mnogomernyh-dannyh-analiz-klassifikatsiya-realizatsiya-prilozheniya-v-tehnicheskih-sistemah (accessed: 15.08.2020) (in Russian).

[4] A.B. Boruzdina et al., "Temperature Dependence of MCU Sensitivity in 65 nm CMOS SRAM," in IEEE Transactions on Nuclear Science. Vol. 62, no. 6. P. 2860–2866, Dec. 2015. DOI: https://doi.org/10.1109/TNS.2015.2499120.

[5] D.G. Mavis, D.R. Alexander and G.L. Dinger, "A chip-level modeling approach for rail span collapse and survivability analyses," in IEEE Transactions on Nuclear Science. Vol. 36, no. 6. P. 2239–2246, Dec. 1989. DOI: https://doi.org/10.1109/23.45430.

[6] Sogoyan A.V., CHumakov A.I. Diffusion model of the ionization reaction of BIS elements under the influence of TCH, "Microelectronics". Mikroelektronika. 2017. Vol. 46, no 4. P. 305–312. DOI: https://doi.org/10.7868/S0544126917040081 (in Russian).

[7] P.K. Skorobogatov, G.G. Davydov, A.A. Pechenkin, D.V. Boychenko. Behavior of modern integrated circuits after latch-up parrying. RAD Conference Proceedings. Vol. 2. P.159–162, 2017. DOI: https://doi.org/10.21175/RadProc.2017.32.

[8] Boruzdina A.B. Methods of experimental research of multiple failures in CMOS chips of static RAM storage devices under the influence of individual nuclear particles: abstract of the dissertation for the competition. scientist. step. Cand. tech. sciences (05.13.05) / Boruzdina Anna Borisovna; Moscow: National research nuclear University MEPhI, 2015. – 25 p.

[9] J.N. Bradford, "Geometric Analysis of Soft Errors and Oxide Damage Produced by Heavy Cosmic Rays and Alpha Particles," in IEEE Transactions on Nuclear Science. Vol. 27, no. 1. P. 941–947, Feb. 1980. DOI: https://doi.org/10.1109/TNS.1980.4330955.

[10] D. Giot, P. Roche, G. Gasiot, J. Autran and R. Harboe-Sorensen, "Heavy Ion Testing and 3-D Simulations of Multiple Cell Upset in 65 nm Standard SRAMs," in IEEE Transactions on Nuclear Science. Vol. 55, no. 4. P. 2048–2054, Aug. 2008. DOI: https://doi.org/10.1109/TNS.2008.916063.

[11] Chumakov, Alexander I. Possibilities and limitations of focused laser technique application for SEE sensitivity parameters estimation. IT Security (Russia), [S.l.]. V. 26, no 3. P. 58–67, sep. 2019. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1217 (accessed: 15.08.2020). DOI: http://dx.doi.org/10.26583/bit.2019.3.05.

[12] Laser installation PIKO-3. URL: http://www.spels.ru/index.php?option=com_content&view=article&id =344:2017-04-20-09-07-42&catid=43:ntk&Itemid=54. (date of access 15.08.2020) (in Russian).

[13] Laser installation RADON-8. URL: http://www.spels.ru/index.php?option=com_content&view=article&id =346:2017-04-20-09-07-42&catid=43:ntk&Itemid=54 (date of access 15.08.2020) (in Russian).

Поступила в редакцию – 26 июля 2020 г. Окончательный вариант – 20 августа 2020 г.
Received – July 26, 2020. The final version – August 20, 2020.

Сергей В. Дуга[1], Андрей И. Труфанов[2]
[1]Экспертно-криминалистический отдел, Следственное управление Следственного комитета Российской Федерации по Иркутской области,
Клары Цеткин ул., 9а, Иркутск, 664039, Россия.
[2]Иркутский национальный исследовательский технический университет,
Лермонтова ул., 83, Иркутск, 664074, Россия
[1]e-mail: siber@list.ru, http://orcid.org/0000-0002-5894-9855
[2]e-mail: troufan@gmail.com, http://orcid.org/0000-0002-6967-3495

СЕТЬ ЗНАНИЙ КАК КОНЦЕПЦИЯ СИСТЕМ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЯ В ПРЕДВАРИТЕЛЬНОМ СЛЕДСТВИИ

DOI: http://dx.doi.org/10.26583/bit.2020.3.05

Аннотация. В настоящее время интеллектуальный анализ данных является важным инструментом для расследования преступлений. В статье предлагается извлечение криминалистически значимых сведений из неструктурированных данных, с использованием методов сетевого анализа (анализа графов). Рассмотрены частные определения термина «Knowledge Graph» (граф знаний), дано обобщающее авторское определение понятия «сети знаний». Раскрыта позиция сети знаний в общем контексте науки о сетях. На реальных примерах показано, каким образом сетевые (графовые) модели данных могут эффективно использоваться в предметной области предварительного следствия. Обсуждаются уровни реализации (сбор, хранение, анализ и визуализация) и основные преимущества концепции. Результаты сетевого интеллектуального анализа данных могут быть использованы для выявления закономерностей, извлечения неопределенных (неочевидных) данных, что в свою очередь будет способствовать раскрытию преступления.

Ключевые слова: информатизация расследования, сеть знаний, графовая модель данных, комплексные сети, сетевой анализ.
Для цитирования: ДУГА, Сергей В.; ТРУФАНОВ, Андрей И. СЕТЬ ЗНАНИЙ КАК КОНЦЕПЦИЯ СИСТЕМ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЯ В ПРЕДВАРИТЕЛЬНОМ СЛЕДСТВИИ. Безопасность информационных технологий, [S.l.], v. 27, n. 3, p. 54–65, 2020. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1292>. Дата доступа: 01 sep. 2020. DOI: http://dx.doi.org/10.26583/bit.2020.3.05.

Sergey V. Duga[1], Andrey I. Trufanov[2]
[1]Investigation Department, Investigative Committee of the Russian Federation Irkutsk Region,
K.Tsetkin str., 9a, Irkutsk, 664039,Russia
[2]Irkutsk National Research Technical University,
Lermontova str., 83, Irkutsk, 664074, Russia
[1]e-mail: siber@list.ru, http://orcid.org/0000-0002-5894-9855
[2]e-mail: troufan@gmail.com, http://orcid.org/0000-0002-6967-3495

The knowledge graph concept of decision support system in preliminary investigation

DOI: http://dx.doi.org/10.26583/bit.2020.3.05

Abstract. Particular definitions of the concept of "Knowledge Graph" (knowledge network) are considered, and a generalizing author's definition of the concept of "knowledge networks" is given. The position of the knowledge network in the general context of network science is revealed. Real-world examples show how network (graph) data models can be effectively used in the subject area of preliminary investigation. The levels of implementation and the main advantages of the concept are discussed.

Keywords: informatization of investigations, knowledge graph, graph data model, complex networks, network analysis.

For citation: DUGA, Sergey V.; TRUFANOV, Andrey I. The knowledge graph concept of decision support system in preliminary investigation. IT Security (Russia), [S.l.], v. 27, n. 3, p. 54–65, 2020. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1292>. Date accessed: 01 sep. 2020. DOI: http://dx.doi.org/10.26583/bit.2020.3.05.

Введение

В последнее время отечественное научное сообщество все больше внимания уделяет применению искусственных нейронных сетей в расследовании преступлений. В частности, в каждой из работ [1–5] делается попытка по-своему раскрыть понятие «искусственный интеллект» в контексте противодействия преступности, его применение по предупреждению преступности.

В целом, в своих попытках авторы надеются, что внедрение подобных систем может не только использоваться в качестве предупредительно-профилактических мер, но и улучшить качество предварительного следствия, сократить его сроки, и, как следствие, повысить имидж и доверие граждан к правоохранительным органам.

В работе [6], авторы определяют три направления расследования преступлений, в которых могут применяться системы искусственного интеллекта – «распознавание (визуальных образов и связей между объектами криминалистического познания), предсказание и классификация». Для достижения результатов, авторами предлагается «сформировать набор данных прикладной области, после чего обучить искусственную нейронную сеть с помощью алгоритмов машинного обучения».

В работе [7], автор предлагает объединение всех баз данных и учётов, ведущихся в МВД России, а также разработку на основе искусственного интеллекта системы ввода полной информации о правонарушениях и преступлениях путём сканирования материалов уголовных дел, материалов об административных правонарушениях. Автор предполагает, что внедрение подобной системы способно значительно повысить качество расследования преступлений.

В то же время нельзя не отметить, что применение систем искусственного интеллекта не должно подменять собой человека, но должно быть направлено на оказание содействия в его повседневной деятельности. Более того, со стороны государства необходимо правовое регулирование, выработка государственной политики в отношении искусственного интеллекта.

Нами предлагается создание системы поддержки принятия решения в предварительном следствии [8], в которой, за счет объединения методов машинного обучения и теории комплексных сетей, реализован мощный аналитический инструмент. Внедрение системы будет содействовать следователям в повседневной деятельности, предоставит возможность анализа получаемых сведений как в рамках расследуемого уголовного дела, так и в контексте других уголовных дел. В результате накопленных системой сведений предполагается формировать т.н. «сеть знаний». Аналог этого понятия в англоязычной терминологии «Knowledge Graph», буквально «граф знаний». Однако на наш взгляд, «сеть знаний» в русской транскрипции в наилучшей степени отражает свойства рассматриваемой сущности и связанные с ней явления и процессы.

Термин «Knowledge Graph» (сеть знаний) стал набирать популярность с 2012 года, после публикации корпорацей «Google» о своей семантической технологии «Google’s Knowledge Graph», расширяющую известную поисковую систему, в частности, позволяющую устранить смысловую неоднозначность поискового запроса [9].

Важно, что интерес к данной тематике прослеживается с середины семидесятых годов прошлого века. В [10] дается определение «Knowledge Graph» (сеть знаний) как «математической структуры с вершинами - единицами знаний, соединенных ребрами,

которые представляют отношения». Хотя в последующие годы и было опубликовано большое количество работ [11–18], самым различным образом формулирующих частные определения «Knowledge Graph» (сеть знаний), в т.ч. и Википедия [19], на сегодняшний день общепринятого формального определения этого понятия не существует.

В своем исследовании мы предлагаем и используем следующее определение «сети знаний»: это крупномасштабная сеть, описывающая сущности реального мира (с указанием семантического типа и свойств), а также отношения между ними (также наделенными свойствами), охватывающая определенную предметную область. Таким образом, сеть знаний организует информацию в структурированном виде путем явного описания отношений между сущностями.

Формально сеть знаний можно описать как $G = \{E, R, F\}$, где E – набор узлов, R – набор связей, F – факты. Факт обозначается триплетом $(h, r, t) \in F$. Каждый триплет связывает две сущности h (субъект) и t (объект) через отношение r (предикат), а также дополнительную информацию, связанную с триплетом, представленную как ключ-значение (k, v) [20].

Сущности реального мира разнообразны и взаимосвязаны. Инструменты науки о сетях [21], включающие теорию графов, теорию вероятностей и линейную алгебру, являются эффективным средством при изучении реальных, сложных систем, таких как технологические, социальные, информационные и др. Сложные сущности практически любой предметной области могут быть представлены сетевыми структурами. Сети являются простым и мощным способом представления моделей связей и взаимодействий между частями системы.

Понятно, что связи в сети могут быть направленными или ненаправленными. Некоторые системы имеют направленные связи, например, электронное письмо, направленное от одного человека к другому. Иные сетевые системы имеют ненаправленные связи, такие как линии электросети, по которым электрический ток может течь в обоих направлениях [22].

Кроме того, узлы и связи в сети могут содержать какую-либо дополнительную информацию (свойства), например, тип, имя, вес связи и т.д., для большей детализации системы.

В табл. 1 приведены некоторые примеры представления различных систем в виде сети.

Таблица 1.

Сеть	**Узлы**	**Связи**
WWW	Веб-страницы	Ссылки
Звонки	Абонент	Звонок
Сеть цитирования	Статьи	Цитаты
Научное сотрудничество	Ученые	Соавторство

Сетевые (графовые) модели являются подходящим инструментом при анализе самых разных наборов данных, в частности [23–26].

Хотя термин «Knowledge Graph» чаще всего ассоциируется с «Google», сети знаний используются не только поисковыми системами. В табл. 2 приведены примеры использования сетей знаний в крупнейших ИТ-компаниях [27].

Таблица 2.

Компания	**Размер графа**	**Стадия разработки**
Microsoft	~ 2 миллиарда вершин	Активно используется в продуктах
Google	1 миллиард вершин	Активно используется в продуктах
Facebook	~ 50 миллиардов вершин	Активно используется в продуктах
eBay	Ожидается около 100 миллионов вершин	Ранние стадии разработки и внедрения
IBM	> 100 миллионов вершин	Активно используется в продуктах

Более того, сегодня сети знаний применяются и в правительственных организациях. Так, при помощи графовой модели, Министерство обороны США отслеживает и анализирует расходы на техническое обслуживание оборудования (от вертолетов и бронированных машин до стрелкового оружия и радиоприемников) [28]. Техническое обслуживание и поддержка этого оборудования требует закупки миллионов запасных частей в год. После внедрения графовой базы данных, Министерство обороны США имеет гораздо более гибкое и надежное представление о требованиях к деталям и стоимости этих частей для всех систем, компонентов и подкомпонентов.

В НАСА сеть знаний [29] составлена из документов, являющихся источником информации для графа. НАСА использует обработку естественного языка для сканирования документов на предмет данных, включаемых в сеть знаний.

Эти данные включают в себя сотни миллионов документов, отчетов, проектных данных, извлеченных уроков, научных исследований, медицинского анализа и многое другое, хранящиеся в общенациональной базе данных.

При регистрации сложной технической проблемы, техническому специалисту отображаются самые похожие проблемы, обработанные ранее, алгоритм ее решения, и все связанные с ней документы. Благодаря этому решение проблемы значительно ускоряется. Отметим, что в наибольшей степени сети знаний отвечает модель в интерпретации комбинированных стволовых сетей [30], способных органично включить и описать разноплановые узлы, связи и факты.

Фактически, концепция сетей знаний осваивается немногочисленными отечественными исследователями [31], зачастую, в неявной и далекой от практики форме [32–33].

1. Предметная область

Сети и их инструмент – графы могут быть использованы для эффективного анализа данных. Намерение, следующее за настоящим обзором, состоит в использовании графовой базы данных для хранения криминалистически значимых сведений, их анализа и визуализации.

При производстве по уголовному делу, следователь анализирует не только отдельные сущности (субъекты, события и т.д.), но и связи между ними.

Данные о преступлении (или преступлениях) могут быть представлены комплексной (сложной) сетью, поскольку они содержат различные отношения между сущностями реального мира, такими как люди, сведения о звонках, сведения о переписке, места, организации и т.д. Такое представление существенно облегчит проверку доказательств по уголовному делу, а именно «сопоставление их с другими доказательствами, имеющимися в уголовном деле, а также установления их источников» (УПК РФ Статья 87).

В [34] предлагается модель данных для расследования преступления «POLE» (рис. 1). «POLE» означает Persons (субъекты), Objects (объекты), Locations (места) и Events (события).

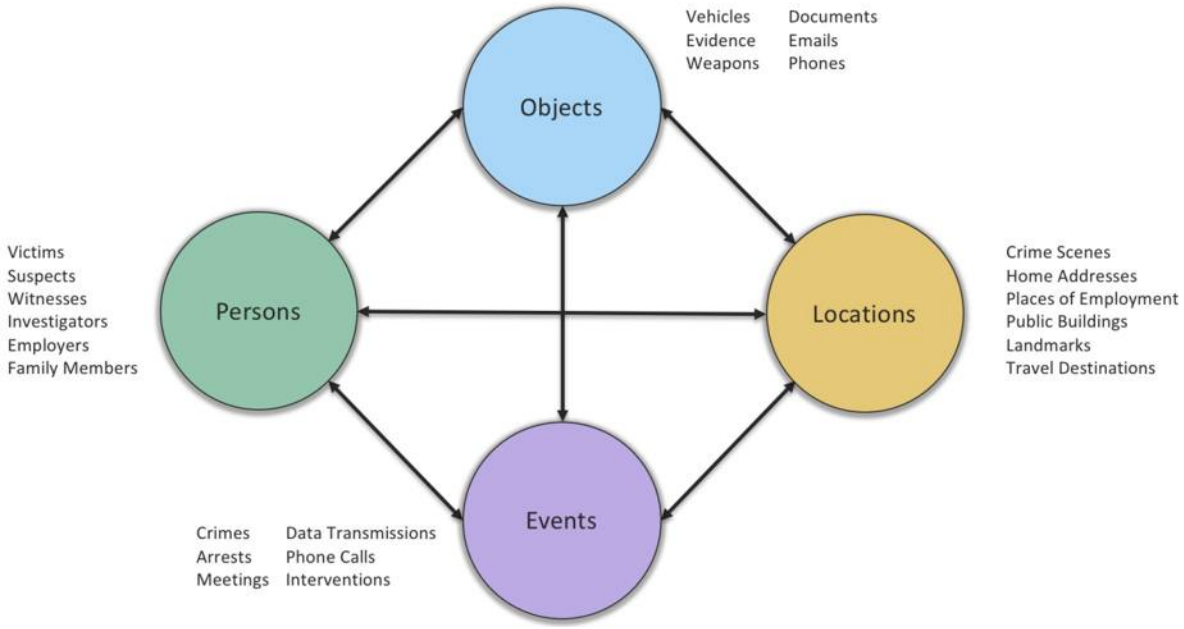


Рис. 1. Модель данных «POLE»
(Fig.1. The "POLE" data model)

В данной модели используются следующие семантические типы узлов:

1. Субъекты. В качестве субъектов могут выступать потерпевшие по уголовному делу, подозреваемые и обвиняемые в совершении преступления, свидетели преступления и т.д.

2. События – время, место, способ и другие обстоятельства совершения преступления, обстоятельства, способствовавшие совершению преступления (УПК РФ Статья 73), а также иные обстоятельства, имеющие значение для уголовного дела (встречи людей, телефонные звонки, передача данных и пр.).

3. Объектами могут быть любые предметы, которые служили орудиями, оборудованием или иными средствами совершения преступления, предметы и документы, которые могут служить средствами для обнаружения преступления и установления обстоятельств уголовного дела (УПК РФ Статья 81).

4. Места – место совершения преступления, домашний/рабочий адрес человека, адрес регистрации юридического лица и пр.

Представление модели данных «POLE» в виде графа представлено на рис. 2.

Другим примером успешного использования графовых баз данных в расследовании являются исследования «Международного консорциума журналистов-расследователей» (The International Consortium of Investigative Journalists (ICIJ)), которые выявили много интересных закономерностей, включая потенциально незаконную деятельность президента Азербайджана [35].

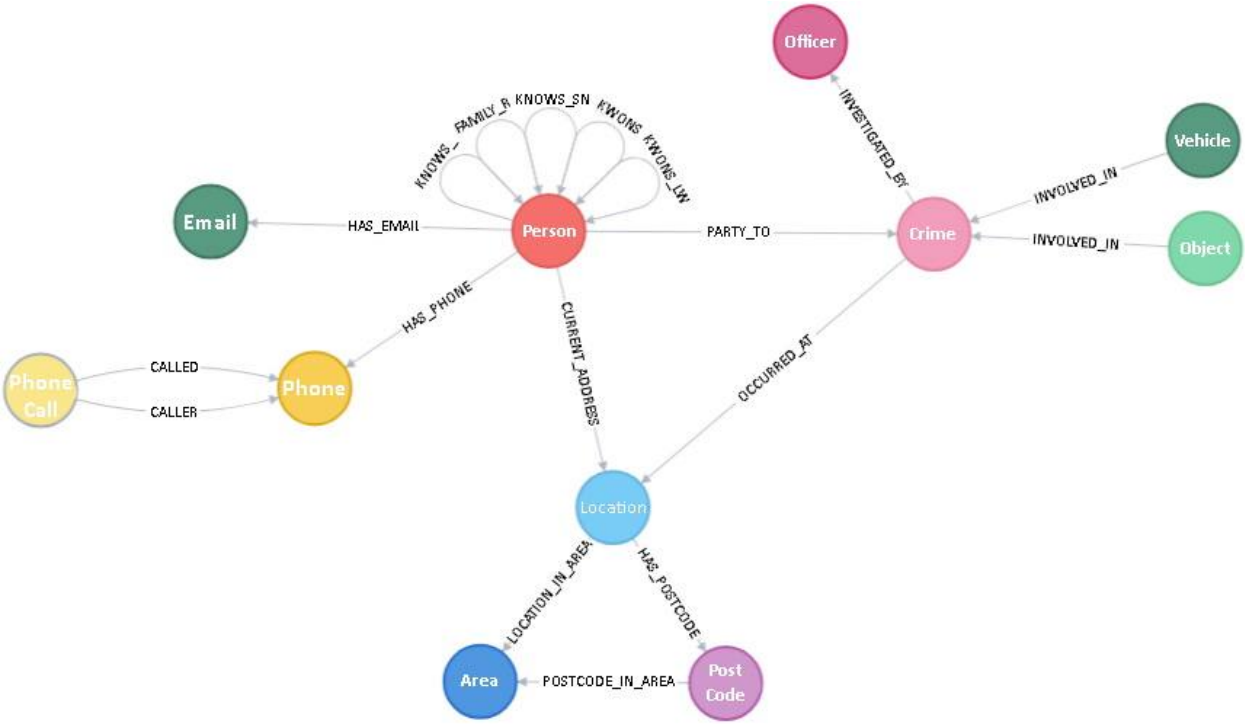


Рис. 2. Представление модели данных «POLE» в виде графа
(Fig. 2. Representation of the "POLE" data model as a graph)

Для понимания сложных данных в наборе данных «ICIJ Offshore Leaks» [36], была построена сетевая (графовая) модель. В данной модели используются следующие семантические типы узлов и связей:

Узлы:

1. Субъект (Person) – люди, которые строят и используют сеть активов.
2. Компания (Company) – компании включают оффшорные компании, поставщиков банковских услуг и предприятия.
3. Адрес (Address) – это места регистрации людей и компаний. Поскольку они имеют юридическую значимость (компания, зарегистрированная в офшоре, платит налогов меньше или вовсе их не платит), адреса могут дать интересную информацию.

Связи:

1. Субъект – Адрес и Компания – Адрес (USES_ADDRESS). Связывает людей и компании по адресам.
2. Субъект – Семья – Субъект (FAMILY). Люди могут быть связаны через семейные узы.
3. Субъект – Связь с – Компания (IS_LINKED_TO). Связь человека с компанией. Также связи между людьми и компаниями имеют свойство «роль» (директор, учредитель и т.д.).
4. Компания – Связь с – Компания (IS_LINKED_TO). Отображает, как первая компания связана со второй компанией. Связь также имеет свойство «роль».
5. Компания – Офшор – Компания (IS_OFFSHORE_PROVIDER_OF). Отображает связь компании с компанией, предоставляющей услуги оффшорной системы.

Полученная сетевая (графовая) модель представлена на рис. 3.

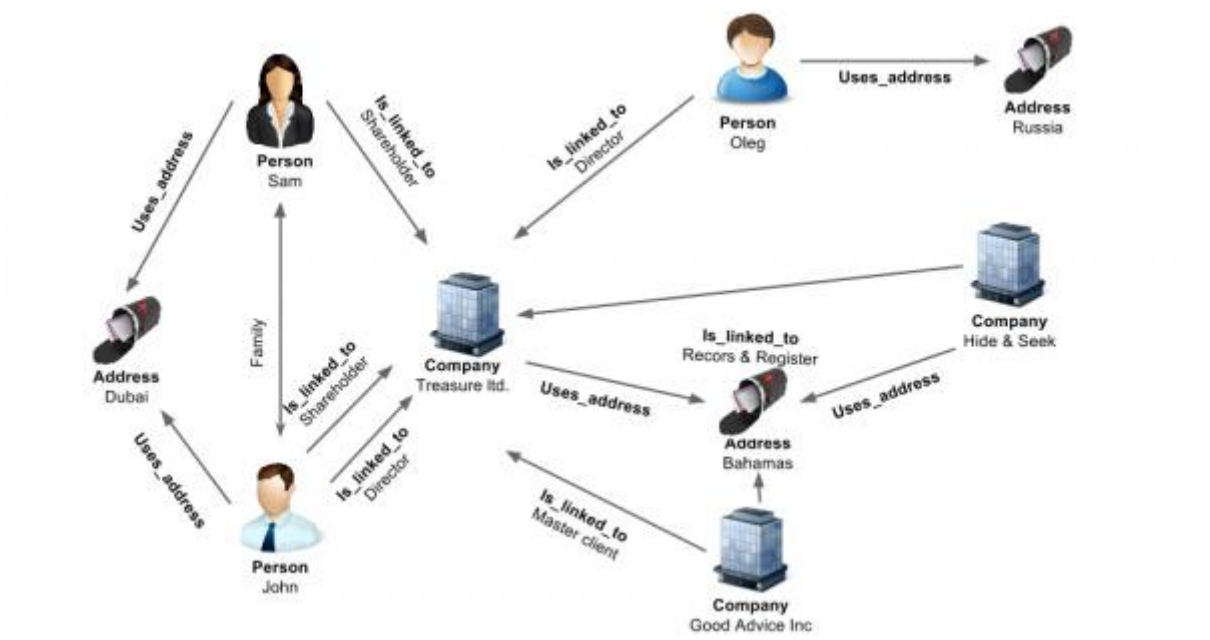


Рис. 3. Сетевая (графовая) модель набора данных «ICIJ Offshore Leaks»
(Fig. 3. Network (graph) model of the "ICIJ Offshore Leaks" data set)

Таким образом, уже сейчас можно с уверенностью утверждать, что сетевые (графовые) модели данных могут эффективно использоваться в рассматриваемой нами предметной области предварительное следствие.

2. Уровни реализации

Модель

Предлагается использовать модель данных, основанную на ориентированных графах с метками.

Модель данных, основанная на ориентированных графах с метками – это среда описания ресурса (Resource Description Framework, RDF), которая разработана и поддерживается консорциумом Всемирной паутины (W3C) [37]. RDF – это общий метод описания данных путем определения отношений между объектами данных. RDF-выражение состоит из субъекта, предиката и объекта.

База данных

В качестве базы данных нами предлагается использовать одну из графовых баз данных, например, [38–40] и др.

Графовые базы данных отлично подходят для:

- когда данные не содержат схемы;
- отношения в данных вносят смысл;
- динамических систем, в которых трудно предсказать топологию данных;
- требуется расширение по мере развития;
- хороши для сложных данных.

Кроме того, моделирование данных в виде графа обеспечивает большую гибкость для интеграции новых источников данных по сравнению со стандартной реляционной моделью, где схема должна быть определена заранее и отслеживаться на каждом этапе.

Язык запросов

Для запросов к базе данных могут быть использованы такие языки как Sparql, Gremlin и Cypher, которые используются для выбора подграфов и анализа.

Анализ

Для анализа могут быть применены различные методы анализа сетевых структур. Перечислим некоторые из них [41]:

– центральность: стремится идентифицировать наиболее значимые узлы или связи сети;

– обнаружение сообщества: цель состоит в том, чтобы идентифицировать сообщества сети, то есть кластеры, которые более плотно связаны внутри, чем с остальной частью сети;

– связность: стремится оценить, насколько хорошо связана сеть, показывая, например, устойчивость и (не) достижимость элементов сети;

– сходство узлов: стремится найти узлы, которые похожи на другие узлы в силу того, как они связаны внутри своего соседства;

– поиск пути: целью является поиск путей в сети, обычно между парами узлов, заданными в качестве входных данных.

Кроме того, векторное представление узлов и связей позволяют применять стандартные методы анализа данных и машинного обучения к сетевым структурам [42]. Машинное обучение может использоваться для уточнения самой сети знаний – прогнозирование новых связей или выявление ошибочных. Сеть знаний также может служить набором данных для обучения моделей.

Для примера, можно использовать методы машинного обучения для определения недостающей информации, когда, учитывая два элемента триплета, необходимо предсказать недостающий: (?, *r, t*), (*h,* ?*, t*) или *(h, r,* ?*)* [43].

Визуализация

Ввиду того, что в разрабатываемой нами системе конечными пользователями являются следователи и криминалисты, не владеющие языками программирования и запросов, пользовательский интерфейс должен обеспечивать графическое представление сети и позволять выполнить визуальный анализ.

Заключение

В последнее время наблюдается растущий интерес к применению методов искусственного интеллекта в расследовании преступлений. Ожидается, что такие методы, используемые для обработки и прогнозирования данных, могут улучшить производительность, скорость и точность процесса расследования преступлений.

В свою очередь, мы считаем, что применение сети знаний в предварительном следствии позволит улучшить процесс принятия решений, извлекать интересующие шаблоны, а графическое представление сети позволит выполнить визуальный анализ накопленных сведений.

Моделирование данных в виде сети обеспечивает большую гибкость для интеграции новых источников данных, а также позволит проводить интеллектуальный анализ текста, извлечение сущностей и анализ социальных сетей.

Сеть знаний может использоваться не только для накопления знаний, но и для вывода новых фактов.

Однако, стоит отметить препятствия, связанные с применением этих методов, в частности, формулирование государственной политики в отношении искусственного интеллекта.

СПИСОК ЛИТЕРАТУРЫ:

1. Суходолов А.П., Бычкова А.М. Искусственный интеллект в противодействии преступности, ее прогнозировании, предупреждении // Всероссийский криминологический журнал. 2018. Т. 12. № 5. С. 753–766. DOI: https://doi.org/10.17150/2500-4255.2018.12(6).753-766.
2. Мазуров В.А., Стародубцева М.А. Искусственный интеллект как средство прогнозирования и противодействия преступности // Российско-азиатский правовой журнал. 2019. № 3. С. 46–50. URL: http://journal.asu.ru/ralj/article/view/6991 (дата обращения: 17.06.2020).
3. Кравцов Д.А. Искусственный разум: предупреждение и прогнозирование преступности // Вестник Московского университета МВД России. 2018. № 3, С. 108–110. URL: https://cyberleninka.ru/article/n/iskusstvennyy-razum-preduprezhdenie-i-prognozirovanie-prestupnosti (дата обращения: 24.06.2020).
4. Осипенко А.Л. Перспективы использования информационно-аналитических технологий в оперативно-розыскной деятельности // Общество и право. 2018. № 4. С. 80–87. URL: https://cyberleninka.ru/article/n/perspektivy-ispolzovaniya-informatsionno-analiticheskih-tehnologiy-v-operativno-rozysknoy-deyatelnosti (дата обращения: 23.06.2020).
5. Себякин А.Г. Искусственный интеллект в криминалистике: система поддержки принятия решений // Baikal Research Journal. 2019. Т. 10. № 4. С. 21–21. DOI: https://doi.org/10.17150/2411-6262.2019.10(4).21. URL: http://cj.bgu.ru/reader/article.aspx?id=23649 (дата обращения: 23.06.2020).
6. Степаненко Д.А., Бахтеев Д.В., Евстратова Ю.А. Использование систем искусственного интеллекта в правоохранительной деятельности // Всероссийский криминологический журнал. 2020. Т. 14, № 2, С. 206–214. DOI: https://doi.org/10.17150/2500-4255.2020.14(2).206-214.
7. Кузьмин И.А. Искусственные нейронные сети: перспективы использования в правоохранительной деятельности // Криминалистика: вчера, сегодня, завтра. 2018. № 4 (8). С. 109–116. URL: https://cyberleninka.ru/article/n/iskusstvennye-neyronnye-seti-perspektivy-ispolzovaniya-v-pravoohranitelnoy-deyatelnosti (дата обращения: 27.06.2020).
8. Дуга, Сергей В. и др. Концепция системы поддержки принятия решения в предварительном следствии. Безопасность информационных технологий, [S.l.]. Т. 26, № 3. С. 45–57, сен. 2019. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1216. (дата обращения: 27.06.2020). DOI: http://dx.doi.org/10.26583/bit.2019.3.04.
9. Singhal A. Introducing the knowledge graph: things, not strings. URL: https://www.blog.google/products/search/introducing-knowledge-graph-things-not (дата обращения: 16.05.2020).
10. Marchi E., Miguel O. On the Structure of the Teaching-learning Interactive Process // International Journal of Game Theory. 1974. Vol. 3. no. 2. P. 83–99. DOI: https://doi.org/10.1007/BF01766394.
11. R.R. Bakker. Knowledge Graphs: Representation and Structuring of Scientific Knowledge // Ph.D. thesis, University of Twente, Enschede. 1987.
12. P.H. de Vries. Representation of Science Texts in Knowledge Graphs // Ph.D. thesis, University of Groningen, Groningen, The Netherlands, 1989.
13. Zhang L. Knowledge graph theory and structural parsing // Twente University Press. 2002. C. 216. URL: https://ris.utwente.nl/ws/portalfiles/portal/6073799/t0000020.pdf (дата обращения: 27.05.2020).
14. Popping R. Knowledge graphs and network text analysis // Social Science Information. 2003. Vol. 42, no. 1. P. 91–106. DOI: https://doi.org/10.1177/0539018403042001798.
15. Lisa Ehrlinger, Wolfram Wöß. Towards a Definition of Knowledge Graphs // Joint Proceedings of the Posters and Demos Track of 12th International Conference on Semantic Systems - SEMANTiCS2016 and 1st International Workshop on Semantic Change & Evolving Semantics (SuCCESS16), Leipzig, Germany. 2016. URL: http://ceur-ws.org/Vol-1695/paper4.pdf (дата обращения: 01.07.2020).
16. Paulheim H. Knowledge graph refinement: A survey of approaches and evaluation methods // Semantic web. 2017. Vol. 8. no. 3. P. 489–508. DOI: https://doi.org/10.3233/SW-160218.
17. Chenyan Xiong. Text representation, retrieval, and understanding with knowledge graphs. // ACM SIGIR Forum. 2018. Vol. 52. no. 2. P. 180–181. DOI: https://doi.org/10.1145/3308774.3308808.
18. Bellomarini L. et al. Knowledge graphs and enterprise AI: the promise of an enabling technology // IEEE 35th International Conference on Data Engineering (ICDE). 2019. P. 26–37. DOI: https://doi.org/10.1109/ICDE.2019.00011.
19. Knowledge Graph. URL: https://ru.wikipedia.org/wiki/Knowledge_Graph (дата обращения: 01.07.2020).
20. Ji S. et al. A survey on knowledge graphs: Representation, acquisition and applications // arXiv preprint arXiv:2002.00388. 2020. URL: https://arxiv.org/abs/2002.00388 (дата обращения: 20.06.2020).

21. Molontay R., Nagy M. Twenty Years of Network Science: A Bibliographic and Co-authorship Network Analysis // arXiv preprint arXiv:2001.09006. 2020. URL: https://arxiv.org/abs/2001.09006 (дата обращения: 25.06.2020).
22. Albert-László Barabási, Márton Pósfai. Network Science // Cambridge University Press. 2016. – 475 p.
23. Saleh M., Esa Y., Mohamed A. Applications of complex network analysis in electric power systems // Energies. 2018. Vol. 11. № 6. DOI: https://doi.org/10.3390/en11061381.
24. Wu X. et al. Analysis of metro network performance from a complex network perspective // Physica A: Statistical Mechanics and its Applications. 2018. Vol. 492. P. 553–563. DOI: https://doi.org/10.1016/j.physa.2017.08.074.
25. Wachs-Lopes G. A., Rodrigues P. S. Analyzing natural human language from the point of view of dynamic of a complex network // Expert Systems with Applications. 2016. Vol. 45. P. 8–22. DOI: https://doi.org/10.1016/j.eswa.2015.09.020
26. Jiang Z. Y. et al. Vehicle demand evolution analysis from the complex network perspective // Physica A: Statistical Mechanics and its Applications. 2019. Vol. 532. DOI: https://doi.org/10.1016/j.physa.2019.121889.
27. Noy N. et al. Industry-scale knowledge graphs: Lessons and challenges // Queue. 2019. Vol. 17. no. 2. P. 48–75. DOI: https://doi.org/10.1145/3331166.
28. Graphs in Government – Fulfilling Your Mission with Neo4j. URL: https://www.paperpicks.com/graphs-in-government-fulfilling-your-mission-with-neo4j (дата обращения: 06.06.2020).
29. How NASA Finds Critical Data through a Knowledge Graph. URL: https://neo4j.com/blog/nasa-critical-data-knowledge-graph/?ref=blog (Дата обращения: 09.06.2020).
30. Ashurova Z, Tikhomirov A, Trufanov A, Kinash N, Berestneva O и Rossodivita. A 2017 Network platform of program governance for E-health service // 2017 12th Int. Sci. and Tech. Conf. on Computer Sciences and Information Technologies (CSIT), Lviv Ukraine. 2017. DOI: https://doi.org/10.1109/STC-CSIT.2017.8099429.
31. Тушканова О. Н., Самойлов В. В. Knowledge Net: модель и система накопления, представления и использования знаний и данных // Онтология проектирования. 2019. Т. 9. № 1. С. 117–131. DOI: https://doi.org/10.18287/2223-9537-2019-9-1-117-131.
32. Подружкина Т. А., Федоров Д. Ю. Алгоритмы планирования процесса обучения на основе семантических сетей знаний // Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». 2017. № 1. С. 107–116. URL: https://cyberleninka.ru/article/n/ispolzovanie-informatsionnyh-tehnologiy-dlya-obespe-cheniya-bezopasnosti-lichnosti-obschestva-i-gosudarstva (дата обращения: 23.06.2020).
33. Савченко А. П. Открытая сеть документированных знаний организации: концептуальная модель // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. 2014. № 103. URL: https://cyberleninka.ru/article/n/otkrytaya-set-dokumentirovannyh-znaniy-organizatsii-kontseptualnaya-model (дата обращения: 22.06.2020).
34. Announcing the Neo4j Crime Investigation Sandbox. URL: https://medium.com/neo4j/announcing-the-neo4j-crime-investigation-sandbox-c0c3bd9e71b1 (дата обращения: 30.06.2020).
35. Neo4j and the Offshore Leaks: the Case of Azerbaijan. URL: https://neo4j.com/graphgist/neo4j-and-the-offshore-leaks-the-case-of-azerbaijan (дата обращения: 02.07.2020).
36. ICIJ Offshore Leaks Database. URL: https://offshoreleaks.icij.org (дата обращения: 02.07.2020).
37. Richard Cyganiak, David Wood, Markus Lanthaler. RDF 1.1 Concepts and Abstract Syntax, W3C Recommendation 25 February 2014. URL: https://www.w3.org/TR/2014/REC-rdf11-concepts-20140225 (дата обращения: 03.07.2020).
38. HypergraphDB - A Graph Database. URL: http://www.hypergraphdb.org (дата обращения: 16.06.2020).
39. AllegroGraph. URL: https://allegrograph.com (дата обращения: 16.06.2020).
40. Neo4j Graph Platform – The Leader in Graph Databases. URL: https://neo4j.com (дата обращения: 16.06.2020).
41. Iosup A. et al. LDBC Graphalytics: A benchmark for large-scale graph analysis on parallel and distributed platforms // Proceedings of the VLDB Endowment. 2016. Vol. 9. no. 13. P. 1317–1328. DOI: https://doi.org/10.14778/3007263.3007270.
42. Hogan A. et al. Knowledge graphs // arXiv preprint arXiv:2003.02320. 2020. URL: https://arxiv.org/abs/2003.02320 (дата обращения: 17.06.2020).
43. Rosso P., Yang D., Cudré-Mauroux P. Beyond triplets: hyper-relational knowledge graph embedding for link prediction // Proceedings of The Web Conference 2020. P. 1885–1896. DOI: https://doi.org/10.1145/3366423.3380257.

REFERENCES:

[1] Sukhodolov A.P., Bychkova A.M. Artificial intelligence in crime counteraction, prediction, prevention and evolution. Russian Journal of Criminology, 2018. Vol. 12, no 5. P. 753–766. DOI: https://DOI:.org/10.17150/2500-4255.2018.12(6).753-766 (in Russian).

[2] Mazurov V. A., Starodubtseva M. A. Artificial intelligence as a means for forecasting and countering crime. Russian-Asian legal journal, 2019, no. 3. P. 46–50. URL: http://journal.asu.ru/ralj/article/view/6991 (accessed: 17.06.2020) (in Russian).

[3] Kravcov D.A. Artificial intelligence: crime prevention and prediction. Vestnik of Moscow University of the Minisrty of Internal Affairs of Russia, 2018, no. 3. P. 108–110. URL: https://cyberleninka.ru/article/n/iskusstvennyy-razum-preduprezhdenie-i-prognozirovanie-prestupnosti (accessed: 24.06.2020) (in Russian).

[4] Osipenko A.L. The prospects of use of information and analytical technologies in operational-search activity. Society and law, 2018, no. 4. P. 80–87. URL: https://cyberleninka.ru/article/n/perspektivy-ispolzovaniya-informatsionno-analiticheskih-tehnologiy-v-operativno-rozysknoy-deyatelnosti (accessed: 23.06.2020) (in Russian).

[5] Sebyakin A.G. Artificial intelligence in criminalistics: system of decision-making support. Baikal Research Journal, 2019. Vol. 10, no. 4. DOI: https://doi.org/10.17150/2411-6262. 2019.10(4).21. URL: http://cj.bgu.ru/reader/article.aspx?id=23649 (accessed: 23.06.2020) (in Russian).

[6] Stepanenko D.A., Bakhteev D.V., Evstratova Y.A. The use of artificial intelligence systems in law enforcement. Russian Journal of Criminology, 2020, vol. 14, no. 2, pp. 206-214. DOI: https://doi.org/10.17150/2500-4255.2020.14(2).206-214 (in Russian).

[7] Kuzmin I.A. Artificial neural networks: prospects for use in law enforcement. Forensics: yesterday, today, tomorrow, 2018, no. 4. URL: https://cyberleninka.ru/article/n/iskusstvennye-neyronnye-seti-perspektivy-ispolzovaniya-v-pravoohranitelnoy-deyatelnosti (accessed: 27.06.2020) (in Russian).

[8] Duga Sergey V. et al. The concept of decision support system in preliminary investigation. IT Security (Russia), [S.l.]. V. 26, n. 3. P. 45–57, sep. 2019. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1216 (accessed: 27.06.2020) DOI: http://dx.doi.org/10.26583/bit.2019.3.04 (in Russian).

[9] Singhal A. Introducing the knowledge graph: things, not strings. URL: https://www.blog.google/products/search/introducing-knowledge-graph-things-not (accessed: 16.05.2020).

[10] E. Marchi, O. Miguel. On the Structure of the Teaching-learning Interactive Process. International Journal of Game Theory, 1974. Vol. 3, no. 2. P. 83–99. DOI: https://doi.org/10.1007/BF01766394

[11] R.R. Bakker. Knowledge Graphs: Representation and Structuring of Scientific Knowledge. Ph.D. thesis, University of Twente, Enschede. 1987.

[12] P.H. de Vries. Representation of Science Texts in Knowledge Graphs. Ph.D. thesis, University of Groningen, Groningen, The Netherlands. 1989.

[13] Zhang L. Knowledge graph theory and structural parsing. Twente University Press, 2002. P. 216. URL: https://ris.utwente.nl/ws/portalfiles/portal/6073799/t0000020.pdf (accessed: 27.05.2020).

[14] Popping R. Knowledge graphs and network text analysis. Social Science Information, 2003. Vol. 42, no. 1. P. 91–106. DOI: https://doi.org/10.1177/0539018403042001798.

[15] Lisa Ehrlinger, Wolfram Wöß. Towards a Definition of Knowledge Graphs. Joint Proceedings of the Posters and Demos Track of 12th International Conference on Semantic Systems - SEMANTiCS2016 and 1st International Workshop on Semantic Change & Evolving Semantics (SuCCESS16), Leipzig, Germany, 2016. URL: http://ceur-ws.org/Vol-1695/paper4.pdf (accessed: 01.07.2020).

[16] Paulheim H. Knowledge graph refinement: A survey of approaches and evaluation methods. Semantic web, 2017. Vol. 8, no. 3. P. 489–508. DOI: https://doi.org/10.3233/SW-160218.

[17] Chenyan Xiong. Text representation, retrieval, and understanding with knowledge graphs. ACM SIGIR Forum, 2018. Vol. 52, no. 2. P. 180–181. DOI: https://doi.org/10.1145/3308774.3308808.

[18] Bellomarini L. et al. Knowledge graphs and enterprise AI: the promise of an enabling technology. IEEE 35th International Conference on Data Engineering (ICDE), 2019. P. 26–37. DOI: https://doi.org/10.1109/ICDE.2019.00011.

[19] Knowledge Graph. URL: https://ru.wikipedia.org/wiki/Knowledge_Graph (accessed: 01.07.2020).

[20] Ji S. et al. A survey on knowledge graphs: Representation, acquisition and applications. arXiv preprint arXiv:2002.00388, 2020. URL: https://arxiv.org/abs/2002.00388 (accessed: 20.06.2020).

[21] Molontay R., Nagy M. Twenty Years of Network Science: A Bibliographic and Co-authorship Network Analysis. arXiv preprint arXiv:2001.09006, 2020. URL: https://arxiv.org/abs/2001.09006 (accessed: 25.06.2020).

[22] Albert-László Barabási, Márton Pósfai. Network Science. Cambridge University Press, 2016. – 475 p.
[23] Saleh M., Esa Y., Mohamed A. Applications of complex network analysis in electric power systems. Energies, 2018. Vol. 11, no. 6. DOI: https://doi.org/10.3390/en11061381.
[24] Wu X. et al. Analysis of metro network performance from a complex network perspective. Physica A: Statistical Mechanics and its Applications, 2018. Vol. 492. P. 553–563. DOI: https://doi.org/10.1016/j.physa.2017.08.074.
[25] Wachs-Lopes G. A., Rodrigues P. S. Analyzing natural human language from the point of view of dynamic of a complex network. Expert Systems with Applications, 2016. Vol. 45. P. 8–22. DOI: https://doi.org/10.1016/j.eswa.2015.09.020.
[26] Jiang Z. Y. et al. Vehicle demand evolution analysis from the complex network perspective. Physica A: Statistical Mechanics and its Applications, 2019. Vol. 532. DOI: https://doi.org/10.1016/j.physa.2019.121889.
[27] Noy N. et al. Industry-scale knowledge graphs: Lessons and challenges. Queue, 2019. Vol. 17, no. 2. P. 48–75. DOI: https://doi.org/10.1145/3331166.
[28] Graphs in Government – Fulfilling Your Mission with Neo4j. URL: https://www.paperpicks.com/graphs-in-government-fulfilling-your-mission-with-neo4j (accessed: 06.06.2020).
[29] How NASA Finds Critical Data through a Knowledge Graph. URL: https://neo4j.com/blog/nasa-critical-data-knowledge-graph/?ref=blog (accessed: 09.06.2020).
[30] Ashurova Z, Tikhomirov A, Trufanov A, Kinash N, Berestneva O, Rossodivita. A 2017 Network platform of program governance for E-health service. 2017 12th Int. Sci. and Tech. Conf. on Computer Sciences and Information Technologies (CSIT), Lviv Ukraine, 2017. DOI: https://doi.org/10.1109/STC-CSIT.2017.8099429.
[31] Tushkanova O.N., Samojlov V. V. Knowledge net: a model and system for accumulating, presenting, and using knowledge and data. Ontology of Designing, 2019. Vol. 9, no 1. P. 117–131. DOI: https://doi.org/10.18287/2223-9537-2019-9-1-117-131(in Russian).
[32] Podruzhkina T.A., Fedorov D.Yu. Scheduling algorithms based on process semantic knowledge networks. Vestnik Sankt-Peterburgskogo universiteta GPS MCHS Rossii, no 1. P. 107–116, 2017. URL: https://cyberleninka.ru/article/n/ispolzovanie-informatsionnyh-tehnologiy-dlya-obespe-cheniya-bezopasnosti-lichnosti-obschestva-i-gosudarstva (accessed: 23.06.2020) (in Russian).
[33] Savchenko A.P. Open network of formal corporative knowledge: a conceptual model. Scientific Journal of KubSAU, 2014, no. 103. URL: https://cyberleninka.ru/article/n/otkrytaya-set-dokumentirovannyh-znaniy-organizatsii-kontseptualnaya-model (accessed: 22.06.2020) (in Russian).
[34] Announcing the Neo4j Crime Investigation Sandbox. URL: https://medium.com/neo4j/announcing-the-neo4j-crime-investigation-sandbox-c0c3bd9e71b1 (accessed: 30.06.2020).
[35] Neo4j and the Offshore Leaks: the Case of Azerbaijan. URL: https://neo4j.com/graphgist/neo4j-and-the-offshore-leaks-the-case-of-azerbaijan (accessed: 02.07.2020).
[36] ICIJ Offshore Leaks Database. URL: https://offshoreleaks.icij.org (accessed: 02.07.2020).
[37] Richard Cyganiak, David Wood, Markus Lanthaler. RDF 1.1 Concepts and Abstract Syntax, W3C Recommendation 25 February 2014. URL: https://www.w3.org/TR/2014/REC-rdf11-concepts-20140225 (accessed: 03.07.2020).
[38] HypergraphDB - A Graph Database. URL: http://www.hypergraphdb.org (accessed: 16.06.2020).
[39] AllegroGraph. URL: https://allegrograph.com (accessed: 16.06.2020).
[40] Neo4j Graph Platform – The Leader in Graph Databases. URL: https://neo4j.com (accessed: 16.06.2020).
[41] Iosup A. et al. LDBC Graphalytics: A benchmark for large-scale graph analysis on parallel and distributed platforms. Proceedings of the VLDB Endowment, 2016. Vol. 9, no. 13. P. 1317–1328. DOI: https://doi.org/10.14778/3007263.3007270.
[42] Hogan A. et al. Knowledge graphs. arXiv preprint arXiv:2003.02320, 2020. URL: https://arxiv.org/abs/2003.02320 (accessed: 17.06.2020).
[43] Rosso P., Yang D., Cudré-Mauroux P. Beyond triplets: hyper-relational knowledge graph embedding for link prediction. Proceedings of The Web Conference, 2020. P. 1885–1896. DOI: https://doi.org/10.1145/3366423.3380257.

Поступила в редакцию – 13 июля 2020 г. Окончательный вариант – 20 августа 2020 г.
Received – July 13, 2020. The final version – August 20, 2020.

Роман И. Гвоздев[1], Иван И. Швецов-Шиловский[2], Сергей Б. Шмаков[3].
[1,2,3]Акционерное общество «Экспериментальное научно-производственное объединение СПЕЦИАЛИЗИРОВАННЫЕ ЭЛЕКТРОННЫЕ СИСТЕМЫ», Каширское ш., 31, Москва, 115409, Россия
[1]e-mail: rigvoz@spels.ru, http://orcid.org/0000-0002-9284-5785
[2]e-mail: iish@spels.ru, http://orcid.org/0000-0002-8161-9926
[3]e-mail: sbshmak@spels.ru, http://orcid.org/0000-0002-4692-9355

АДАПТИРОВАННАЯ МЕТОДИКА КОНТРОЛЯ ФУНКЦИОНАЛЬНЫХ СБОЕВ В NOR FLASH-ПАМЯТИ ПРИ ИСПЫТАНИЯХ НА СТОЙКОСТЬ К ВОЗДЕЙСТВИЮ ТЯЖЁЛЫХ ЗАРЯЖЕННЫХ ЧАСТИЦ

DOI: http://dx.doi.org/10.26583/bit.2020.3.06

Аннотация. В данной статье предложена адаптированная методика контроля функциональных сбоев в NOR flash-памяти при испытаниях на стойкость к воздействию тяжёлых заряженных частиц. Эксперимент проводился на базе циклотрона У-400. Экспериментальные результаты апробации адаптированной методики показали необходимость разделения функциональных сбоев (ФС) на 5 типов в зависимости от характера каждого ФС и подтверждают необходимость адаптации методики и средств контроля для оценки параметров чувствительности к воздействию тяжёлых заряженных частиц (ТЗЧ) по одиночным радиационным эффектам (ОРЭ) ФС. Полученные результаты предоставляют дополнительные данные о параметрах чувствительности микросхем к воздействию ТЗЧ по ОРЭ производителю аппаратуры для разработки системы парирования наблюдаемых эффектов в аппаратуре, чтобы увеличить безопасность хранящейся информации.

Ключевые слова: функциональный сбой, тяжёлые заряженные частицы, стойкость, микросхема, аппаратно-программный комплекс.
Для цитирования: ГВОЗДЕВ, Роман И.; ШВЕЦОВ-ШИЛОВСКИЙ, Иван И.; ШМАКОВ, Сергей Б. Шмаков. АДАПТИРОВАННАЯ МЕТОДИКА КОНТРОЛЯ ФУНКЦИОНАЛЬНЫХ СБОЕВ В NOR FLASH-ПАМЯТИ ПРИ ИСПЫТАНИЯХ НА СТОЙКОСТЬ К ВОЗДЕЙСТВИЮ ТЯЖЁЛЫХ ЗАРЯЖЕННЫХ ЧАСТИЦ. Безопасность информационных технологий, [S.l.], v. 27, n. 3, p. 66–75, 2020. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1293>. Дата доступа: 02 sep. 2020. DOI: http://dx.doi.org/10.26583/bit.2020.3.06.

Roman I. Gvozdev[1], Ivan I. Shvetsov-Shilovskiy[2], Sergey B. Shmakov[3]
[1,2,3]Joint Stock Company "Experimental Research and Production Association SPECIAL ELECTRONIC SYSTEM", Kashirskoe sh., 31, Moscow, 115409, Russia
[1]e-mail: rigvoz@spels.ru, http://orcid.org/0000-0002-9284-5785
[2]e-mail: iish@spels.ru, http://orcid.org/0000-0002-8161-9926
[3]e-mail: sbshmak@spels.ru, http://orcid.org/0000-0002-4692-9355

Adapted method for monitoring functional failures in NOR FLASH-memory during tests for resistance to heavy charged particles

DOI: http://dx.doi.org/10.26583/bit.2020.3.06

Abstract. This study offers an adapted method for monitoring functional failures in NOR flash memory during tests for resistance to heavy charged particles. The experiment was conducted on the basis of the "U-400" cyclotron. Experimental results of approbation of the adapted method have shown the need to divide functional failures (FF) into 5 types depending on the nature of each FF and confirm the need to adapt the methodology and monitoring tools to assess the parameters of sensitivity to the effects of heavy charged particles (HCP) on single radiation effects (SRE) of the FF. The obtained results provide additional data on the parameters of the sensitivity of chips to the effects of HCP on the SRE to the

equipment manufacturer for the development of a system for parrying the observed effects in the equipment in order to increase the security of stored information.
Keywords: functional failures, heavy charged particles, resistance, chip, a hardware-software complex.
For citation: GVOZDEV, Roman I.; SHVETSOV-SHILOVSKIY, Ivan I.; SHMAKOV, Sergey B. Adapted method for monitoring functional failures in NOR FLASH-memory during tests for resistance to heavy charged particles. IT Security (Russia), [S.l.], v. 27, n. 3, p. 66–75, 2020. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1293>. Date accessed: 02 sep. 2020. DOI: http://dx.doi.org/10.26583/bit.2020.3.06.

Введение

Особое значение среди факторов, влияющих на космические аппараты, имеет воздействие полей ионизирующих излучений (ИИ) космического пространства – электронов, протонов, ионов [1]. ИИ создаётся ядерными частицами, к основным из них относятся: ионы, нейтроны, протоны, гамма-кванты электроны и фотоны. Ядерные частицы можно разделить на незаряженные (нейтроны, гамма-кванты, фотоны) и заряженные (протоны, ионы, электроны). К ТЗЧ относятся протоны и ионы [2].

Одиночные ядерные частицы (ОЯЧ) вызывают эффекты в интегральных схемах из-за локального энерговыделения в микрообъёме элемента интегральной схемы [2]. Возникающие эффекты приводят к нарушению работоспособности и изменению значений параметров электронной компонентной базы, комплектующих космической аппаратуры, для которых проблема ОРЭ стоит наиболее остро [3–4]. Выделившаяся энергия преобразуется в неравновесный заряд, который собирает чувствительная область. Заряд из чувствительной области преобразуется в «помехи» (токи, напряжения), из-за которых развивается ОРЭ [2, 5, 6].

В настоящее время наиболее критичным радиационным эффектом в интегральных схемах электронной аппаратуры космического назначения из-за воздействия отдельных ТЗЧ стали ОРЭ. [7–8]

Нарушение сохранности информации в ячейках памяти и/или нарушение работы управляющих узлов регистрируется как ФС, который может привести к потере информации, хранящейся в ячейках памяти, что в последствии может привести к сбоям систем управления космического назначения [2, 9, 10] и разработчику аппаратуры критически необходимо знать характер каждого из ФС для разработки системы парирования наблюдаемых эффектов в аппаратуре для увеличения безопасности хранящейся информации.

Микросхемы flash-памяти используются в системах космического назначения для хранения кодов программ и данных в аппаратуре. Преимуществами flash-памяти является энергонезависимость, возможность перепрограммирования и большая ёмкость памяти.

В связи с постоянным развитием микросхем, добавляется более гибкое конфигурирование, добавляются расширенные настройки, а также совершенствуются существующие интерфейсы и появляются новые, необходимо адаптировать имеющуюся методику контроля ФС для определения параметров чувствительности микросхем к воздействию ОЯЧ по ОРЭ.

1. Контроль функциональных сбоев при исследованиях микросхем nor flash-памяти

Основной причиной нарушений сохранности информации в микросхемах flash-памяти является потеря заряда с элемента хранения транзистора ячейки. В результате потери заряда происходит сдвиг порогового напряжения транзистора ячейки, и управляющая схема воспринимает ячейку как стёртую [9].

ФС при воздействии ОЯЧ определяются по реакции микросхемы в процессе выполнения командных циклов. Командный цикл – это цикл, на протяжении которого выполняется команда, отправленная в микросхему. При контроле командных циклов используются управляющие регистры. С помощью опроса регистров во время выполнения командного цикла, можно отследить его время выполнения, что является параметром функционирования в технической документации [2, 9].

В процессе опроса регистров, возможно нарушение сохранности данных управляющих регистров (энергозависимых и энергонезависимых), что регистрируется как ФС, который приводит к нарушению установленных режимов работы микросхемы (нарушение установленного режима ввода/вывода данных, блокировка секторов памяти для операций стирания/записи). Также, во время функционирования микросхемы, ФС проявляется как спонтанный запуск командных циклов операций записи/считывания/стирания, сопровождающиеся резким увеличением/уменьшением тока потребления микросхемы, который восстанавливался до исходного значения самопроизвольно или после отправки команды программного сброса микросхемы.

Во время считывания проявлением одиночного сбоя (ОС) является ошибка в полученном коде. Для восстановления функционирования необходимо перезаписать ячейки памяти, в которых произошёл сбой, или повторно считать информационный код. При регистрации сбоя считывания все последующие циклы могут быть с ошибками, поэтому требуется провести программный сброс или выключение питания микросхемы [9].

Сбой, во время выполнения командного цикла стирания/записи предлагается определять с помощью управляющих регистров: бит отвечающий за выполнение операции стирания/записи не сбрасывается в состояние «Готов» по прошествии максимального времени выполнения командного цикла стирания/записи, указанного в технической документации. Также ток в цепи питания резко падает. Чтобы восстановить функционирование проводится программный сброс или выключение питания, или перезапуск операции стирания [9, 11, 12].

Запуск спонтанного стирания памяти проявляется как потеря информации и ток потребления возрастает до значения равному при выполнении операции стирания. Повторная запись информационного кода устранит сбой [9].

2. Методика и аппаратно-программные средства контроля функциональных сбоев

Испытания электронной компонентной базы (ЭКБ) на стойкость к ОРЭ при воздействии ИИ проводятся на ускорителях ионов, протонов и лазерных установках со сфокусированным излучением. ОРЭ в изделиях ЭКБ, вызываемые воздействием ИИ, считают адекватными по признаку идентичности ионизационных реакций – параметрических и/или ФС и отказов, определяемых по внешним выводам изделий. Во время проведения испытаний, при фиксированном значении линейных потерь энергии ионов регистрируются ОРЭ.

На рис. 1 представлена адаптированная методика проведения исследований стойкости flash-памяти к воздействию ОЯЧ по эффектам ФС [9, 11, 13].

Контроль тиристорного эффекта (ТЭ) при испытательном воздействии проводится в активном режиме, с контролем тока потребления и контролем работоспособности. Пороговый уровень ТЭ устанавливается в зависимости от среднего уровня тока потребления, с учетом изменений тока при изменении режимов работы. При регистрации катастрофического отказа (КО) в каком-либо из режимов облучение микросхемы прекращалось.

Рис. 1. Методика проведения исследований стойкости флэш-памяти к воздействию ОЯЧ по эффектам функциональных сбоев
(Fig. 1. Methods for conducting research on the resistance of flash memory to the effects of SNP on the effects of functional failures)

В методику добавлены дополнительные действия во время исследований, а именно: контроль командных циклов и управляющих регистров. Дополненная последовательность действий во время исследований позволит контролировать выполнения операций и режимов работы, в которых находится микросхема.

3. Аппаратно-программная реализация средств контроля функциональных сбоев

Для реализации контроля командных циклов и управляющих регистров адаптирован стандартный аппаратно-программный комплекс, разработанный на основе оборудования фирмы National Instruments, структурная схема которого представлена на рис. 2. Особенностью является обмен данными с использованием расширенного интерфейса SPI по четырём линиям ввода/вывода (Quad SPI protocol). Комплекс подходит для микросхем NOR flash-памяти с интерфейсом SPI, у которых предусмотрена возможность обмена данными по четырём линиям ввода/вывода.

На рис. 2 введены следующие обозначения: G1 – источник питания (PXI-4110); G2 – вспомогательный источник напряжения (PXI-6229); A1, A2 – измерители тока PXI-4171 и PXI-4071; V2 – вольтметр; K1 размыкается только при контроле тока потребления; K2 замыкается только при контроле выходного напряжения; R1=510 Ом; C1=0,1 мкФ; Q0:Q(N-1) – сигнальные линии ввода/вывода; N – количество линий ввода/вывода (всего можно использовать от 1 до 4 линий); S# – выбор устройства; C – тактовый сигнал.

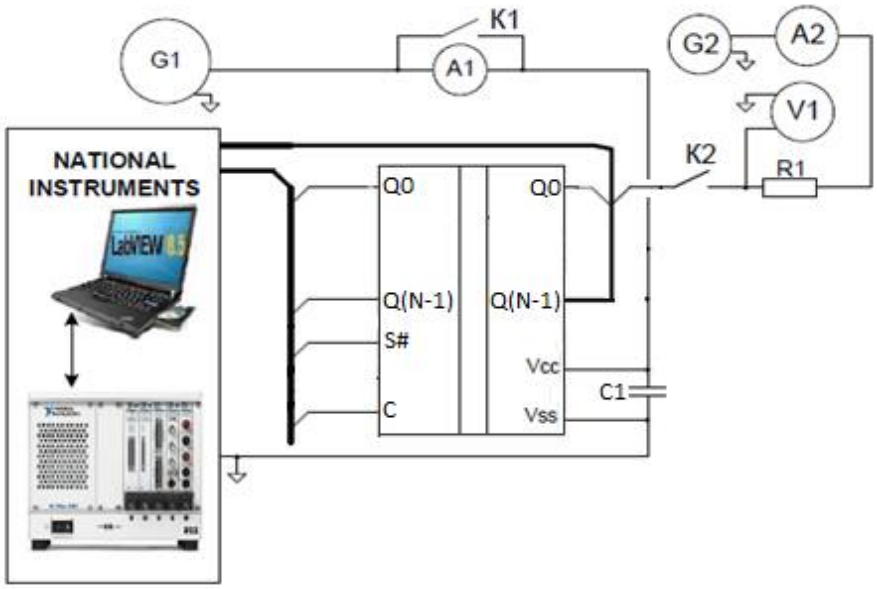


Рис. 2. Структурная схема аппаратно-программного комплекса
(Fig. 2. Block diagram of a hardware-software complex)

Контроль выходных напряжений осуществляется вольтметром V1 на выводе Q0. Режимный ток выхода устанавливается регулировкой напряжения вспомогательного источника G2 на резисторе R1 и контролируется измерителем тока A2.

Ключ K1 предназначен для переключения линии цепи питания, если требуется измерить потребляемый микросхемой ток. Ключ K2 предназначен для переключения линии ввода/вывода Q0 на вольтметр V1 при измерении выходных напряжений.

В аппаратно-программном комплексе используются следующие аппаратные средства:

- PXI-1033 – 5-слотовое шасси. Предназначено для управления модулями через персональный компьютер.
- Модуль PXI-4110 – 3-канальный программируемый источник питания постоянного тока. Имеет 3 канала питания с ограничением до 1 А на каждый канал. Используется для питания микросхемы, а также питания цифрового модуля PXI-6581.
- Модуль PXI-4071 – цифровой мультиметр. Используется для контролирования тока в цепи питания.
- Модуль PXI-7951R – используется вместе с адаптерным модулем PXI-6581.
- Модуль PXI-6581 – 54-канальный цифровой адаптер ввода/вывода. Совместно с PXI-7951R создают настраиваемый прибор цифрового ввода-вывода, который можно запрограммировать с помощью ПО LabVIEW FPGA для взаимодействия с микросхемой. Используется для взаимодействия с микросхемами в режиме реального времени с частотой до 100 МГц.
- Модуль PXI-6229 – многофункциональный модуль ввода/вывода, имеющий 32 аналоговых входа, 4 аналоговых выхода и 48 цифровых вводов-выводов. Используется как преобразователь напряжения для задания нагрузочного тока и контроля выходных напряжений.

Контроль выходных напряжений V_H и V_L осуществлялся с помощью PXI-6229 на выводе Q0 в режиме статической выборки логического 0 или логической 1 до и после облучения.

Контроль тока потребления во время облучения проводился с помощью измерителя тока, совмещённого с источником питания PXI-4110.

Контроль тока потребления (I_1, I_2) до и после облучения осуществлялся с измерителем тока потребления PXI-4071.

Взаимодействие с микросхемами обеспечивается с помощью персонального компьютера с разработанным программным обеспечением в среде LabVIEW.

На рис. 3 приведена блок-схема адаптированной управляющей программы, где представлены функции и подфункции, из которых состоят части «Host» и «Target». Программа является конечным автоматом вместе с дополнительными функциями, которые выполняются параллельно (выделено жирно).

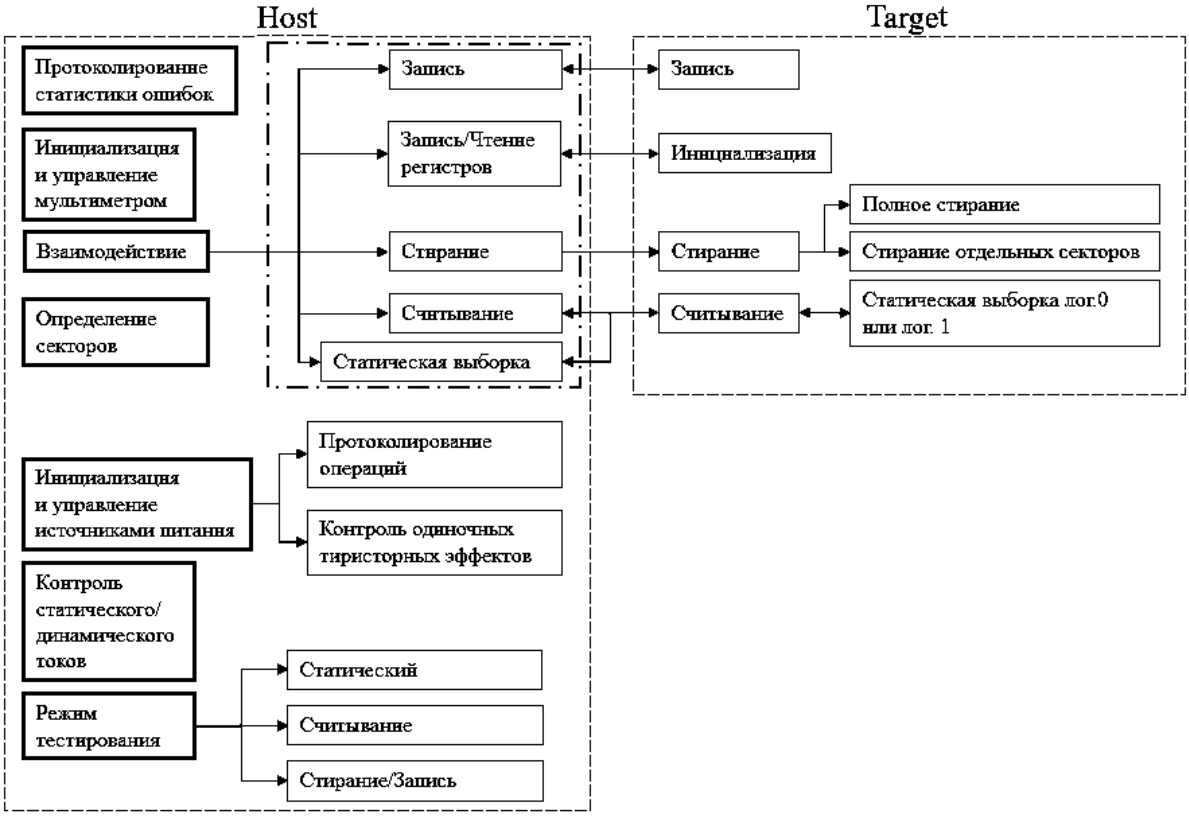


Рис. 3. Блок-схема управляющей программы
(Fig. 3. The block diagram of the control program)

Программа представляет собой многофункциональный интерфейс управления для взаимодействия с микросхемой, поддерживающий следующие основные операции:

- Запись всего объёма памяти эталонным кодом
- Считывание всего объёма памяти
- Стирание всего объёма памяти
- Сравнение считанных данных с эталонным кодом
- Контроль динамического и статического токов потребления
- Контроль выходных логических уровней
- Контроль одиночных тиристорных эффектов

Также реализованы дополнительные функции:

- Стирание отдельных секторов
- Считывание отдельных секторов
- Запись отдельных секторов эталонным кодом
- Запись/считывание управляющих регистров

Объектом исследований являются микросхемы flash-памяти NOR-типа информационной ёмкостью 256 Мбит с интерфейсом SPI. Микросхема изготовлена по технологии 65 нм. Диапазон напряжений питания от 2,7 В до 3,6 В.

В микросхеме реализована постраничная запись данных. Каждая страница может быть индивидуально запрограммирована. Биты программируются из единицы в ноль. Имеется возможность стереть подсектор, сектор или всю память. Всего в памяти 33 554 432 байта; 512 секторов (64 Кбайт каждый); 8192 подсектора (4 Кбайт каждый); 131 072 страницы (256 байт каждая) и 64 однократно программируемых байта, расположенных отдельно от остальной памяти.

Поддерживается 3-х байтный и 4-х байтный адресный режим.

Устройство имеет энергозависимые и энергонезависимые регистры, к которым пользователь может получить доступ, а именно:

- Регистр статуса – используется для контроля командного цикла записи и запрета записи/стирания.
- Энергозависимые и энергонезависимые регистры конфигурации – используются для включения/выключения протоколов интерфейса SPI.
- Адресный регистр – используется для переключения между верхним и нижним сегментом памяти при использовании 3-х байтного адреса.
- Регистр флагов – используется для контроля командного цикла стирания.

4. Порядок проведения и результаты эксперимента

Эксперимент проводился на базе циклотрона У-400 (ЛЯР ОИЯИ, г. Дубна Московской области). Последовательность режимов во время эксперимента при испытательном воздействии:

- Статический режим с периодическим контролем работоспособности.
- Режим считывания с контролем сохранности данных конфигурирующих регистров и командных циклов.
- Режим стирания/записи с контролем сохранности данных конфигурирующих регистров и командных циклов.

Контроль функционирования во время эксперимента заключался в проверке сохранности информации, а также возможности её перезаписи. Тестирование микросхемы проводилось в следующем порядке:

- Инициализация микросхемы эталонным кодом («инкрементный», «декрементный»).
- Считывание записанной информации, сравнение с эталонным значением.

Экспериментальные результаты показали, что необходимо разделить функциональные сбои на несколько типов, так как различалась реакция микросхемы при взаимодействии. Зарегистрированные функциональные сбои представлены в табл. 1.

Таблица 1. Тип и критерии зарегистрированных ФС во время эксперимента

Тип ФС	Реакция микросхемы на команды считывания или стирания	Предпринятые действия для восстановления функционирования
ФС1	Отсутствие реакции на команды	Перезапись энергозависимых управляющих регистров
ФС2	Нарушение сохранности информации в блоке памяти размеров 524 288 бит	Стирание блока памяти и повторная запись эталонным кодом
ФС3	Отсутствие реакции микросхемы на команду Bulk Erase (полное стирание накопителя)	Опрос регистра статуса. В случае активации запрета стирания/записи перезаписать регистр
ФС4	Увеличение тока потребления 150мА с самопроизвольным восстановлением	Запуск программного сброса
ФС5	Увеличение тока потребления до уровня 5-50мА с восстановлением после подачи команд или сброса питания	Запуск программного сброса

Заключение

Апробирована адаптированная методика контроля ФС для определения параметров чувствительности микросхем к воздействию ОЯЧ по ОРЭ.

В процессе подготовки к эксперименту адаптирован стандартный аппаратно-программный комплекс, разработанный на основе оборудования фирмы National Instruments.

Рассмотрены возникающие ФС по контролю командных циклов и управляющих регистров. Экспериментальные результаты апробации адаптированной методики показали необходимость разделения ФС на 5 типов в зависимости от реакции микросхемы на команды.

В процессе эксперимента обнаружен сбой регистра статуса (ФС3). Разряды отвечающие за запрет операции записи/стирания сбивались, что приводило к блокировке команды полного стирания накопителя (Bulk Erase), микросхема не реагировала на команду. Без контроля сохранности данных в регистре, такая реакция считалась бы катастрофическим отказом микросхемы, так как одна из операций стала недоступна.

Также обнаружен сбой конфигурирующего регистра (ФС1). Разряды, отвечающие за режимы работы интерфейса SPI, сбивались, что приводило к неправильной работе управляющей программы, так как в микросхеме изменился режим работы интерфейса. Контролирование управляющего регистра способствовало улучшению функционального контроля микросхемы при облучении.

СПИСОК ЛИТЕРАТУРЫ:

1. Чумаков А.И. «Действие космической радиации на интегральные схемы». М.: Радио и связь. 2004. – 320 с. URL: https://www.elibrary.ru/item.asp?id=19635287 (дата обращения: 29.07.2020).
2. Чумаков, А.И. Радиационная стойкость изделий ЭКБ [Текст] / А.И. Чумаков // Общая характеристика ионизирующих излучений: сб. статей. – М.: НИЯУ МИФИ, 2015. – 512 с.
3. Беляков В.В., Чумаков А.И., Никифоров А.Ю., Першенков В.С., Скоробогатов П.К., Согоян А.В. Расчётно-экспериментальные методы прогнозирования эффектов одиночных сбоев в элементах современной микроэлектроники // Микроэлектроника, 2003. Т. 32, № 2. С. 134–151. URL: https://www.elibrary.ru/item.asp?id=17262938 (дата обращения: 29.07.2020). DOI: https://doi.org/10.1023/A:1022656102956.

4. Sogoyan A.V., Chumakov A.I. and Smolin A.A., "Single Event Rate Prediction Method for Advanced CMOS Technologies," 2018 International Conference on Radiation Effects of Electronic Devices (ICREED), Beijing, China, 2018. P. 1–5. DOI: https://doi.org/10.1109/ICREED.2018.8905071.
5. A.B. Boruzdina, A.V. Yanenko, A.V. Ulanova, A.I. Chumakov, D.V. Bobrovskiy and V.M. Uzhegov, "Microdose effects in SRAM cells under heavy ion irradiation," 2017 17th European Conference on Radiation and Its Effects on Components and Systems (RADECS), Geneva, Switzerland, 2017. P. 1–3, DOI: https://doi.org/10.1109/RADECS.2017.8696109.
6. A.A. Pechenkin, A.B. Boruzdina, A.V. Yanenko, D.E. Protasov, I.I. Shvetsov-Shilovskiy and A.A. Sangalov, "SEL and cell failures in MRAM under ion and focused laser irradiation," 2017 17th European Conference on Radiation and Its Effects on Components and Systems (RADECS), Geneva, Switzerland, 2017. P. 1–6. DOI: https://doi.org/10.1109/RADECS.2017.8696211.
7. Чумаков, Александр И. и др. Требования и нормы испытаний по радиационной стойкости интегральных схем к эффектам воздействия тяжёлых заряженных частиц. Безопасность информационных технологий, [S.l.], Т. 27, №. 1. С. 83–97, фев. 2020. URL: https://bit.mephi.ru/index.php/bit/article/view/1254 (дата обращения: 18.08.2020). DOI: http://dx.doi.org/10.26583/bit.2020.1.07.
8. Чумаков А.И. и др. Оценка показателей стойкости интегральных схем при воздействии тяжелых заряженных частиц с использованием различных моделей. Безопасность информационных технологий, [S.l.]. Т. 24, № 1. С. 73–84, 2017. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/58 (дата обращения: 18.08.2020). DOI: http://dx.doi.org/10.26583/bit.2017.1.09.
9. Петров, А.Г. Функциональные отказы в микросхемах флэш-памяти от воздействия ионизирующих излучений космического пространства [Текст]: автореф. дис. на соиск. учен. степ. канд. техн. наук (05.13.05) / Петров Андрей Григорьевич; НИЯУ МИФИ – Москва, 2014 – 22 с. URL: https://www.elibrary.ru/item.asp?id=30416686 (дата обращения: 29.07.2020).
10. R. Koga, S. H. Penzin, K. B. Crawford and W. R. Crain, "Single event functional interrupt (SEFI) sensitivity in microcircuits," RADECS 97. Fourth European Conference on Radiation and its Effects on Components and Systems (Cat. No.97TH8294), Cannes, France, 1997. P. 311–318. DOI: https://doi.org/10.1109/RADECS.1997.698915.
11. Петров А.Г., Яненко А.В., Васильев А.Л., Чумаков А.И. «Поведение тока потребления микросхем флэш-памяти при возникновении эффектов сбоев типа SEFI» // Радиационная стойкость электронных систем – «Стойкость-2013», вып. 16, Москва, 2013. С. 163–164. URL: http://www.spels.ru/index.php?option=com_content&view=article&id=179&Itemid=73 (дата обращения: 18.08.2020) (in Russian).
12. Петров А.Г. «Регистрация функциональных сбоев, приводящих к стиранию информации во флэш ЗУ при воздействии одиночных ядерных частиц». URL: https://www.elibrary.ru/item.asp?id=25658477 (дата обращения: 18.08.2020).
13. Петров А.Г., Уланова А.В., Чумаков А.И., Васильев А.Л. Исследования потери информации в микросхемах флэш-памяти в активном и пассивном режимах при ионизирующем воздействии // Радиационная стойкость электронных систем – «Стойкость-2014», вып.17, Москва, 2014. С. 175–176. URL: http://www.spels.ru/index.php?option=com_content&view=article&id=179&Itemid=73 (дата обращения: 18.08.2020).

REFERENCES:

[1] Chumakov A.I. Dejstvie kosmicheskoj radiacii na integral'nye shemy [Tekst]. Moskva.: Radio i svjaz', 2004. – 320 s. URL: https://www.elibrary.ru/item.asp?id=19635287 (in Russian).
[2] Chumakov A.I. Radiation resistance of electronic component base products. General characteristics of ionizing radiation: collection of articles., Moscow: National research nuclear University MEPhI, 2015. – 512 p. (in Russian).
[3] Beljakov V.V., Chumakov A.I., Nikiforov A.Ju., Pershenkov V.S., Skorobogatov P.K., Sogojan A.V. Raschjotno-jeksperimental'nye metody prognozirovanija jeffektov odinochnyh sboev v jelementah sovremennoj mikrojelektroniki. Mikrojelektronika, 2003. T. 32, № 2. S. 134–151. URL: https://www.elibrary.ru/item.asp?id=17262938 (дата обращения: 29.07.2020). DOI: https://doi.org/10.1023/A:1022656102956. (in Russian).
[4] Sogoyan A.V., Chumakov A.I. and Smolin A.A., "Single Event Rate Prediction Method for Advanced CMOS Technologies," 2018 International Conference on Radiation Effects of Electronic Devices (ICREED), Beijing, China, 2018. P. 1–5. DOI: https://doi.org/10.1109/ICREED.2018.8905071.
[5] A.B. Boruzdina, A.V. Yanenko, A.V. Ulanova, A.I. Chumakov, D.V. Bobrovskiy and V.M. Uzhegov, "Microdose effects in SRAM cells under heavy ion irradiation," 2017 17th European Conference on Radiation

and Its Effects on Components and Systems (RADECS), Geneva, Switzerland, 2017. P. 1–3, DOI: https://doi.org/10.1109/RADECS.2017.8696109.

[6] A.A. Pechenkin, A.B. Boruzdina, A.V. Yanenko, D.E. Protasov, I.I. Shvetsov-Shilovskiy and A.A. Sangalov, "SEL and cell failures in MRAM under ion and focused laser irradiation," 2017 17th European Conference on Radiation and Its Effects on Components and Systems (RADECS), Geneva, Switzerland, 2017. P. 1–6. DOI: https://doi.org/10.1109/RADECS.2017.8696211.

[7] Chumakov Aleksandr I. et al. Hardness assurance levels and requirements for single event effects testing of integrated circuits. IT Security (Russia), [S.l.]. V. 27, no. 1. P. 83–97, feb. 2020. URL: https://bit.mephi.ru/index.php/bit/article/view/1254 (accessed: 18.08.2020). DOI: http://dx.doi.org/10.26583/bit.2020.1.07 (in Russian)

[8] Chumakov Aleksandr I. et al. Single Event Effects Rate Calculation with Different Models. IT Security (Russia), [S.l.]. V. 24, no 1. P. 73–84, 2017. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/58 (accessed: 18.08.2020). DOI: http://dx.doi.org/10.26583/bit.2017.1.09 (in Russian).

[9] Petrov A.G. Funkcional'nye otkazy v mikroshemah fljesh-pamjati ot vozdejstvija ionizirujushhih izluchenij kosmicheskogo prostranstva [Tekst]: avtoref. dis. na soisk. uchen. step. kand. tehn. nauk (05.13.05). Petrov Andrej Grigor'evich; NIJaU MIFI – Moskva, 2014 – 22 s. URL: https://www.elibrary.ru/item.asp?id=30416686 (accessed: 29.07.2020) (in Russian).

[10] R. Koga, S.H. Penzin, K.B. Crawford and W. R. Crain, "Single event functional interrupt (SEFI) sensitivity in microcircuits," RADECS 97. Fourth European Conference on Radiation and its Effects on Components and Systems (Cat. No.97TH8294), Cannes, France, 1997. P. 311–318. DOI: https://doi.org/10.1109/RADECS.1997.698915.

[11] Petrov A.G., Yanenko A.V., Vasil'ev A.L., Chumakov A.I. Povedenie toka potrebleniya mikroskhem flesh-pamyati pri vozniknovenii effektov sboev tipa SEFI. Radiacionnaya stojkost' elektronnyh sistem – «Stojkost'-2013», vyp. 16, Moskva, 2013. S. 163–164 URL: http://www.spels.ru/index.php?option=com_content&view=article&id=179&Itemid=73 (accessed: 18.08.2020) (in Russian).

[12] Petrov A.G. «Registracija funkcional'nyh sboev, privodjashhih k stiraniju informacii vo fljesh ZU pri vozdejstvii odinochnyh jadernyh chastic». URL: https://www.elibrary.ru/item.asp?id=25658477 (accessed: 18.08.2020) (in Russian).

[13] Petrov A.G., Ulanova A.V., Chumakov A.I., Vasil'ev A.L. Issledovanija poteri informacii v mikroshemah fljesh-pamjati v aktivnom i passivnom rezhimah pri ionizirujushhem vozdejstvii // Radiacionnaja stojkost' jelektronnyh sistem – «Stojkost'-2014», vyp. 17, Moskva, 2014. S. 175–176. URL: http://www.spels.ru/index.php?option=com_content&view=article&id=179&Itemid=73 (accessed: 18.08.2020) (in Russian).

Поступила в редакцию – 26 июля 2020 г. Окончательный вариант – 20 августа 2020 г.
Received – July 26, 2020. The final version – August 20, 2020.

Роман С. Торшин[1], Георгий С. Сорокоумов[2], Дмитрий В. Бобровский[3],
Александр А. Демидов[4], Анастасия В. Уланова[5]
[1-5]Акционерное общество «Экспериментальное научно-производственное объединение СПЕЦИАЛИЗИРОВАННЫЕ ЭЛЕКТРОННЫЕ СИСТЕМЫ», Каширское ш., 31, Москва, 115409, Россия
[1]e-mail: rstor@spels.ru, https://orcid.org/0000-0001-8053-1343
[2]e-mail: gssor@spels.ru, https://orcid.org/0000-0002-8446-6144
[3]e-mail: dvbob@spels.ru, https://orcid.org/0000-0003-3036-2953
[4]e-mail: aadem@spels.ru, https://orcid.org/0000-0001-7123-7644
[5]e-mail: avulan@spels.ru, https://orcid.org/0000-0001-7376-6339

ИЗМЕРЕНИЕ КРИТЕРИАЛЬНЫХ ПАРАМЕТРОВ АНАЛОГО-ЦИФРОВЫХ ПРЕОБРАЗОВАТЕЛЕЙ И КОНТРОЛЬ ИХ ИЗМЕНЕНИЯ ВО ВРЕМЯ РАДИАЦИОННОГО ЭКСПЕРИМЕНТА

DOI: http://dx.doi.org/10.26583/bit.2020.3.07

Аннотация. В данной работе апробируется метод тестирования микросхем аналого-цифровых преобразователей (АЦП), предназначенный для измерения основных параметров преобразователей методом гистограмм (или плотности кода). Данный метод хорошо подходит для современных высокочастотных АЦП с широкой полосой, совместим со стандартным программным обеспечением персональных компьютеров (ПК) и оценочных плат производителей АЦП, дает возможность на том же оборудовании определять и динамические характеристики АЦП, используя методы цифровой обработки сигнала (ЦОС). В качестве контрольно-измерительного оборудования, необходимого для проведения теста, использовались модульные измерительные приборы фирмы National Instruments, а также генератор сигналов SMA100B фирмы ROHDE&SCHWARZ. С помощью данного метода вычислены основные статические и динамические параметры АЦП AD7888. Приведена деградация критериальных параметров АЦП AD7888 при воздействии поглощенной дозы на рентгеновском источнике «РИК-0401».

Ключевые слова: аналого-цифровой преобразователь, метод гистограмм, статические параметры АЦП, динамические параметры АЦП, тестирование микросхем, поглощенная доза.
Для цитирования.: *ТОРШИН, Роман С. et al. ИЗМЕРЕНИЕ КРИТЕРИАЛЬНЫХ ПАРАМЕТРОВ АНАЛОГО-ЦИФРОВЫХ ПРЕОБРАЗОВАТЕЛЕЙ И КОНТРОЛЬ ИХ ИЗМЕНЕНИЯ ВО ВРЕМЯ РАДИАЦИОННОГО ЭКСПЕРИМЕНТА.Безопасность информационных технологий, [S.l.], v. 27, n. 3, p. 76–88, 2020. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1294>. Дата доступа: 08 sep. 2020. DOI: http://dx.doi.org/10.26583/bit.2020.3.07.*

Roman S. Torshin[1], Georgy S. Sorokoumov[2], Dmitry V. Bobrovsky[3],
Alexander A. Demidov[4], Anastasya V. Ulanova[5]
[1–5]Joint Stock Company "Experimental Research and Production Association SPECIAL ELECTRONIC SYSTEM" Kashirskoe sh., 31, Moscow, 115409, Russia
[1]e-mail: rstor@spels.ru, https://orcid.org/0000-0001-8053-1343
[2]e-mail: gssor@spels.ru, https://orcid.org/0000-0002-8446-6144
[3]e-mail: dvbob@spels.ru, https://orcid.org/0000-0003-3036-2953
[4]e-mail: aadem@spels.ru, https://orcid.org/0000-0001-7123-7644
[5]e-mail: avulan@spels.ru, https://orcid.org/0000-0001-7376-6339

Measurement of criteria parameters of analog-to-digital converters and monitoring of their changes during the radiation experiment

DOI: http://dx.doi.org/10.26583/bit.2020.3.07

Abstract. The paper presents a method for testing ADC, intended for measurement the basic parameters of converters by histogram test (or code density test). This method is ideally suited for modern wide bandwidth high precision ADCs and is universally accepted, especially with the proliferation of standard PC-based software and ADC manufacturer's evaluation boards. The histogram and Fast Fourier transform (FFT) tests use essentially the same hardware, both are normally part of a comprehensive ADC test plan [1]. Modular Instrumentation System PXI of NI and Signal Generator SMA100B (ROHDE & SCHWARZ) were used as test equipment for the tests. The basic static and dynamic parameters of the ADC AD7888 were calculated using this method. The degradation of the main parameters of the ADC AD7888 under the influence of the absorbed dose at the «RIK-0401» x-ray unit is presented in the paper.

Keywords: analog to digital converter, histogram test, dynamic parameters ADC, static parameters ADC, testing microchips, absorbed dose.

For citation: TORSHIN, Roman S. et al. Measurement of criteria parameters of analog-to-digital converters and monitoring of their changes during the radiation experiment. IT Security (Russia), [S.l.], v. 27, n. 3, p. 76-88, 2020. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1294>. Date accessed: 08 sep. 2020. DOI: http://dx.doi.org/10.26583/bit.2020.3.07.

Введение

Современный мир оперирует огромными объемами информации, передача и обработка которых проводится с помощью автоматических и автоматизированных систем. Большинство первичных блоков систем, осуществляющих прием информации, оснащены трактами предварительной обработки аналогового сигнала и перевода его в цифровой вид. Одной из областей применения автоматических систем является аппаратура космического назначения, для которой критичным являются вопросы безотказной работы и сроки активного существования аппаратуры. Таким образом, вопросы безопасности информации неразрывно связаны с исследованием параметров стойкости микросхем АЦП при воздействии ионизирующего излучения космического пространства.

Существует множество методов для тестирования статических и динамических характеристик АЦП, но тесты на базе ЦОС стали практически универсальными промышленными стандартами для современных преобразователей. В статье предлагается гистограммный метод тестирования АЦП, который заключается в накоплении большого количества оцифрованных отсчетов входного сигнала с известной плотностью вероятности за определенный период времени.

1. Описание метода гистограмм для тестирования статических параметров АЦП

Характеристика преобразования (ХП) АЦП определяется при помощи статистического анализа отсчетов. Входным сигналом для гистограммного метода является линейно изменяющийся, или синусоидальный сигнал, слегка выходящий за пределы входного диапазона АЦП. В ходе теста подсчитывается количество выпадений каждого кода. Конфигурация гистограммного тестера представлена на рис. 1. Частота входного сигнала не должна быть субгармоникой частоты дискретизации АЦП, в противном случае кодовые комбинации в каждом периоде входного сигнала будут повторяться, что приведет к искажению измерения дифференциальной нелинейности (ДНЛ) и сделает их бессмысленными [1].

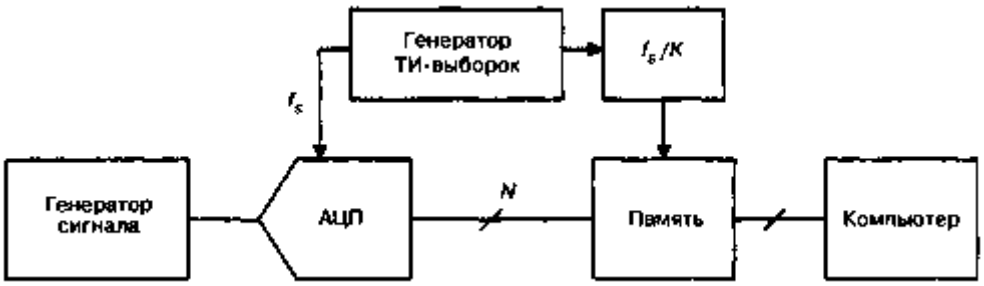


Рис. 1. Структурная схема гистограммного метода
(Fig. 1. Flow chart of the histogram test)

Измерение передаточной характеристики АЦП, по сути, направлено на определение уровней напряжения, соответствующих межкодовым переходам. На рис. 2а представлена статическая передаточная характеристика, которая задана через кодовые переходы, которые могут быть измерены напрямую. Сложность определения уровня межкодового перехода заключается в том, что код АЦП даже при фиксированном значении входного напряжения, при приближении уровня входного сигнала к уровню межкодового перехода, может интенсивно переключаться, что особенно характерно для быстродействующих преобразователей (рис. 2б) [2, 3].

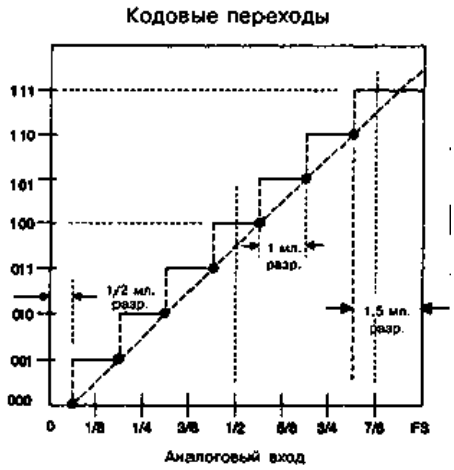


Рис. 2а. Статическая ХП АЦП
(Fig. 2a. ADC static transfer function)

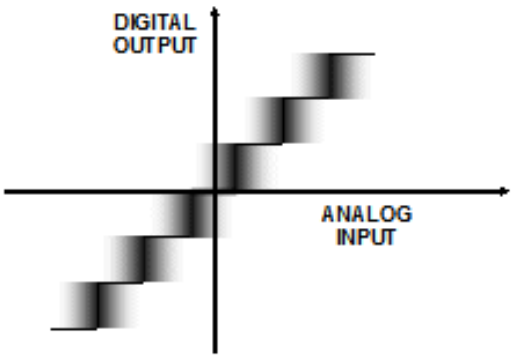


Рис. 2б. Кодовые переходы реальной ХП АЦП
(Fig. 2b. Code transitions of the real ADC transfer function)

Суть гистограммного метода тестирования АЦП заключается в том, что для кодов от 0 до 2^{N-1} собирается статистика их выпадения, подсчитывается весовой коэффициент, соответствующий частоте выпадения каждого кода (или реальный шаг квантования). В случае линейного изменения тестового сигнала идеальный шаг квантования можно вычислить следующим образом:

$$v_i = \frac{V_{ref}}{2^N}. \quad (1)$$

Реальный шаг квантования определяется согласно формуле:

$$v_j = \frac{m_j * \Delta V}{M}, \quad (2)$$

где ΔV – диапазон изменения входного аналогового сигнала, m_j – количество событий j–го кода, $M = \sum_{j=0}^{2^N-1} m_j$ – полное количество событий всех кодов.

Необходимо учитывать число отсчетов переполнения, соответствующих попаданиям в интервалы кодов из одних нулей (код 0) и одних единиц (код 2^{N-1}). Сигнал необходимо отрегулировать таким образом, чтобы АЦП не был сильно перегружен (рекомендуется работа с 10 %-ой перегрузкой) [4, 5].

Типичный вид гистограммы представлен на рис. 3, на котором легко определить широкие, узкие и пропущенные коды.

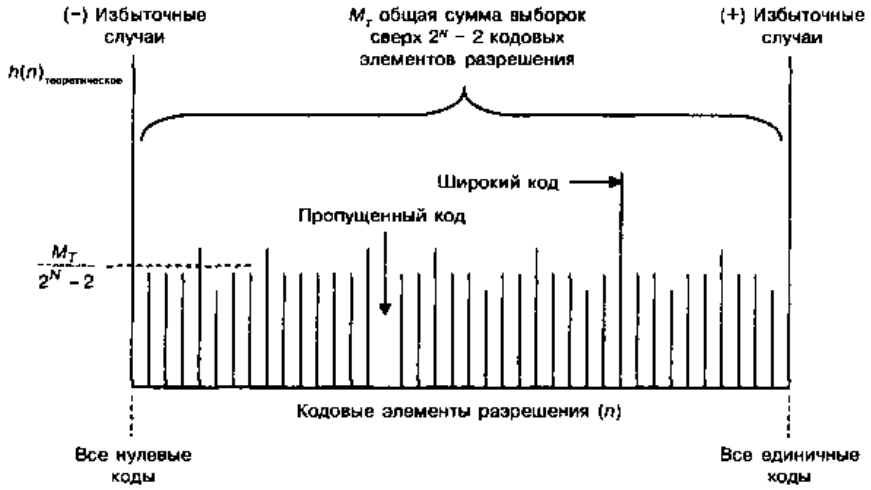


Рис. 3. Типичный вид гистограммы для линейно возрастающего входного сигнала (Fig. 3. Typical histogram for a linear input ramp signal)

Дифференциальная нелинейность (ДНЛ) определяется выражением:

$$DNL_j = \frac{(v_j - v_i)}{v_i} \quad (3)$$

После построения аппроксимирующей прямой вида «*ax*+*b*» определяется интегральная нелинейность (ИНЛ):

$$INL_j = \frac{\frac{n_j - b}{a} - (V_0 + \Delta V * \frac{\frac{m_j}{2} + \sum_{k=0}^{k-1} m_k}{M})}{v_i}, \quad (4)$$

где n_j – текущее значение кода.

Погрешность смещения нуля (аддитивная погрешность) может быть определена как смещение всей ХП АЦП влево или вправо относительно идеальной ХП и определяется согласно формуле:

$$E_0 = \frac{(^{v_i}/_2 - (V_0 + \frac{m_0 * \Delta V}{M}))}{v_i}, \quad (5)$$

где V_0–начальное значение входного тестового напряжения, m_0 – количество событий кода 00..00.

Погрешность усиления (мультипликативная погрешность) представляет собой разность между реальной и идеальной передаточными характеристиками в точке максимального выходного значения при условии нулевой аддитивной погрешности (при отсутствии смещения) и определяется согласно формуле:

$$E_g = \frac{(V_{ref} - \frac{3v_i}{2}) - (V_1 - \frac{m_g * \Delta V}{M})}{v_i} - E_0, \quad (6)$$

где V_1–конечное значение входного тестового напряжения, m_g – количество событий кода 11..11, V_{ref} – опорное напряжение АЦП.

Для синусоидального входного сигнала вероятность выпадения кодов не одинакова. Для *N*-разрядного АЦП с входным диапазоном полной шкалы $\pm V_{FS}$ и амплитудой A, вероятность появления кода n определяется выражением [6, 7, 8]:

$$p(n) = \frac{1}{\pi} * \left(\arcsin\left(\frac{V_{FS}*(n-2^{N-1})}{A*2^N}\right) - \arcsin\left(\frac{V_{FS}*(n-1-2^{N-1})}{A*2^N}\right)\right). \quad (7)$$

График этой функции вместе с реальным распределением выходных кодов для микросхемы AD7888 представлен на рис.4. Стоит обратить внимание, что вероятность выпадения кода возрастает в пиках синусоиды, так как *dv/dt* в этих точках мало (больше попаданий в интервал), чем в районе пересечения нуля, где *dv/dt* максимально (меньше попаданий в интервал).

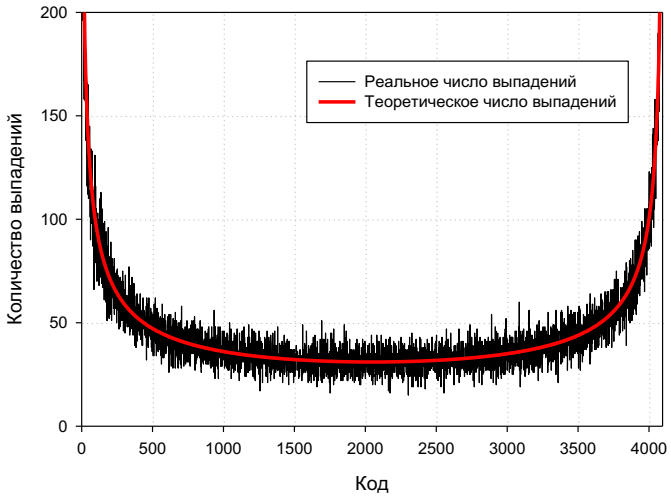


Рис. 4. Сопоставление реального распределения выходных кодов микросхемы AD7888 с теоретическим
(Fig. 4. Actual and theoretical code distribution for ADC AD7888)

Для вычисления точностных параметров АЦП из данной статистики необходимо рассчитать теоретическое число выпадений каждого кода согласно формуле:

$$h(n)_{\text{теор.}} = p(n) * M. \quad (8)$$

Соответствующая погрешность ДНЛ и ИНЛ определяются выражениями:

$$DNL(n) = \frac{h(n)_{\text{реал.}}}{p(n)*M} - 1, \quad (9)$$

$$INL(n) = \sum_{i=1}^{n} DNL(n). \quad (10)$$

Стоит отметить, что для корректного вычисления погрешности ИНЛ после вычисления кумулятивной суммы из ДНЛ необходимо построить наиболее подходящую линию, таким образом, чтобы ИНЛ равнялась 0 в конечных точках, а затем разность двух полученных зависимостей даст ИНЛ [4].

При измерении ИНЛ и ДНЛ гистограммным методом в качестве входного сигнала чаще используется синусоидальный, а не линейно возрастающий сигнал, так как при соответствующей фильтрации можно формировать синусоидальные сигналы с крайне высокой линейностью и низким шумом. На рис. 5а и 5б представлены графики зависимостей ДНЛ и ИНЛ для линейно возрастающего и синусоидального входного сигнала соответственно.

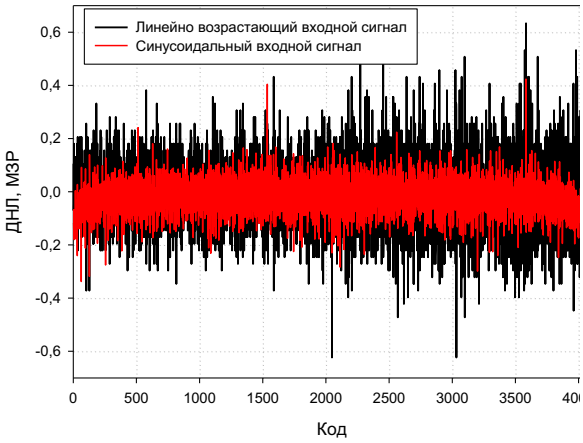


Рис. 5а. ДНЛ микросхемы AD7888 при синусоидальном и линейно возрастающем входном сигнале

(Fig. 5a. DNL for sinusoidal and linear ramp input signals for ADC AD7888)

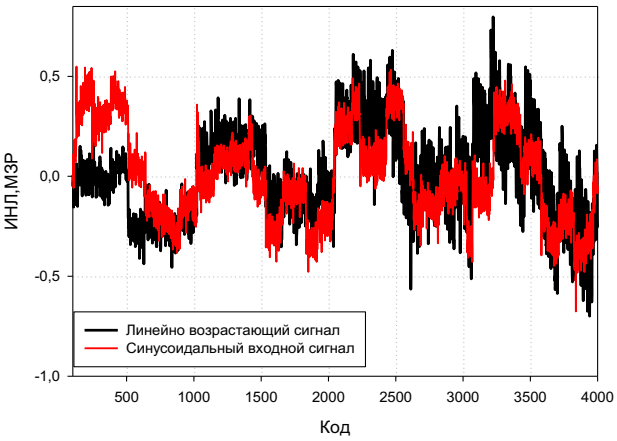


Рис. 5б. ИНЛ микросхемы AD7888 при синусоидальном и линейно возрастающем входном сигнале

(Fig. 5b. INL for sinusoidal and linear ramp input signals for ADC AD7888)

Из приведенных рис. 5а и 5б видно, что использование в качестве сигнала прецизионного синуса с фильтром низких частот дает лучшие значения ДНЛ и ИНЛ, что объясняется тем, что точность измерения ИНЛ и ДНЛ АЦП не может превышать точность ИНЛ входного сигнала с ЦАП, а также любой высокочастотный шум, присутствующий в линейно изменяющимся сигнале нельзя убрать фильтрацией (поскольку она тоже повлияет на линейность).

Гистограммный тест устраняет влияние приведенного к входу шума путем усреднения его по всем кодовым интервалам. Поэтому он хорошо подходит для современных высокочастотных АЦП с широкой полосой, совместим со стандартным программным обеспечением ПК и оценочных плат производителей АЦП. Из недостатков метода – невозможность определения монотонности статической ХП АЦП, то есть порядок появления кодов по отношению к входному сигналу с помощью этого теста определить нельзя.

2. Расчет динамических параметров АЦП на основе методов ЦОС

Для определения динамических характеристик АЦП также используются методы ЦОС. Дискретное преобразование Фурье (ДПФ) над оцифрованным сигналом позволяет преобразовать его из временной области, в его эквивалентное представление в частотной. Количество отсчетов M для ДПФ должно равняться степени двойки (необходимо для процедур вычисления быстрого преобразования Фурье (БПФ) – алгоритма, позволяющего уменьшить требуемое число математических вычислений). На рис. 6 представлен усредненный результат от взятия десяти БПФ от выходного сигнала АЦП AD7888 с приведенными значениями основных динамических параметров АЦП: SNR, SINAD, THD, SFDR. Усреднение результатов нескольких отдельных БПФ не приводит к изменению шумового порога, а только уменьшает разброс шумовых составляющих.

Отношение сигнал/шум (SNR) — это отношение среднеквадратического значения величины входного сигнала к среднеквадратическому значению величины шума (за исключением гармонических искажений), выраженное в децибелах.

Отношение сигнал/шум и коэффициент искажений (SINAD, или S/N+D) – это отношение среднеквадратичного значения амплитуды сигнала к среднему значению корня

из суммы квадратов всех других спектральных компонентов, включая гармоники, но исключая постоянную составляющую.

Динамический диапазон, свободный от гармоник (SFDR) определяется как отношение среднеквадратичного значения амплитуды сигнала к наиболее мощной паразитной гармоники в первой зоне Найквиста от 0 до $f_s/2$. Обычно SFDR выражается относительно амплитуды несущей (дБн).

Полные нелинейные искажения (THD) определяются как отношение среднеквадратичного значения основной частоты сигнала к среднему значению корня из суммы квадратов гармоник (обычно существенны только первые пять) [1].

Из рис. 6 видно, что минимальный уровень шума, полученного с помощью БПФ, приблизительно равен 110 дБ от полной шкалы АЦП, тогда как теоретическое отношение сигнал/шум 12-разрядного АЦП равно 74 дБ. Минимальный уровень шума от БПФ не равен отношению сигнал/шум АЦП, потому что БПФ действует, подобно аналоговому анализатору спектра с шириной полосы $\frac{f_S}{M}$ [1].

Теоретически минимальный уровень шума БПФ равен $10\log\left(\frac{M}{2}\right)$ дБ, то есть ниже минимального уровня шума квантования из-за выигрыша БПФ в отношении сигнал/шум [2, 4]. При испытаниях АЦП, использующих БПФ, важно быть уверенным, что количество точек БПФ достаточно велико для того, чтобы нелинейные искажения можно было отличить от минимального уровня шума БПФ.

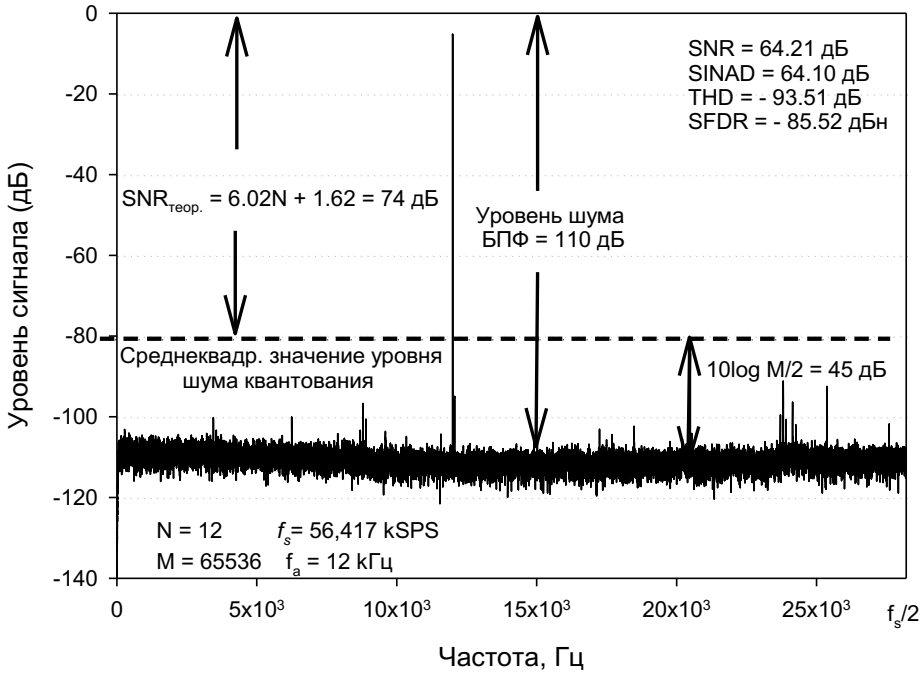


Рис. 6. БПФ массива 65536 точек для микросхемы АЦП AD7888
(Fig. 6. FFT array of 65536 points for ADC AD7888)

3. Используемое оборудование

Для измерения критериальных параметров микросхемы AD7888 использовался следующий набор модулей, объединенных в единую контрольно-измерительную систему при помощи NI PXI-1033 – PXI шасси со встроенным дистанционным контроллером:

NI PXI-4461 – звуковой и вибрационный модуль, располагающий двумя каналами для динамической генерации сигнала и двумя каналами для оцифровки. Использовался в качестве генератора линейно возрастающего сигнала (24-разрядный ЦАП).

NI PXI-7841R – многофункциональный модуль PXI, имеющий в своем составе ПЛИС Virtex-5 LX30, 96 цифровых линий, 8 аналоговых входов и 8 аналоговых выходов с 16-битным разрешением.

NI PXI-4110 – 3-х канальный программируемый источник питания.

NI PXI-4071 – высокопроизводительный цифровой мультиметр с разрешением 7½ разряда и напряжением 1000 В.

Для подачи синусоидального сигнала использовался SMA100B – генератор сигналов, предназначенный для формирования немодулированных колебаний высокой спектральной чистоты в диапазоне от 8 кГц до 3 ГГц.

ПО для связи всех используемых блоков и проведения автоматизированного радиационного эксперимента было написано в САПР LabVIEW.

4. Проведение автоматизированного радиационного эксперимента

Исследования на стойкость микросхемы AD7888 к воздействию накопленной дозы проводились с использованием рентгеновского источника «РИК-0401».

Алгоритм обмера критериальных параметров исследуемой микросхемы при работе на рентгеновском источнике был следующим: каждые 30 с проводился ФК микросхемы, и параметры АЦП (ИНЛ, ДНЛ, SNR, SINAD, V_{ref}, I_{cc}) записывались в файл-отчет, на анализе которого в последствии была установлена их деградация из-за воздействия дозового эффекта [9, 10].

Типичными эффектами от поглощенной дозы в АЦП является деградация ХП микросхемы и связанные с этим ухудшения точностных параметров: интегральной нелинейности, дифференциальной нелинейности, ошибки смещения и усиления [11, 12]. График изменения ХП АЦП при воздействии поглощенной дозы для разных значений поглощенной дозы приведен на рис. 7.

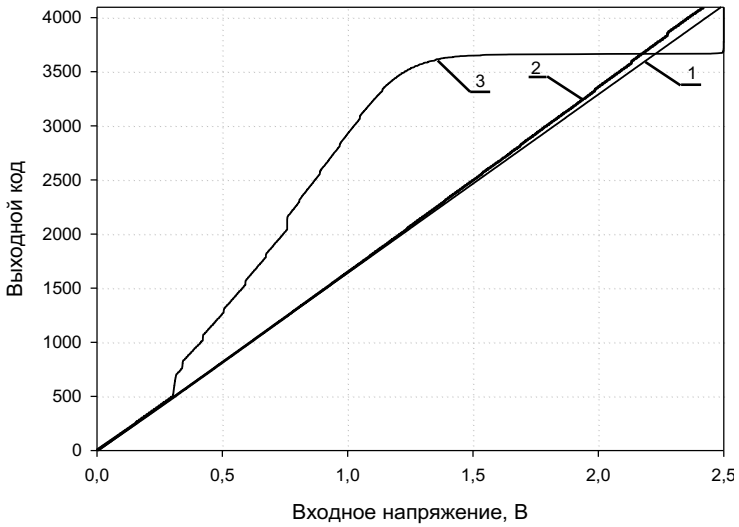


Рис. 7. ХП АЦП для различных уровней набранной дозы:
1 – исходная ХП; 2 – 9×10³ ед.;3 – 11×10³ ед.
(Fig. 7. ADC transfer function for different irradiation steps
1 – initial TF; 2 – 9×10³ un.;3 – 11×10³ un.)

Графики изменения электрических параметров (тока потребления и напряжения внутреннего источника опорного напряжения (ИОН)) приведены на рис. 8а и 8б соответственно. Образец №4 облучался в режиме работы с внешним ИОН.

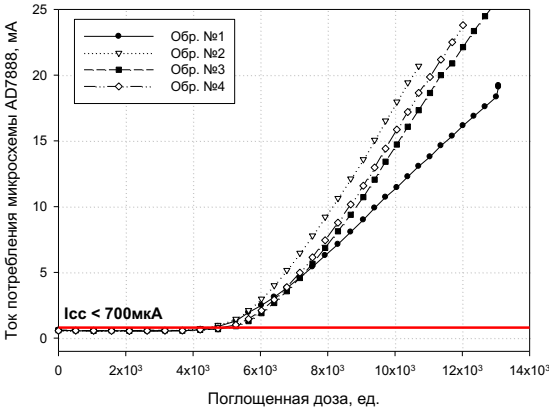


Рис. 8а. Изменение тока потребления микросхемы AD7888 при воздействии поглощенной дозы

(Fig. 8a. Power supply currents AD7888 during irradiation)

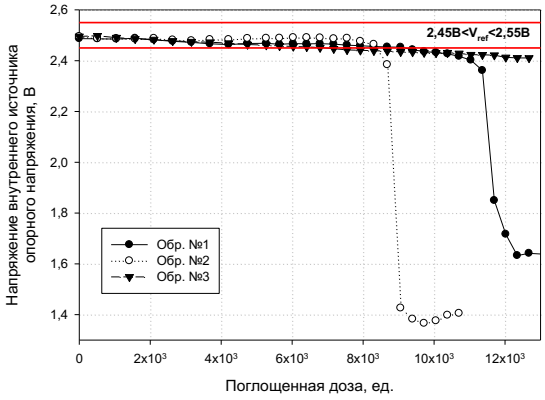


Рис. 8б. Изменение напряжения внутреннего ИОН микросхемы AD7888 при воздействии поглощенной дозы

(Fig. 8b. The input reference voltage AD7888 during irradiation)

График изменения ДНЛ на образце №1 в зависимости от поглощенной дозы, а также график изменения минимального и максимального ДНЛ приведены на рис. 9а и 9б соответственно. Видно, что АЦП начинает пропускать коды, начиная примерно с 8×10^3ед. Выход параметра за указанные в документации нормы обозначен красной линией на графике.

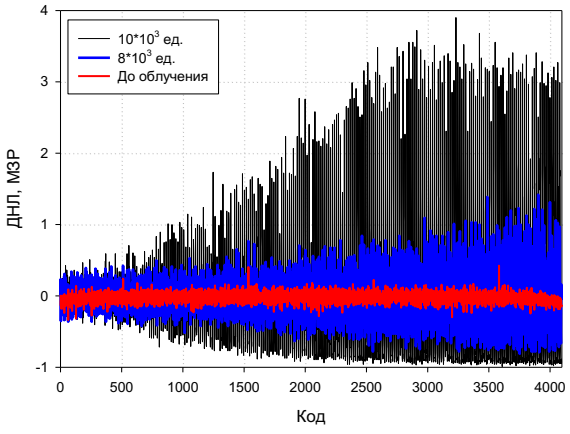


Рис. 9а. Изменение ДНЛ микросхемы AD7888 при воздействии поглощенной дозы

(Fig .9a. DNL AD7888 for different irradiation steps)

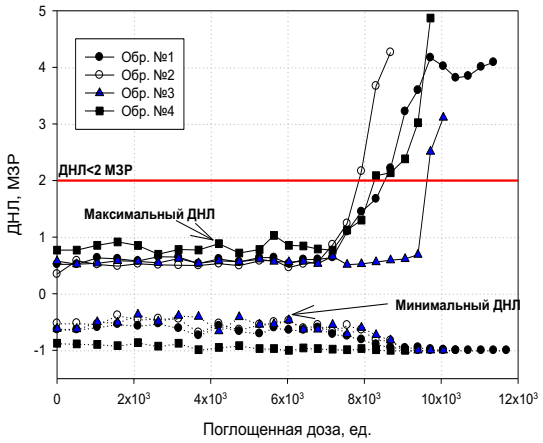


Рис. 9б. Изменение максимальной и минимальной ДНЛ микросхемы AD7888 при воздействии поглощенной дозы

(Fig. 9b. DNL AD7888 during irradiation)

ИНЛ является мерой отклонения фактической ХП от идеальной. Видно, что реальная ХП все дальше отклоняется от идеальной в обе стороны. Это можно увидеть на рис. 10а, 10б.

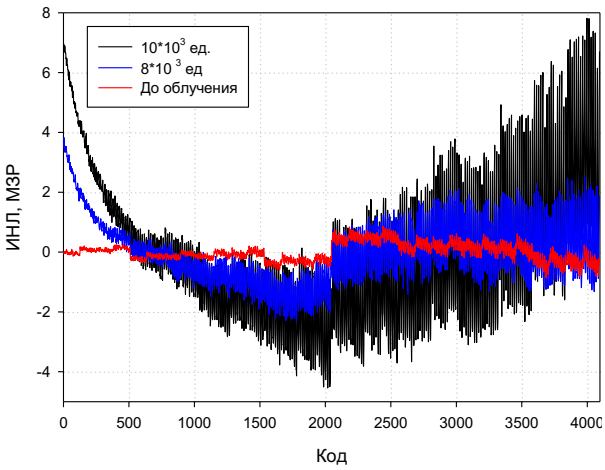


Рис. 10а. Изменение ИНЛ микросхемы AD7888 при воздействии поглощенной дозы

(Fig. 10a. INL AD7888 for different irradiation steps)

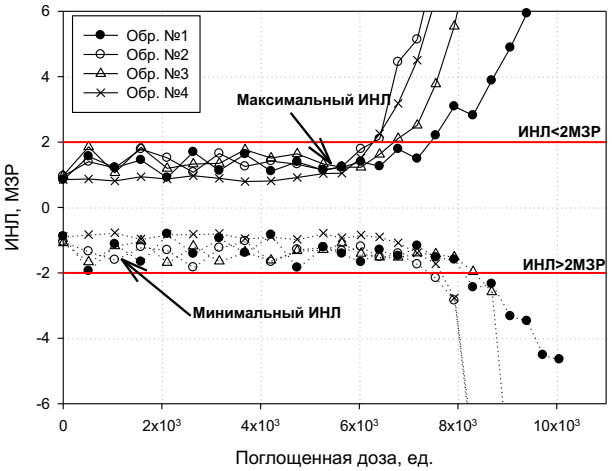


Рис. 10б. Изменение максимальной и минимальной ИНЛ микросхемы AD7888 при воздействии поглощенной дозы

(Fig. 10b. INL AD7888 during irradiation)

Можно отметить различное поведение графиков ИНЛ и ДНЛ при накоплении дозы. На графике ИНЛ наблюдается рост «зубьев» и увеличивается общее искажение (изгиб), в то же время на графике ДНЛ наблюдается увеличение амплитуды пиков при определенных выходных кодах АЦП [3].

Изменение ошибки усиления АЦП AD7888 представлено на рис. 11. Видно, что начиная с 8×10^3 ед. ошибка усиления начинает сильно увеличиваться. Это можно хорошо наблюдать на графике изменения ХП АЦП AD7888 в зависимости от поглощенной дозы (рис. 7).

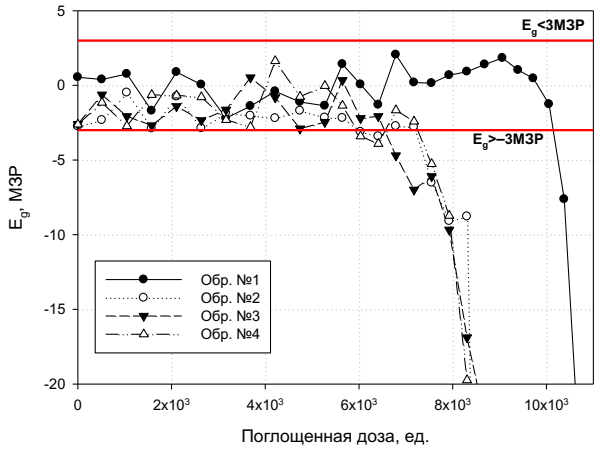


Рис. 11. Изменение ошибки усиления АЦП AD7888 при воздействии поглощенной дозы
(Fig. 11. ADC AD7888 gain error during irradiation)

Изменение динамических параметров SNR и SINAD приведено на рис. 12а и 12б.

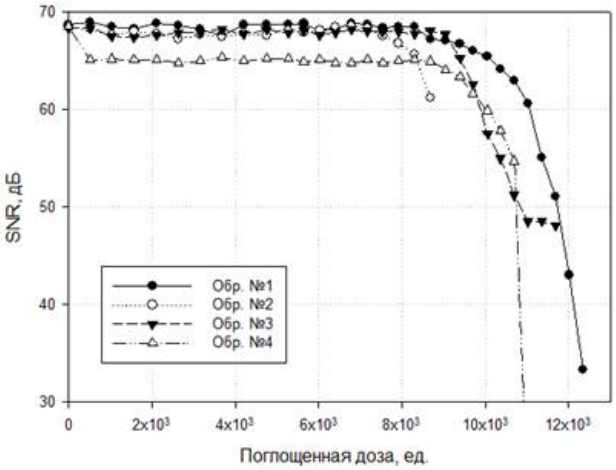


Рис. 12а. Изменение SNR микросхемы AD7888 при воздействии поглощенной дозы

(Fig. 12a. ADC AD7888 SNR during irradiation)

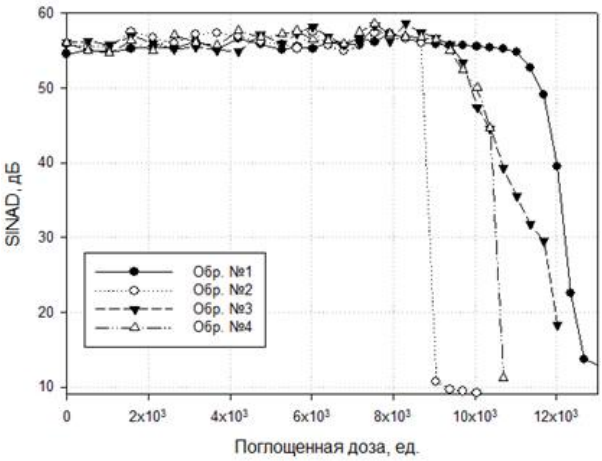


Рис. 12б. Изменение SINAD микросхемы AD7888 при воздействии поглощенной дозы

(Fig. 12b. ADC AD7888 SINAD during irradiation)

Результат выполнения БПФ над выходным оцифрованным сигналом АЦП AD7888 до облучения и после набора 12×10^3 ед. представлен на рис. 13. Частота выборки f_s = 104 kSPS, частота сигнала f_a = 10 кГц, количество отсчетов БПФ = 65536 точек.

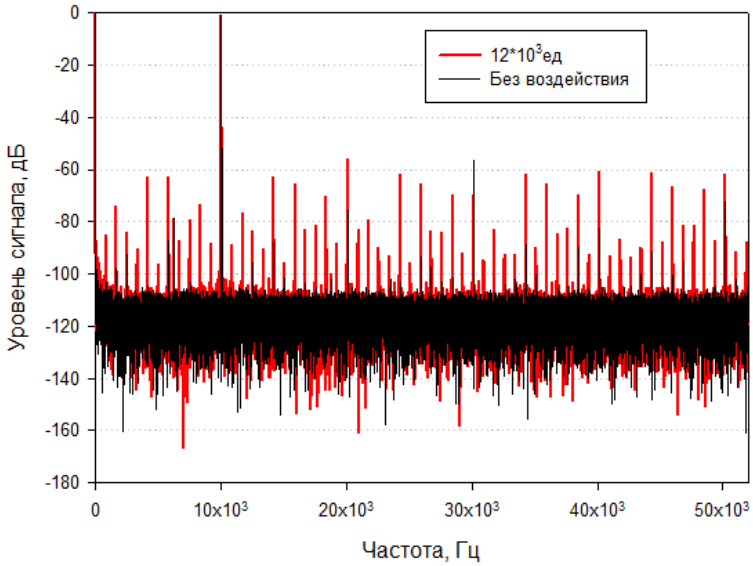


Рис. 13. Результат выполнения БПФ над выходным оцифрованным сигналом АЦП AD7888 до облучения и после набора 12×10^3 ед.

(Fig. 13. FFT array of 65536 points for ADC AD7888 before and after irradiation)

Заключение

Представленные методы тестирования динамических и статических параметров АЦП позволяют дать полную картину об испытываемой микросхеме, а в совокупности с установками, имитирующими воздействия ионизирующего излучения (ИИ) на интегральные схемы (ИС), позволяют прогнозировать их поведение в условиях воздействия

ИИ космического пространства. Данные методы могут быть реализуемы на одном оборудовании, что характеризует их универсальность.

Необходимость полноценного измерения всех критериальных параметров обуславливается в дальнейшем применении микросхем [8]: к примеру, есть приложения, в которых АЦП используется для измерения медленно изменяющихся сигналов. В таком случае статические погрешности будут играть главную роль, а при использовании АЦП в таких приложениях как видео и связь важны высокие значения SFDR и SNR.

СПИСОК ЛИТЕРАТУРЫ:

1. Кестер У. Аналого-цифровое преобразование. – М.: Техносфера, 2007. – 1016 с. ISBN 978-5-94836-146-8.
2. W. Kester, "A Brief History of Data Conversion: A Tale of Nozzles, Relays, Tubes, Transistors, and CMOS," in IEEE Solid-State Circuits Magazine. Vol. 7, no. 3. P. 16–37, Summer 2015. DOI: https://doi.org/10.1109/MSSC.2015.2442371.
3. Торшин Р.С. / Проявление сбоев при воздействии ТЗЧ в современном ЦАП / Сорокоумов Г.С., Бобровский Д.В., Демидов А.А., Калашников О.А., Телец В.А. // 22-я Всероссийская научно-техническая конференция «Стойкость-2019»: тезисы докладов. 2019, Лыткарино, 4-5 июня. С. 244–245.
4. Kester W. / Mixed-Signal and DSP Design Techniques. – M.: Newnes/Elsevier, 2002. – 611 c.
5. I.O. Loskutov, A.B. Karakozov and P.V. Nekrasov, "Automated test setup for functional and parametrical control of microcontrollers with internal ADC," 2016 International Siberian Conference on Control and Communications (SIBCON), Moscow, 2016. P. 1–4. DOI: https://doi.org/10.1109/SIBCON.2016.7491799.
6. IEEE Standard for Terminology and Test Methods for Analog-to-Digital Converters," in IEEE Std 1241-2010 (Revision of IEEE Std 1241-2000). P. 1–139, 14 Jan. 2011, DOI: https://doi.org/10.1109/IEEESTD.2011.5692956.
7. A.O. Akhmetov et al., "Proton Accelerator's Direct Ionization Single Event Upset Test Procedure," 2019 IEEE 31st International Conference on Microelectronics (MIEL), Nis, Serbia, 2019. P. 107–110, DOI: https://doi.org/10.1109/MIEL.2019.8889634.
8. A.Y. Egorov, I.A. Mozhaev, P.V. Nekrasov, D.V. Boychenko and I.O. Loskutov, "Comparison of on-chip ADC testing techniques," 2017 IEEE 30th International Conference on Microelectronics (MIEL), Nis, 2017. P. 247–250. DOI: https://doi.org/10.1109/MIEL.2017.8190113.
9. Барбашов, Вячеслав М.; Калашников, Олег А. Функционально-логическое моделирование дозовых радиационных отказов сф-блоков систем на кристалле. Безопасность информационных технологий, [S.l.]. Т. 24, № 4. P. 80–86, ноябрь 2017. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/283 (дата обращения: 20.07.2020). DOI: http://dx.doi.org/10.26583/bit.2017.4.09.
10. Чумаков А.И. и др. Оценка показателей стойкости интегральных схем при воздействии тяжелых заряженных частиц с использованием различных моделей. Безопасность информационных технологий, [S.l.]. Т. 24, № 1. С. 73–84, 2017. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/58. DOI: http://dx.doi.org/10.26583/bit.2017.1.09.
11. Никифоров А.Ю. / Радиационные эффекты в КМОП ИС.//Телец В.А., Чумаков *А.*И. – М.: Радио и связь, 1994. – 165 с.
12. Чумаков А.И. / Действие космической радиации на интегральные схемы. – М. – Радио и связь, 2004. – 319 с.
13. Dressendorfer P.V. / Ionizing Radiation Effects in MOS devices and Circuits, // T.P.Ma. – M.: Willey, 1989. – 587 p.
14. Demidov, Alexander & Kalashnikov, Oleg & Nikiforov, A. & Tararaksin, Alexander & Telets, Vitaly. (2015). Radiation Behavior and Test Specifics of A-D and D-A Converters. Informacije MIDEM. 45. 153-159.
15. A.B. Karakozov, P.V. Nekraso, D.V. Bobrovsky, G.S. Sorokoumov and V.A. Telets, "Single Event Effects And Total Dose Testing Of Digital To Analog Converters," 2017 17th European Conference on Radiation and Its Effects on Components and Systems (RADECS), Geneva, Switzerland, 2017. P. 1–5, DOI: https://doi.org/10.1109/RADECS.2017.8696263.

REFERENCES:

[1] Kester W. Analog-Digital Conversion. – Copyright © 2004 By Analog Devices, Inc. Printed in the United States of America., 2007. – 1016 p.
[2] Kester W. "A Brief History of Data Conversion: A Tale of Nozzles, Relays, Tubes, Transistors, and CMOS," in IEEE Solid-State Circuits Magazine. Vol. 7, no. 3. P. 16–37, Summer 2015. DOI: https://doi.org/10.1109/MSSC.2015.2442371.

[3] Torshin R.S. Manifestation of failures under the influence of HCP in a modern DAC. Sorokoumav G.S., Bobrovsky D.V., Demidov A.A., Kalashnikov O.A., Telets V.A. 22-ya Vserossiyskaya nauchno-tehnicheskaya konferenciya «Stoykost'-2019»: tezisi dokladov. 2019, Litkarino, 4-5 ijynya. S. 244–245. (in Russian).
[4] Kester W. Mixed-Signal and DSP Design Techniques. – M.: Newnes/Elsevier, 2002. – 611 p.
[5] I.O. Loskutov, A.B. Karakozov and P.V. Nekrasov, "Automated test setup for functional and parametrical control of microcontrollers with internal ADC," 2016 International Siberian Conference on Control and Communications (SIBCON), Moscow, 2016. P. 1–4. DOI: https://doi.org/10.1109/SIBCON.2016.7491799.
[6] IEEE Standard for Terminology and Test Methods for Analog-to-Digital Converters," in IEEE Std 1241-2010 (Revision of IEEE Std 1241-2000). P. 1–139, 14 Jan. 2011, DOI: https://doi.org/10.1109/IEEESTD.2011.5692956.
[7] A.O. Akhmetov et al., "Proton Accelerator's Direct Ionization Single Event Upset Test Procedure," 2019 IEEE 31st International Conference on Microelectronics (MIEL), Nis, Serbia, 2019. P. 107–110, DOI: https://doi.org/10.1109/MIEL.2019.8889634.
[8] A.Y. Egorov, I.A. Mozhaev, P.V. Nekrasov, D.V. Boychenko and I.O. Loskutov, "Comparison of on-chip ADC testing techniques," 2017 IEEE 30th International Conference on Microelectronics (MIEL), Nis, 2017. P. 247–250. DOI: https://doi.org/10.1109/MIEL.2017.8190113. Barbashov, Vyacheslav M.; Kalashnikov, Oleg A. Functional-logic simulation of IP-blocks dose functional
[9] Barbashov, Vyacheslav M.; Kalashnikov, Oleg A. Functional-logic simulation of IP-blocks dose functional failures. IT Security (Russia), [S.l.]. V. 24, no. 4. P. 80–86, nov. 2017. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/283 (accessed: 20.07.2020). DOI: http://dx.doi.org/10.26583/bit.2017.4.09.
[10] Chumakov A.I. et al. Evaluation of indicators of resistance of integrated circuits when exposed to heavy charged particles using various models. IT Security (Russia), [S.l.]. V. 24, no 1. P. 73–84, 2017. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/58. DOI: http://dx.doi.org/10.26583/bit.2017.1.09.
[11] Nikiforov A.Yu. Radiation effects in CMOS IC . Telets V.A., Chumakov A.I. – M.: Radio and communications, 1994. – 165 p. (in Russian).
[12] Chumakov A.I., Effects of Cosmic Radiation on IC, Moscow: Radio i Svyaz', 2004. – 319 p. (in Russian).
[13] Dressendorfer P.V. Ionizing Radiation Effects in MOS devices and Circuits, T.P.Ma. – M.: Willey, 1989. – 587 p.
[14] Demidov, Alexander & Kalashnikov, Oleg & Nikiforov, A. & Tararaksin, Alexander & Telets, Vitaly. (2015). Radiation Behavior and Test Specifics of A-D and D-A Converters. Informacije MIDEM. 45. 153-159.
[15] A.B. Karakozov, P.V. Nekraso, D.V. Bobrovsky, G.S. Sorokoumov and V.A. Telets, "Single Event Effects And Total Dose Testing Of Digital To Analog Converters," 2017 17th European Conference on Radiation and Its Effects on Components and Systems (RADECS), Geneva, Switzerland, 2017. P. 1–5, DOI: https://doi.org/10.1109/RADECS.2017.8696263.

Поступила в редакцию - 26 июля 2020 г. Окончательный вариант – 20 августа 2020 г.
Received – July 26, 2020. The final version – August 20, 2020.

Дмитрий О. Титовец[1], Николай Д. Кравченко[2], Андрей Б. Каракозов[3],
Александр И. Чумаков[4], Дмитрий В. Бобровский[5]
[1–5]Акционерное общество «Экспериментальное научно-производственное объединение СПЕЦИАЛИЗИРОВАННЫЕ ЭЛЕКТРОННЫЕ СИСТЕМЫ»
Каширское ш., 31, Москва, 115409, Россия
[1]e-mail: dotit@spels.ru, http://orcid.org/0000-0002-4934-5945
[2]e-mail: ndkrav@spels.ru, http://orcid.org/0000-0003-4891-3733
[3]e-mail: abkar@spels.ru, http://orcid.org/0000-0002-2910-8870
[4]e-mail: aichum@spels.ru, https://orcid.org/0000-0001-6270-2663
[5]e-mail: dvbob@spels.ru, https://orcid.org/0000-0003-3036-2953

ИСПОЛЬЗОВАНИЕ ФУНКЦИИ ГЕНЕРАЦИИ ЗАРЯДА ПРИ ОЦЕНКЕ ПАРАМЕТРОВ ЧУВСТВИТЕЛЬНОСТИ КМОП МИКРОСХЕМ К ОДИНОЧНЫМ СБОЯМ ПРИ ВОЗДЕЙСТВИИ НЕЙТРОНОВ

DOI: http://dx.doi.org/10.26583/bit.2020.3.08

Аннотация. В связи с текущей тенденцией уменьшения проектных норм микросхем все чаще возникает проблема возникновения одиночных радиационных эффектов сбоев (ОРЭ ОС) в микросхемах при воздействии нейтронов, что приводит к сбоям в работе аппаратуры и потере информации. Для оценки частоты данного эффекта в заданных условиях эксплуатации необходимо иметь зависимость сечения эффекта от энергии нейтронов или параметры чувствительности. В статье предлагается использовать методику на основе функции генерации заряда (ФГЗ) или Burst Generation Rate (BGR) для оценок параметров чувствительности микросхемы по ОРЭ ОС при воздействии нейтронов, а также приведены результаты ее апробации на нескольких микросхемах с малыми проектными нормами: программируемые логические интегральные схемы (ПЛИС) семейств Artix-7 и Spartan-7 фирмы Xilinx и микроконтроллер (МК) семейства STM32 фирмы ST Microelectronics. В качестве контрольно-измерительного оборудования, необходимого для проведения контроля возникновения ОС, использовались модульные измерительные приборы фирмы National Instruments. Рассмотрены области, для которых актуальна данная тема, проведен обзор имеющихся результатов исследований ОС в микросхемах при воздействии нейтронов, описана методика на основе ФГЗ и представлены результаты эксперимента по оценке параметров чувствительности микросхем при воздействии нейтронов.

Ключевые слова: безопасность информации, одиночные сбои, нейтроны, КМОП сверхбольшая интегральная схема (СБИС), функция генерации заряда, микропроцессоры (МП), микроконтроллеры (МК), программируемые логические интегральные схемы (ПЛИС).
Для цитирования: ТИТОВЕЦ, Дмитрий О. et al. ИСПОЛЬЗОВАНИЕ ФУНКЦИИ ГЕНЕРАЦИИ ЗАРЯДА ПРИ ОЦЕНКЕ ПАРАМЕТРОВ ЧУВСТВИТЕЛЬНОСТИ КМОП МИКРОСХЕМ К ОДИНОЧНЫМ СБОЯМ ПРИ ВОЗДЕЙСТВИИ НЕЙТРОНОВ. Безопасность информационных технологий, [S.l.], v. 27, n. 3, p. 89–97, 2020. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1295>. Дата доступа: 08 sep. 2020. DOI: http://dx.doi.org/10.26583/bit.2020.3.08.

Dmitry O. Titovets[1], Nikolay D. Kravchenko[2], Andrey B. Karakozov[3],
Alexander I. Chumakov[4], Dmitry V. Bobrovsky[5]
Joint Stock Company "Experimental Research and Production Association SPECIAL ELECTRONIC SYSTEM",
Kashirskoe sh., 31, Moscow, 115409, Russia
[1]e-mail: dotit@spels.ru, http://orcid.org/0000-0002-4934-5945
[2]e-mail: ndkrav@spels.ru, http://orcid.org/0000-0003-4891-3733
[3]e-mail: abkar@spels.ru, http://orcid.org/0000-0002-2910-8870
[4]e-mail: aichum@spels.ru, https://orcid.org/0000-0001-6270-2663
[5]e-mail: dvbob@spels.ru, https://orcid.org/0000-0003-3036-2953

Using the burst generation rate function to evaluate the parameters of cmos chip sensitivity to single event upsets when exposed to neutrons

DOI: http://dx.doi.org/10.26583/bit.2020.3.08

Abstract. The development of the technological process in electronics has led to the problem of single event upsets (SEU) in microchips when exposed to neutrons causing loss of information and errors. To evaluate sensitivity of CMOS VLSI to SEU caused by neutrons we propose BGR method. To test this approach we apply BGR method to the data obtained by irradiation of several types of ICs: Artix and Spartan FPGAs (Xilinx) and STM32 microcontroller (ST Microelectronics). Test setup was built using modular devices by National Instruments. In this study, we also consider the areas for which neutron influence evaluation is relevant and present an overview of the available data on neutron induced SEU in CMOS chips. A description of the BGR method and experimental results are given.

Keywords: information security, single event upset (SEU), neutrons, CMOS Very Large-Scale Integration (VLSI), Burst Generation Rate (BGR), microprocessors (MPU), microcontrollers (MCU), field-programmable gate array (FPGA).

For citation: TITOVETS, Dmitry O. et al. Evaluating CMOS chip sensitivity parameters to single event upsets under influence of neutrons by the burst generation rate function. IT Security (Russia), [S.l.], v. 27, n. 3, p. 89–97, 2020. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1295>. Date accessed: 08 sep. 2020. DOI: http://dx.doi.org/10.26583/bit.2020.3.08.

Введение

Безопасность информации зависит от устойчивости ее носителей к влиянию различных внешних факторов, в том числе специальных факторов. На протяжении многих лет в России и за рубежом ведутся разработки электронной компонентной базы (ЭКБ), устойчивой к воздействию различных специальных факторов [1–4]. Тенденция уменьшения технологических норм проектирования сверх больших интегральных схем (СБИС) очевидно приводит к снижению пороговых энергий переключений и отказов модулей СБИС [5–7], что в свою очередь приводит к росту чувствительности микросхем к воздействию нейтронного излучения.

1. Актуальные области применения оценок сбоеустойчивости микросхем при воздействии нейтронов

Проблема сбоев от нейтронного излучения актуальна как для микросхем специального применения, например, атомные электростанции и другие ядерные силовые установки, так и для микросхем, применяемых в гражданских отраслях, таких как авионика, суперкомпьютеры, дата-центры и т.д.

Поток нейтронов на высоте 12000 м примерно на три порядка превосходит поток над уровнем моря, а сложность систем управления в авиации требует применения все более мощных вычислительных средств, что объясняет актуальность проблемы оценок сбоеустойчивости системы при воздействии нейтронного излучения.

Поток нейтронов у поверхности Земли на несколько порядков ниже, чем на высотах эксплуатации авиационной аппаратуры, однако из-за огромного количества процессорных СБИС и микросхем памяти, используемых в наземных вычислительных комплексах, частоты сбоев могут превосходить частоты для авионики [8].

ЭКБ современных ядерных установок (как промышленных, так и современных) может включать в себя компоненты, выполненные по техпроцессу менее 500 нм, т.е. потенциально существует риск возникновения ОРЭ ОС в электронных системах ядерных установок [9].

Также оценка параметров чувствительности СБИС по ОРЭ ОС при воздействии нейтронов становится актуальной в области испытаний ЭКБ на стойкость к спецфакторам.

В настоящее время ЭКБ принято испытывать на стойкость к воздействию нейтронов по эффектам структурных повреждений. Однако для ЭКБ с современными проектными нормами выясняется, что изделия, стойкие к эффектам структурных повреждений при воздействии спецфакторов зачастую могут быть чувствительными к эффектам ОС.

2. Методика оценки параметров чувствительности микросхем по ОРЭ ОС при воздействии нейтронов на основе функции генерации заряда

В [10] предложена BGR – методика оценки параметров чувствительности КМОП СБИС к ОС при воздействии нейтронов. Методика BGR основана на использовании функции генерации заряда (ФГЗ), предложенной E. Normand в [11].

Данная методика позволяет построить зависимость сечения ОРЭ в зависимости от энергии нейтронов. Для использования методики BGR достаточно иметь данные о сечения ОС при воздействии нейтронов 2,5 МэВ, 14 МэВ и более 50 МэВ. Воздействие нейтронов с энергией более 50 МэВ допускается заменять протонами с аналогичной энергией.

Зависимость строится в следующей последовательности:

1. Проводятся облучения изделия протонами с энергией более 50 МэВ (рекомендуется 200 МэВ) и нейтронами с энергиями 2,5 МэВ и 14 МэВ и определяются сечения ОРЭ ОС.

2. Определяются отношения сечений ОРЭ ОС:

- отношение сечения ОРЭ ОС при воздействии 200 МэВ протонов к сечению ОРЭ ОС при воздействии 14 МэВ нейтронов;
- отношение сечения ОРЭ ОС при воздействии 14 МэВ нейтронов к сечению ОРЭ ОС при воздействии 2,5 МэВ нейтронов.

3. По графику семейства кривых BGR (рис. 1) определяются отношения значений BGR-функций для каждой кривой при энергиях, равных энергиям в п.2.

4. Из семейства кривых BGR (рис. 1) выбирается та кривая, отношение значений которой наиболее близки с отношениями значений сечений ОРЭ ОС испытуемого объекта. Более высокий приоритет имеет отношение при энергиях 14 МэВ и 2,5 МэВ. Отношение при энергиях 200 МэВ и 14 МэВ используется в случае отсутствия ОРЭ ОС при воздействии 2,5 МэВ нейтронов.

5. Выбранная кривая нормируется таким образом, чтобы она проходила через экспериментально полученные значения сечений ОРЭ ОС.

6. Нормированная кривая принимается за зависимость сечения ОРЭ ОС от энергии нейтронов и используется в дальнейшем для расчета частот событий для заданных условий эксплуатаций.

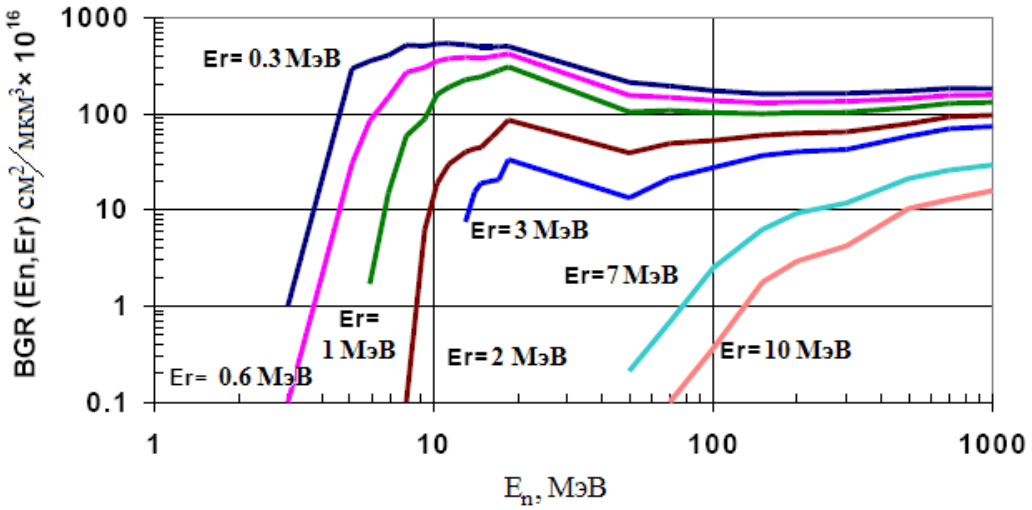


Рис. 1. Семейство кривых BGR
(Fig. 1. Family of graphs)

3. Подготовка КМОП СБИС к проведению испытаний на чувствительность к ОРЭ ОС при воздействии нейтронов

Выбор объектов испытаний

В качестве объектов испытаний были выбраны следующие изделия:

1. XC7A100T (Далее – Artix-7) – ПЛИС;
   - 215000 логических ячеек
   - 13 Мбит памяти ОЗУ
   - Напряжение питания 1,2–3,3 В
   - Проектные нормы 28 нм
2. XC7S25 (Далее – Spartan-7) – ПЛИС;
   - 102000 логических ячеек
   - 4,2 Мбит памяти ОЗУ
   - Напряжение питания 1,2–3,3 В
   - Проектные нормы 28 нм
3. STM32H743 (Далее – STM32) – МК;
   - Техпроцесс 40 нм
   - Ядро ARM Cortex-M7
   - Разрядность 32 бита
   - 2 МБ Flash памяти
   - 512 КБ СОЗУ
   - Проектные нормы 40 нм

Выбор объектов обусловлен, прежде всего, малыми проектными нормами и потенциальным наличием ОРЭ ОС при воздействии нейтронов.

Выбор установок для проведения испытаний

Для проведения экспериментальных испытаний были выбраны следующие установки:

1. НГ-24. Источник нейтронов с возможностью генерации нейтронов с энергиями 2,5 МэВ и 14 МэВ. Использовался в режиме генерации 2,5 МэВ нейтронов. Поток нейтронов $1{,}3 \cdot 10^{11}$ $с^{-1}$.

2. НГ-14. Источник нейтронов с возможностью генерации нейтронов с энергиями 2,5 МэВ и 14 МэВ. Использовался в режиме генерации 14 МэВ нейтронов. Поток нейтронов равен $2{,}0 \cdot 10^{10}$ $с^{-1}$.

3. ПРОМЕТЕУС. Источник протонного пучка с энергией протонов от 50 до 250 МэВ. Использовался в режиме генерации протонного пучка с энергией 200 МэВ.

Методика регистрации ОС в объектах испытаний

Методика регистрации ОС в объектах испытаний имеет принципиальное различие для объектов Artix-7, Spartan-7 и объекта STM32.

В случае испытаний объектов Artix-7 и Spartan-7 до воздействия в конфигурационную память ПЛИС через интерфейс JTAG загружается тестовая прошивка. Затем проводилась верификация зашивки. В случае успешной верификации проводилось облучение частицами с заданной энергией и флюенсом, после которого еще раз производилась верификация, показывающая количество сбившихся ячеек памяти.

В случае испытаний объекта STM32 до испытательного воздействия в МК загружалась тестовая программа, позволяющая проводить запись и контроль сохранности информации в блоках памяти МК во время испытательного воздействия и передавать результаты по интерфейсу UART. Во время воздействия непрерывно тестировался блок памяти ОЗУ МК. ОС накапливались и информация об их количестве записывалась в лог-файл.

4. Результаты испытаний изделий по ОРЭ ОС при воздействии нейтронов

Количество ОС в объектах испытаний, а также сечение ОС при различных значениях энергий частиц приведено в табл. 1.

Таблица 1. Количество ОС в объектах испытаний при различных значениях энергий частиц

Образец	Энергия частиц, МэВ	Количество ОС	Емкость, бит	Флюенс, $1/см^2$	Сечение, $см^2$/бит
Artix-7	2,5	24	13 Мбит	$2{,}7 \cdot 10^{10}$	$7{,}0 \cdot 10^{-17}$
	14	1517		$1{,}0 \cdot 10^{10}$	$1{,}2 \cdot 10^{-14}$
	200	1254		$1{,}0 \cdot 10^{10}$	$1{,}0 \cdot 10^{-14}$
Spartan-7	2,5	8	4,2 Мбит	$4{,}7 \cdot 10^{10}$	$4{,}3 \cdot 10^{-17}$
	14	3274		$1{,}0 \cdot 10^{10}$	$7{,}9 \cdot 10^{-14}$
	200	407		$1{,}0 \cdot 10^{10}$	$9{,}8 \cdot 10^{-15}$
STM32	14	152	4 Мбит	$6{,}0 \cdot 10^{10}$	$6{,}1 \cdot 10^{-16}$
	200	35		$6{,}0 \cdot 10^{10}$	$1{,}4 \cdot 10^{-16}$

Из табл. 2 и 3 видно, что для образца Artix-7 наиболее точно подходит кривая BGR с Er = 0,3 МэВ, а для образца Spartan-7 кривая с Er = 0,6 МэВ.

Таблица 2. Отношения значений функции BGR при энергиях частиц 2,5 МэВ, 14 МэВ и 200 МэВ

Кривая BGR	Отношение 200 к 14 МэВ	Отношение 14 к 2,5 МэВ
Er = 0,3 МэВ	0,321	110,703
Er = 0,6 МэВ	0,339	750,027
Er = 1 МэВ	0,422	157,620
Er = 2 МэВ	1,366	–
Er = 3 МэВ	2,633	–

Таблица 3. Отношения значений сечечний ОС в испытанных образцах при энергиях частиц 2,5 МэВ, 14 МэВ и 200 МэВ

Образец	Отношение 200 к 14 МэВ	Отношение 14 к 2,5 МэВ
Artix-7 ()	0,867	164,835
Spartan-7	0,124	1833,333
STM32	0,229	–

Пронормировав выбранные кривые BGR на экспериментальные значения сечений эффекта получаются зависимости сеченияэффекта от энергии нейтронов (рис. 2–4).

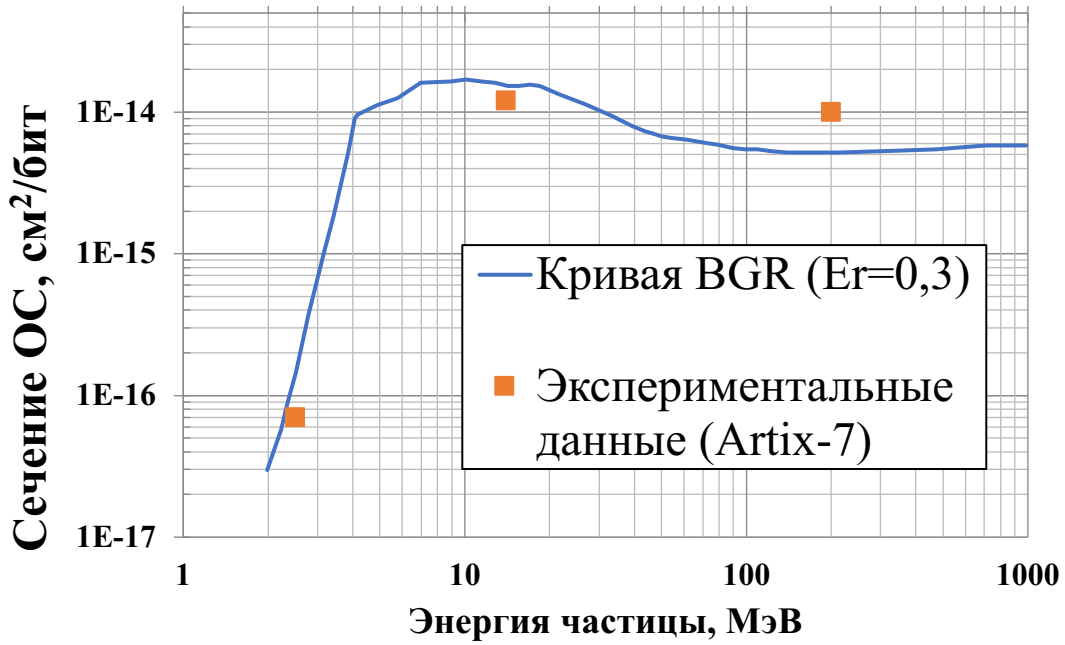


Рис. 2. Зависимость сечения ОС в Artix-7 от энергии нейтронов
(Fig. 2. Dependence of the cross section of SEU in Artix-7 on the energy of particles)

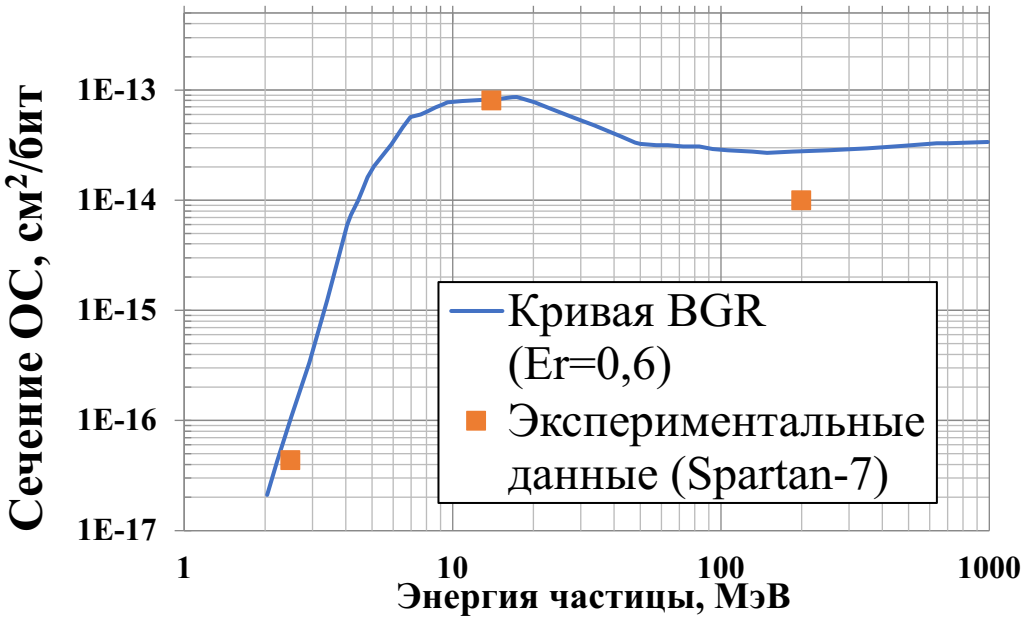


Рис. 3. Зависимость сечения ОС в Spartan-7 от энергии нейтронов
(Fig. 3. Dependence of the cross section of SEU in Spartan-7 on the energy of particles)

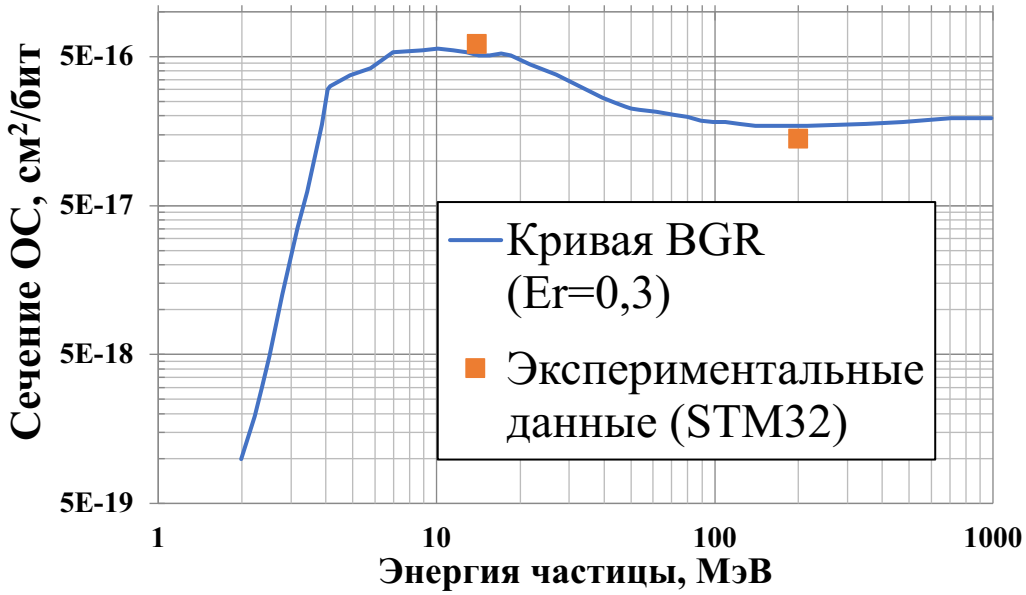


Рис. 4. Зависимость сечения ОС в STM32 от энергии нейтронов
(Fig. 4. Dependence of the cross section of SEU in STM32 on the energy of particles)

Заключение

В статье представлены результаты апробации методики оценки параметров чувствительности микросхем к воздействию нейтронов по ОРЭ ОС на трех типах микросхем (микроконтроллер STM32H743, ПЛИС XC7A100T, ПЛИС XC7S25), которая основана на пропорциональности зависимостей сечения эффекта ОС и функции BGR от энергии воздействующего нейтронного излучения. Выбор объектов обуславливался

малыми проектными нормами и потенциальной чувствительностью к воздействию нейтронного излучения.

Экспериментальные результаты удовлетворительно согласуются с теоретическими зависимостями BGR и являются аргументом в пользу применимости данного метода оценки параметров чувствительности микросхем к воздействию нейтронов по ОРЭ.

СПИСОК ЛИТЕРАТУРЫ:

1. Никифоров А.Ю. / Радиационные эффекты в КМОП ИС.//Телец В.А., Чумаков А.И. – М.: Радио и связь, 1994. – 165 с.
2. Чумаков А.И. / Действие космической радиации на интегральные схемы. – М. – Радио и связь, 2004. – 319 с.
3. G.C. Messenger and M. Ash Single Event Phenomena London U.K.:Chapman & Hall 1997. – 368 p.
4. Чумаков, Александр И. и др. Требования и нормы испытаний по радиационной стойкости интегральных схем к эффектам воздействия тяжёлых заряженных частиц. Безопасность информационных технологий, [S.l.], Т. 27, №. 1. С. 83–97, фев. 2020. URL: https://bit.mephi.ru/index.php/bit/article/view/1254 (дата обращения: 18.08.2020). DOI: http://dx.doi.org/10.26583/bit.2020.1.07.
5. A.E. Rudenkov, A.O. Akhmetov, D.V. Bobrovsky, A.I. Chumakov, A.V. Yanenko and V.M. Uzhegov, "The prediction for single event latchup sensitivity parameters of digital CMOS ICs based on its technological features," 2017 IEEE 30th International Conference on Microelectronics (MIEL), Nis, 2017. P. 287–290. DOI: http://dx.doi.org/10.1109/MIEL.2017.8190123.
6. A.B. Boruzdina, A.V. Yanenko, A.V. Ulanova, A.I. Chumakov, D.V. Bobrovskiy and V.M. Uzhegov, "Microdose effects in SRAM cells under heavy ion irradiation," 2017 17th European Conference on Radiation and Its Effects on Components and Systems (RADECS), Geneva, Switzerland, 2017. P. 1–3, DOI: https://doi.org/10.1109/RADECS.2017.8696109.
7. Chumakov, A.I., Bobrovsky, D.V., Pechenkin, A.A. et al. Mechanisms of Initiation of Unstable Latchup Effects in CMOS ICs. Russ Microelectron 48, 250–254 (2019). DOI: https://doi.org/10.1134/S1063739719040036.
8. E. Normand, "Single-event effects in avionics," in IEEE Transactions on Nuclear Science. Vol. 43, no. 2. P. 461–474, April 1996. DOI: https://doi.org/10.1109/23.490893.
9. A.I. Chumakov, A.V. Sogoyan, A.B. Boruzdina, A.A. Smolin and A. A. Pechenkin, "Multiple Cell Upset Mechanisms in SRAMs," 2015 15th European Conference on Radiation and Its Effects on Components and Systems (RADECS), Moscow, 2015. P. 1–5. DOI: https://doi.org/10.1109/RADECS.2015.7365638.
10. А.И. Чумаков, А.В. Афонин. Оценка энергетической зависимости сечений одиночных радиационных эффектов при нейтронном облучении// Научн.-техн. Сборник «Радиационная стойкость электронных систем – Стойкость-2015».-М.: СПЭЛС-НИИП. 2015. С. 177–178.
11. E. Normand and W.R. Doherty, "Incorporation of ENDF-V neutron cross section data for calculating neutron-induced single event upsets," in IEEE Transactions on Nuclear Science. Vol. 36, no. 6. P. 2349–2355, Dec. 1989. DOI: https://doi.org/0.1109/23.45447.

REFERENCES:

[1] Nikiforov A.Yu. Radiation effects in CMOS IC. Telets V.A., Chumakov A.I. – M.: Radio and communications, 1994. – 165 p. (in Russian).
[2] Chumakov A.I., Effects of Cosmic Radiation on IC, Moscow: Radio i Svyaz’, 2004. – 319 p. (in Russian).
[3] G. C. Messenger and M. Ash Single Event Phenomena London U.K.:Chapman & Hall 1997. – 368 p.
[4] Chumakov, Aleksandr I. et al. Hardness assurance levels and requirements for single event effects testing of integrated circuits. IT Security (Russia), [S.l.]. V. 27, no. 1. P. 83–97, feb. 2020. URL: https://bit.mephi.ru/index.php/bit/article/view/1254 (accessed: 18.08.2020). DOI: http://dx.doi.org/10.26583/bit.2020.1.07 (in Russian).
[5] A.E. Rudenkov, A.O. Akhmetov, D.V. Bobrovsky, A.I. Chumakov, A.V. Yanenko and V.M. Uzhegov, "The prediction for single event latchup sensitivity parameters of digital CMOS ICs based on its technological features," 2017 IEEE 30th International Conference on Microelectronics (MIEL), Nis, 2017. P. 287–290. DOI: http://dx.doi.org/10.1109/MIEL.2017.8190123.
[6] A.B. Boruzdina, A.V. Yanenko, A.V. Ulanova, A.I. Chumakov, D.V. Bobrovskiy and V.M. Uzhegov, "Microdose effects in SRAM cells under heavy ion irradiation," 2017 17th European Conference on Radiation and Its Effects on Components and Systems (RADECS), Geneva, Switzerland, 2017. P. 1–3, DOI: https://doi.org/10.1109/RADECS.2017.8696109.

[7] Chumakov A.I., Bobrovsky D.V., Pechenkin A.A. et al. Mechanisms of Initiation of Unstable Latchup Effects in CMOS ICs. Russ Microelectron 48, 250–254 (2019). DOI: https://doi.org/10.1134/S1063739719040036.

[8] E. Normand, "Single-event effects in avionics," in IEEE Transactions on Nuclear Science. Vol. 43, no. 2. P. 461–474, April 1996. DOI: https://doi.org/10.1109/23.490893.

[9] A.I. Chumakov, A.V. Sogoyan, A.B. Boruzdina, A.A. Smolin and A. A. Pechenkin, "Multiple Cell Upset Mechanisms in SRAMs," 2015 15th European Conference on Radiation and Its Effects on Components and Systems (RADECS), Moscow, 2015. P. 1–5. DOI: https://doi.org/10.1109/RADECS.2015.7365638.

[10] A.I. Chumakov, A.V. Afonin. Estimation of the energy dependence of cross sections of single radiation effects under neutron irradiation // Sci.-tech. Magazine «Radiation resistance of electronic systems – Stoikost-2015».- M.: SPELS-NIIP. 2015. P.177–178 (in Russian).

[11] E. Normand and W.R. Doherty, "Incorporation of ENDF-V neutron cross section data for calculating neutron-induced single event upsets," in IEEE Transactions on Nuclear Science. Vol. 36, no. 6. P. 2349–2355, Dec. 1989. DOI: https://doi.org/0.1109/23.45447.

Поступила в редакцию – 26 июля 2020 г. Окончательный вариант – 20 августа 2020 г.
Received – July 26, 2020. The final version – August 20, 2020.

Владислав Д. Калашников[1], Алексей Ю. Егоров[2], Армен В. Согоян[3],
Анастасия В. Уланова[4], Андрей Б. Каракозов[5], Павел А. Баламутов[6]
[1–4]Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, Москва, 115409, Россия
[5]Акционерное общество «Экспериментальное научно-производственное объединение
СПЕЦИАЛИЗИРОВАННЫЕ ЭЛЕКТРОННЫЕ СИСТЕМЫ»,
Каширское ш., 31, Москва, 115409, Россия
[6]Госкорпорация «Росатом»
ул. Большая Ордынка, 24, Москва, 119017, Россия
[1]e-mail: vdkal@spels.ru, http://orcid.org/0000-0003-1876-2540
[2]e-mail: ayegor@spels.ru, http://orcid.org/0000-0001-5588-0437
[3]e-mail: avsog@spels.ru, http://orcid.org/0000-0002-9380-239X
[4]e-mail: avulan@spels.ru, http://orcid.org/0000-0001-7376-6339
[5]e-mail: abkar@spels.ru, http://orcid.org/0000-0002-2910-8870
[6]e-mail: PaABalamutov@rosatom.ru, http://orcid.org/0000-0001-6185-3654

ВЛИЯНИЕ ПОВЫШЕННОЙ ИНТЕНСИВНОСТИ НАБОРА ДОЗЫ ИОНИЗИРУЮЩЕГО ИЗЛУЧЕНИЯ НА СТОЙКОСТЬ КМОП МИКРОСХЕМ СИСТЕМ ПЕРЕДАЧИ ИНФОРМАЦИИ

DOI: http://dx.doi.org/10.26583/bit.2020.3.09

Аннотация. В данной работе проведено исследование влияния интенсивности воздействия при наборе дозы на стойкость КМОП интегральных схем (ИС). Исследовано 3 типа микросхем, изготовленных по проектным нормам от 0,8 мкм до 3 мкм, использующихся в различных системах передачи информации: 1586ИН4, HEF4093BT и MC14504B. Исследования проводились с использованием ускорителя электронов У-31/33, работающего в тормозном режиме (средняя интенсивность воздействия) и режиме генерации пачки электронных импульсов (повышенная интенсивность). В результате исследований установлено, что повышение интенсивности воздействия на четыре порядка может приводить к снижению уровня стойкости ИС до 30 раз. Данное обстоятельство необходимо учитывать при проведении испытаний КМОП ИС на стойкость к воздействию импульсного ионизирующего излучения. Результаты, полученные в представленной работе, подтверждают теоретические представления о влиянии эффектов повышенной интенсивности набора дозы ионизирующего излучения на дозовую стойкость КМОП ИС.
Ключевые слова: безопасность информации, радиационная стойкость, КМОП СБИС, поглощённая доза, интенсивность набора дозы.
Для цитирования: КАЛАШНИКОВ, Владислав Д. et al. ВЛИЯНИЕ ПОВЫШЕННОЙ ИНТЕНСИВНОСТИ НАБОРА ДОЗЫ ИОНИЗИРУЮЩЕГО ИЗЛУЧЕНИЯ НА СТОЙКОСТЬ КМОП МИКРОСХЕМ СИСТЕМ ПЕРЕДАЧИ ИНФОРМАЦИИ. Безопасность информационных технологий, [S.l.], v. 27, n. 3, p. 98–103, 2020. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1296>. Дата доступа: 14 sep. 2020. DOI: http://dx.doi.org/10.26583/bit.2020.3.09.

Vladislav D. Kalashnikov[1], Alexey Yu. Egorov[2], Armen V. Sogoyan[3],
Anastasia V. Ulanova[4], Andrey B. Karakozov[5], Pavel A. Balamutov[6]
[1-4]National Research Nuclear University MEPhI (Moscow Engineering Physics Institute),
Kashirskoe sh., 31, Moscow, 115409, Russia
[5]Joint Stock Company "Experimental Research and Production Association
SPECIAL ELECTRONIC SYSTEM"
Kashirskoe sh., 31, Moscow, 115409, Russia
[6]State Atomic Energy Corporation «Rosatom»
Bolshaya Ordynka St., 24, Moscow, 119017, Russia
[1]e-mail: vdkal@spels.ru, http://orcid.org/0000-0003-1876-2540
[2]e-mail: ayegor@spels.ru, http://orcid.org/0000-0001-5588-0437
[3]e-mail: avsog@spels.ru, http://orcid.org/0000-0002-9380-239X
[4]e-mail: avulan@spels.ru, http://orcid.org/0000-0001-7376-6339

[5]*e-mail: abkar@spels.ru, http://orcid.org/0000-0002-2910-8870*
[6]*e-mail: PaABalamutov@rosatom.ru, http://orcid.org/0000-0001-6185-3654*

The influence of high ionizing dose rate on CMOS IC radiation hardness used in data transmission elements

DOI: http://dx.doi.org/10.26583/bit.2020.3.09

Abstract. In this work, the effect of the irradiation intensity on the radiation hardness of CMOS integrated circuits (ICs) was studied. We investigated 3 types of ICs manufactured according to design rules from 0.8 to 3 microns, and used in various information transmission systems: 1586IN4, HEF4093BT and MC14504B. The U-31/33 accelerator of electrons has been used for the study in both gamma-ray mode (for moderate intensity) and pulse electron generation mode (for high intensity). As a result, it was revealed that an increase in the intensity of exposure by 4 orders of magnitude might result in a radiation hardness decrease up to factor of 30. This circumstance has to be taken into account when testing CMOS ICs for radiation hardness to high intensity effects. The obtained experimental data confirm theoretical understanding of the influence of increased irradiation intensity on the dose hardness of CMOS ICs.
Keywords: information security, radiation hardness, CMOS VLSI, total dose effect, dose-rate.
For citation: KALASHNIKOV, Vladislav D. et al. The influence of high ionizing dose rate on CMOS IC radiation hardness used in da-ta transmission elements. IT Security (Russia), [S.l.], v. 27, n. 3, p. 98–103, 2020. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1296>. Date accessed: 14 sep. 2020. DOI: http://dx.doi.org/10.26583/bit.2020.3.09.

Введение

Работоспособность накопителей памяти и обслуживающих их электронных компонентов (повторители, преобразователи уровня, приемопередатчики) зависит от внешних условий их эксплуатации. Одним из наиболее критичных внешних дестабилизирующих факторов, способных нарушить работоспособность устройств накопления и передачи информации является ионизирующее излучение (ИИ).

1. Теоретические представления о повышенной интенсивности набора дозы ИИ

Реакция современных КМОП СБИС на воздействие импульсного ИИ [1–3], в общем случае, будет определяться как процессами переноса неравновесного заряда в полупроводниковой структуре (эффекты «мощности дозы» – кратковременные параметрические и функциональные отказы, защелкивание), так и процессами переноса, захвата и релаксации радиационно-индуцированного заряда в паразитных диэлектрических структурах (эффекты «полной дозы») [4–10].

Сложившаяся практика радиационных испытаний изделий электронной компонентной базы (ЭКБ) предполагает определение времени потери работоспособности изделий по эффектам мощности дозы, тогда как переходным процессам, обусловленным накопленной дозой (перенос и релаксация заряда в диэлектрике) [11, 12], традиционно уделяется меньшее внимание. При этом экспериментальная оценка стойкости СБИС к воздействию импульсного ИИ по отношению к эффектам поглощенной дозы проводится на моделирующих установках при интенсивностях ИИ 10…1000 рад/с. Такой подход может приводить к существенной переоценке уровня стойкости и недооценке времени потери работоспособности СБИС по сравнению с воздействием импульсного излучения в реальных условиях [13]. Это обстоятельство требует развития методов испытаний, позволяющих учесть влияние эффектов переноса и релаксации заряда в диэлектрике при импульсном наборе дозы.

Как правило, на малых временах реакция изделия, связанная с формированием заряда в диэлектрике, определяется переносом заряда, а на более позднем этапе – его релаксацией (отжигом) [14, 15]. Процесс релаксации захваченного заряда проявляется в

зависимости уровня отказа изделия от интенсивности ИИ [4, 13] при временах облучения, превосходящих характерную длительность переноса носителей через диэлектрик.

2. Объект исследования

В работе исследовалось влияние данного механизма на уровень стойкости КМОП БИС при воздействии ИИ высокой интенсивности. Объектами исследований являлись микросхемы передачи информации [11], такие как: микросхемы серии 1586ИН4 (двухканальный приемник двуполярного последовательного кода), предназначенные для построения приемных устройств каналов информационного обмена по ГОСТ 18977, изготовленные по КМОП технологии с проектными нормами 2 мкм; микросхемы HEF4093BT (четыре двухвходовых вентиля И-НЕ с входами триггера Шмидта), изготовленные по КМОП технологии, фирмы Phillips и микросхемы MC14504B (не инвертирующий ТТЛ-КМОП/КМОП-КМОП преобразователь логического уровня), изготовленные по КМОП технологии с проектными нормами 3 мкм с питаниями входа и выхода 3–18 В фирмы On Semiconductor.

На вход D1A микросхемы серии 1586ИН4 подавался периодический сигнал (меандр) частотой 1 МГц с размахом сигнала от 0 В до +5 В. На вход микросхемы D1B синфазно с входом D1A подавался периодический сигнал (меандр) частотой 1 МГц с размахом сигнала от 0 В до +5 В. На остальные входы микросхемы были поданы сигналы низкого логического уровня. Контроль функционирования производился с помощью осциллографа по выходному сигналу микросхемы OUTA_1. Критерием работоспособности являлось наличие на выходе переменного сигнала (меандра) с амплитудой не менее 1,65 В.

На вход I1 микросхемы HEF4093BT подавался периодический сигнал (меандр) частотой 20 кГц. Остальные входы микросхемы были подтянуты к питанию с помощью резисторов номиналом 5 кОм. Контроль функционирования проводился с помощью осциллографа по выходному сигналу O1 микросхемы. Критерием работоспособности являлось наличие на выходе переменного сигнала (меандра).

На входы A_{IN} микросхемы MC14504B подавался периодический сигнал (меандр) частотой 1 МГц с размахом сигнала от 0 В до +3,6 В. На остальные входы микросхемы были поданы сигналы низкого логического уровня. Контроль функционирования проводился с помощью осциллографа по выходным сигналам микросхем A_{OUT}. Критерием работоспособности являлось наличие на выходе переменного сигнала (меандра).

Исследования проводились с использованием ускорителя электронов «У-31/33», работающего в режиме тормозного излучения и в режиме электронного пучка. Образцы были разделены на две группы. Образцы первой группы облучались при интенсивностях 20 ед./с (1586ИН4), 40 ед./с (HEF4093BT), и 134 ед./с (MC14504B), образцы второй группы облучались при интенсивностях $7 \cdot 10^5$ ед./с (1586ИН4) и $2{,}4 \cdot 10^6$ ед./с (HEF4093BT) и $0{,}95 \cdot 10^6$ ед./с (MC14504B). Зависимости выходного уровня микросхемы 1586ИН4 от набранной дозы приведены на рис. 1.

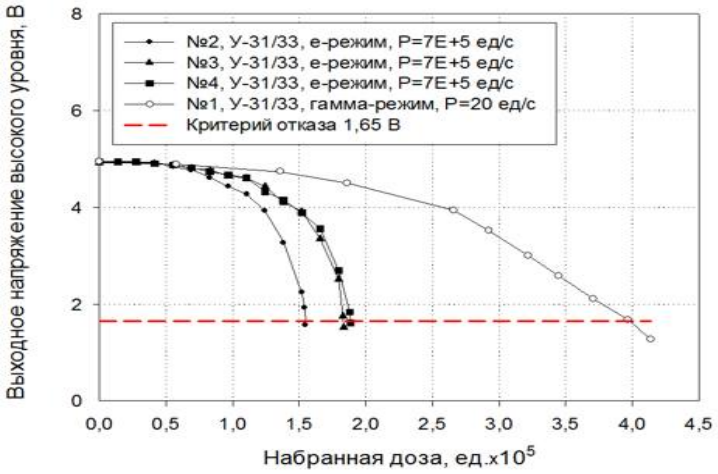


Рис. 1. Зависимости выходного напряжения высокого уровня U_{OH} микросхемы 1586ИН4 от набранной дозы при использовании линейного ускорителя электронов «У-31/33», работающего в электронном (черные маркеры) и тормозном (белые маркеры) режимах

Fig. 1. The output voltage VOH of the 1586IN4 IC as function of total dose for different irradiation intensities. Black markers - high intensity (pulse electron irradiation); white markers - moderate intensity (gamma ray irradiation).

3. Результаты исследований

Установленные уровни отказа микросхем приведены в табл. 1. Отличие в уровнях стойкости составило около трех раз при разнице в интенсивностях на четыре порядка (для 1586ИН4) и на пять порядков (для HEF4093BT).

Таблица 1. Уровни отказа микросхем

Образец	Интенсивность, ед/с	Доза отказа, ед.
Микросхемы 1586ИН4		
1	20	$39 \cdot 10^4$
2	$7 \cdot 10^5$	$15 \cdot 10^4$
3	$7 \cdot 10^5$	$18 \cdot 10^4$
4	$7 \cdot 10^5$	$19 \cdot 10^4$
Микросхемы HEF4093BT		
21	40	$4{,}3 \cdot 10^4$
25	40	$4{,}7 \cdot 10^4$
2	$2{,}4 \cdot 10^6$	$1{,}7 \cdot 10^4$
8	$2{,}4 \cdot 10^6$	$1{,}7 \cdot 10^4$
3	$2{,}4 \cdot 10^6$	$1{,}7 \cdot 10^4$
Микросхемы MC14504B		
4	$0{,}95 \cdot 10^6$	$1 \cdot 10^4$
5	$0{,}95 \cdot 10^6$	$1 \cdot 10^4$
1	134	$31 \cdot 10^4$
2	134	$29 \cdot 10^4$

Заключение

Полученные в работе данные дают количественную оценку влияния высокой интенсивности воздействия на дозовую стойкость исследованных объектов. Так, для микросхемы MC14504B соотношение уровней отказа при средней и высокой интенсивностях составляет около 30 раз, а для остальных типов – 3-4 раза. Результаты экспериментов позволяют сделать вывод о значимости исследованного эффекта.

СПИСОК ЛИТЕРАТУРЫ:

1. Никифоров А.Ю. Радиационные эффекты в КМОП ИС // Телец В.А., Чумаков А.И. – М: Радио и связь, 1994. – 165с.
2. Устюжанинов В.Н. Эффекты импульсного облучения цифровых электронных систем // Вопросы атомной науки и техники. Серия: Физика радиационного воздействия на радиоэлектронную аппаратуру. 2013. № 1. С 50–54. URL: https://elibrary.ru/title_about.asp?id=25748 (дата обращения: 01.08.2020).
3. Устюжанинов В.Н. Ионизационные эффекты импульсного облучения БИС // Вопросы атомной науки и техники. Серия: Физика радиационного воздействия на радиоэлектронную аппаратуру. 2013. № 1. С. 55–60.
4. Ionizing Radiation Effects in MOS devices and Circuits, ed. by T.P.Ma and P.V. Dressendorfer, J.Wiley& Sons, New York, 1989. DOI: https://doi.org/10.1148/radiology.174.3.886.
5. H. Barnaby. Total-ionizing-dose effects in modern CMOS technologies, Nuclear Science, IEEE Transactions on Vol. 53. P. 3103–3121, Dec 2006. DOI: https://doi.org/10.1109/TNS.2006.885952.
6. Согоян А.В. Оценка стойкости КМОП СБИС к фактору поглощенной дозы при воздействии импульсного излучения // Микроэлектроника. 2011. Т. 40, № 3. С. 200–208 URL: https://www.elibrary.ru/item.asp?id=15257433 (дата обращения: 01.08.2020).
7. Согоян А.В., Давыдов Г.Г. Особенности формирования и релаксации заряда в КНС структурах при воздействии ионизирующего излучения // Микроэлектроника. 2011. Т. 40, № 3. С. 209–223 URL: https://elibrary.ru/title_about.asp?id=7900 (дата обращения: 01.08.2020).
8. H. Barnaby, M. Mclain, I. S. Esqueda. Total-ionizing-dose effects on isolation oxides in modern CMOS technologies, Nuclear Instruments and Methods in Physics Research B 261 (2007) 1142–1145. DOI: https://doi.org/ 10.1016/j.nimb.2007.03.109.
9. Y.M. Moskovskaya, A. Y. Nikiforov, D.V.Bobrovsky, A.V. Ulanova, and A. A Zhukov. Process Parameters Variations Influence on CMOS IC's Hardness to total Ionizing Dose, in Proc. 30th Int. Conf. on Microelectronics, MIEL 2017; Nis, Serbia, October 2017. P. 275–277. DOI: https://doi.org/10.1109/MIEL.2017.8190120.
10. Барбашов, Вячеслав М.; Калашников, Олег А. Функционально-логическое моделирование дозовых радиационных отказов сф-блоков систем на кристалле. Безопасность информационных технологий, [S.l.]. Т. 24, №. 4. С. 80–86, ноябрь 2017. ISSN 2074-7136. URL: <https://bit.mephi.ru/index.php/bit/article/view/283> (дата обращения: 01.08.2020). DOI: https://doi.org/10.26583/bit.2017.4.09.
11. Киргизова А.В., Никифоров А.Ю., Григорьев Н.Г., Поляков И.В., Скоробогатов П.К. Доминирующие механизмы информационных сбоев КМОП КНС БИС оперативных запоминающих устройств при воздействии импульсного ионизирующего излучения» // Микроэлектроника . 2006, Т. 35, № 3. С. 191–208.
12. Зинченко В.Ф., Романенко А.А., Усеинов Р.Г., Ужегов В.М. Радиационные эффекты в изделиях полупроводниковой микроэлектроники современных технологий, Вопросы атомной науки и техники. Серия: Физика радиационного воздействия на радиоэлектронную аппаратуру. 2016. № 1. С 29–36. URL: https://www.elibrary.ru/item.asp?id=26131819 (дата обращения: 01.08.2020).
13. Никифоров А.Ю., Согоян А.В. Моделирование дозовых эффектов в паразитных МОП-структурах КМОП БИС при воздействии высокоинтенсивного импульсного ионизирующего излучения // Микроэлектроника. 2004. Т. 33. № 2. С. 108. URL: https://www.elibrary.ru/item.asp?id=17662355 (дата обращения: 01.08.2020).
14. Sogoyan A.V. and Polunin V.A. Modeling of recombination in SiO_2 under the effect of ionizing radiation by the Monte Carlo method, Russian Microelectronics. Vol. 40, no. 3. P. 176–184, 2011. DOI: https://doi.org/10.1134/S1063739711030061.
15. Таперо К.И. Эффекты низкоинтенсивного облучения в приборах и интегральных схемах на базе кремения // Известия высших учебных заведений. Материалы электронной техники. 2016. Т. 19, № 1. С. 5–21. DOI: https://doi.org/10.17073/1609-3577-2016-1-5-21.

REFERENCES:

[1] Nikiforov A.Yu. Radiation effects in CMOS IC. Telets V.A., Chumakov A.I. – M.: Radio and communications, 1994. – 165 p. (in Russian).

[2] Ustyuzhaninov V.N. Effekty impul'snogo oblucheniya cifrovyh elektronnyh sistem. Voprosy atomnoj nauki i tekhniki. Seriya: Fizika radiacionnogo vozdejstviya na radioelektronnuyu apparaturu. 2013. No 1. S. 50–54. URL: https://elibrary.ru/title_about.asp?id=25748 (accessed: 01.08.2020) (in Russian).

[3] Ustyuzhaninov V.N. Ionizacionnye effekty impul'snogo oblucheniya BIS. Voprosy atomnoj nauki i tekhniki. Seriya: Fizika radiacionnogo vozdejstviya na radioelektronnuyu apparaturu. 2013. No 1. S. 55–60 (in Russian).

[4] Ionizing Radiation Effects in MOS devices and Circuits, ed. by T.P.Ma and P.V. Dressendorfer, J.Wiley& Sons, New York, 1989. DOI: https://doi.org/10.1148/radiology.174.3.886.

[5] H. Barnaby. Total-ionizing-dose effects in modern CMOS technologies, Nuclear Science, IEEE Transactions on, Vol. 53. P. 3103–3121, Dec 2006 DOI: https://doi.org/10.1109/TNS.2006.885952.

[6] Sogoyan A.V. Otsenka stojkosti KMOP SBIS k faktoru pogloshchennoj dozy pri vozdejstvii impul'snogo izlucheniya. Mikroelektronika. 2011. T. 40, no 3. S. 200–208 (in Russian). URL: https://www.elibrary.ru/item.asp?id=15257433 (accessed: 01.08.2020).

[7] Sogoyan A.V., Davydov G.G. Osobennosti formirovaniya i relaksacii zaryada v KNS strukturah pri vozdejstvii ioniziruyushchego izlucheniya. Mikroelektronika. 2011. T. 40, no 3. S. 209–223. URL: https://elibrary.ru/title_about.asp?id=7900 (accessed: 01.08.2020) (in Russian).

[8] H. Barnaby, M. Mclain, I.S. Esqueda. Total-ionizing-dose effects on isolation oxides in modern CMOS technologies, Nuclear Instruments and Methods in Physics Research B 261 (2007), 1142–1145. DOI: https://doi.org/10.1016/j.nimb.2007.03.109.

[9] Y.M. Moskovskaya, A.Y. Nikiforov, D.V.Bobrovsky, A.V. Ulanova and A.A Zhukov. Process Parameters Variations Influence on CMOS IC's Hardness to total Ionizing Dose, in Proc. 30th Int. Conf. on Microelectronics, MIEL 2017; Nis, Serbia, October 2017. P. 275–277.

[10] Barbashov, Vyacheslav M.; Kalashnikov, Oleg A. Functional-logic simulation of IP-blocks dose functional failures. IT Security (Russia), [S.l.], V. 24, no 4. P. 80–86, nov. 2017. ISSN 2074-7136. URL: <https://bit.mephi.ru/index.php/bit/article/view/283>. Date accessed: 10 sep. 2020. DOI: http://dx.doi.org/10.26583/bit.2017.4.09.

[11] Kirgizova A.V., Nikiforov A.Yu., Grigor'ev N.G., Polyakov I.V., Skorobogatov P.K. Dominiruyushchie mekhanizmy informacionnyh sboev KMOP KNS BIS operativnyh zapominayushchih ustrojstv pri vozdejstvii impul'snogo ioniziruyushchego izlucheniya. Mikroelektronika – 2006. T. 35, no 3. S. 191–208 (in Russian).

[12] Zinchenko V.F., Romanenko A.A., Useinov R.G., Uzhegov V.M. Radiacionnye effekty v izdeliyah poluprovodnikovoj mikroelektroniki sovremennyh tekhnologij, Voprosy atomnoj nauki i tekhniki. Seriya: Fizika radiacionnogo vozdejstviya na radioelektronnuyu apparaturu. 2016. no 1. S. 29–36. URL: https://www.elibrary.ru/item.asp?id=26131819 (accessed: 01.08.2020) (in Russian).

[13] Nikiforov A.Yu., Sogoyan A.V. Modelirovanie dozovyh effektov v parazitnyh MOP-strukturah KMOP BIS pri vozdejstvii vysokointensivnogo impul'snogo ioniziruyushchego izlucheniya. Mikroelektronika. 2004. T. 33, no 2. S. 108. URL: https://www.elibrary.ru/item.asp?id=17662355 (in Russian).

[14] Sogoyan A.V. and Polunin V.A. Modeling of recombination in SiO_2 under the effect of ionizing radiation by the Monte Carlo method, Russian Microelectronics. Vol. 40, no. 3. P. 176–184, 2011. DOI: https://doi.org/10.1134/S1063739711030061.

[15] K.I. Tapero. Effekty nizkointensivnogo oblucheniya v priborah i integral'nyh skhemah na baze kremeniya. Izvestiya vysshih uchebnyh zavedenij. Materialy elektronnoj tekhniki. 2016. T. 19, no 1. S 5–21. DOI: https://doi.org/10.17073/1609-3577-2016-1-5-21 (in Russian).

Поступила в редакцию – 26 июля 2020 г. Окончательный вариант – 26 августа 2020 г.
Received – July 26, 2020. The final version – August 26, 2020.

Рукописи, предоставляемые в редакцию, должны соответствовать следующим требованиям:

– тема статьи должна быть актуальной, иметь научное или практическое значение и публиковаться авторами впервые;

– рукопись должна быть оформлена только в формате *.doc или *.docx, полоса А4, кегль 12, шрифт TimesNewRoman, интервал одинарный;

– в начале статьи идут сведения о статье **на русском языке**: Имя О. Фамилия авторов (по центру, строчными буквами); далее сведения об авторах – должность, ученая степень, ученое звание, место работы с почтовым адресом, контактный телефон, адрес электронной почты и личный идентификатор ORCID (по центру, строчными буквами, курсив); затем название статьи (по центру, ПРОПИСНЫМИ буквами), в случае выполнения статьи в рамках НИР, гранда и пр. возможно оформление сноски на благодарность; благодарность (курсивом) - пишутся сведения об источнике финансирования; ключевые слова (не более шести, по ширине, курсив); аннотация (200 – 250 слов, по ширине, строчными буквами – см. **правила оформления аннотации**);

– далее повторяются все сведения о статье **на английском языке.**

– название статьи на английском оформляется по центру, строчными буквами, полужирно с подчеркиванием;

– затем идет текст статьи на русском или английском языке, кегль 12, интервал одинарный, рекомендуемый общий объем статьи не должен превышать 10 страниц, включая таблицы, иллюстрации; подписи под иллюстрациями на русском языке дублируются на английском языке;

– в конце статьи приводится СПИСОК ЛИТЕРАТУРЫ, в котором указан библиографический список источников литературы, оформленный в соответствии с действующими стандартами (как правило, не менее 15 наименований в научной статье и 50 – в обзорной статье);

– после списка литературы идет REFERENCES, в котором указанные библиографические данные автора(авторов) и название статьи должны быть на английском языке, исходные данные русскоязычного издания и издательства должны быть представлены в транслитерации (т.е. латинскими буквами).

Правила оформления аннотации

Аннотация является источником информации о содержании статьи и изложенных в ней результатах исследований и дает возможность установить основное содержание статьи, определить его релевантность и решить, следует ли обращаться к полному тексту статьи. Аннотация используется в информационных, в том числе автоматизированных, системах для поиска документов и информации (на английский язык переводятся: название, аннотация и ключевые слова, и по ним зарубежный читатель судит о содержании статьи).

Структура аннотации должна соответствовать структуре статьи и должна быть объемом не менее 100 слов, но не более 250 слов.

Аннотация включает следующие аспекты содержания статьи**:**

- предмет, цель статьи;
- метод или методологию проведения научной работы, описываемой в статье;
- результаты научной работы;
- область применения результатов;
- выводы.

Аннотация к статье должна быть информативной (не содержать общих слов) и оригинальной. Сведения, содержащиеся в заглавии статьи, не должны повторяться в тексте аннотации. Текст аннотации не должен содержать интерпретацию содержания статьи, критические замечания и точку зрения автора, а также информацию, которой нет в статье. Следует избегать лишних вводных фраз (например, «автор статьи рассматривает...»).

Исторические справки, если они не составляют основное содержание статьи, описание ранее опубликованных работ и общеизвестные положения в аннотации не приводятся.

В тексте аннотации следует употреблять синтаксические конструкции, свойственные языку научных и технических документов, избегать сложных грамматических конструкций.

В тексте аннотации следует применять значимые (ключевые) слова из текста статьи.

Метод или методологию проведения работы целесообразно описывать в том случае, если они отличаются новизной или представляют интерес с точки зрения данной работы. В аннотации статьи, описывающей экспериментальные работы, указывают источники данных и характер их обработки.

Результаты работы описывают предельно точно и информативно. Приводятся основные теоретические и экспериментальные результаты, фактические данные, обнаруженные взаимосвязи и закономерности. При этом отдается предпочтение новым результатам и данным долгосрочного значения,

важным открытиям, выводам, которые опровергают существующие теории, а также данным, которые, по мнению автора, имеют практическое значение.

Выводы могут сопровождаться рекомендациями, оценками, предложениями, гипотезами, описанными в статье.

Правила оформления текстов для публикации

1. Статьи необходимо подавать в электронном виде (*.doc или *.rtf) с распечаткой (или файлом в формате *.pdf) – во избежание неточностей прочтения формул.
2. Рисунки, графики, фотографии и другие виды иллюстраций следует предоставлять не только включенными в текст, но и отдельными файлами в исходном формате (не интегрированными в документ Word). Подписи под иллюстрациями делать на русском и английском языках.
3. Сокращения и аббревиатуры, которых нет в списке сокращений, необходимо раскрывать (в скобках или в сноске).
4. Давая в тексте статьи ссылки на формулы, выражения или ограничения, пожалуйста, убедитесь в том, что соответствующие объекты в статье есть и пронумерованы.
5. Ссылки на литературу следует давать в тексте в квадратных скобках, в случае цитирования – с указанием страниц.
6. При оформлении списка литературы обязательно проверить наличие и корректность выходных данных работ и исключить повторные указания одной и той же работы под разными номерами.
7. В список литературы не рекомендуется помещать источники старше 5 лет (рекомендация ВАК), а также источники, которых нет научных электронных базах (российские - это Elibrary, Ciberleninka).
8. Не надо помещать в список литературы анонимные источники - законы, нормативные акты, инструкции и пр. Их, при необходимости, помещать в постраничной ссылке или прямо по тексту.
9. Нельзя ссылаться на справочно-поисковые системы типа «Консультант» вместо ссылок на оригиналы.
10. Недопустимо в научной статье ссылаться на учебники и учебные пособия (на учебники допустимо ссылаться только в обзорных статьях).
11. Иноязычные слова, термины и фамилии, написание которых допускает варианты, просьба писать в пределах одной статьи одинаково.

Условия опубликования статьи:

– статья должна быть выслана по электронной почте, загружена самостоятельно на сайте журнала или представлена в редакцию на электронном носителе;

– редакционная коллегия журнала следует этическим нормам, принятым в международном научном сообществе, опираясь на рекомендации Комитета по этике научных публикаций, не противоречащим нормам российского законодательства в областях регулирования деятельности средств массовой информации и авторского права;

– статьи, не соответствующие установленным требованиям представления и оформления, не рассматриваются и не публикуются;

– в одном номере журнала публикуется, как правило, только одна статья автора, в том числе с соавторами;

– авторы должны предоставлять только оригинальные работы, при использовании текстовой или графической информации, полученной из работ других лиц, необходимы ссылки на соответствующие публикации или письменное разрешение автора;

– решение о публикации рукописи принимается редакционной коллегией на основании результата двойного слепого рецензирования и экспертной оценки квалифицированными специалистами в области ИБ, срок рецензирования не превышает 30 дней;

– в случае приема рукописи к публикации автор должен оперативно давать ответы на вопросы редакции, связанные с замечаниями по статье;

– в случае отказа в публикации редакционная коллегия должна предоставить автору копию рецензии и обоснование отказа в публикации;

– подача статьи в более чем в один журнал одновременно расценивается как неэтичное поведение и является неприемлемой;

– статьи публикуются бесплатно.

Заранее спасибо,
редакционная коллегия

The articles submitted to the editors must meet the following requirements:

– the topic of the article should be relevant, have scientific or practical significance and be published by the authors for the first time;

– the manuscript should be formatted only in * .doc or pdf format, A4 strip, size 12, TimesNewRoman font, one-and-a-half interval;

– in the beginning of the article there are information about the article in English: I.O. Name of authors (centered, lower case); Further information about authors - position, academic degree, academic title, place of work, contact phone number, e-mail address and personal identifier ORCID (centered, lowercase, italics); Then the title of the article (centered, lowercase, bold with underline); Keywords (no more than six, in width, italics); Annotation (8-12 lines, width, lower case);

– further information on the article is in Russian: I.O. The authors' surname (for jubilus, lower case letters); Further information about authors - position, academic degree, academic title, place of work, contact phone number, e-mail address and personal identifier ORCID (centered, lowercase, italics); Then the title of the article (centered, lowercase, bold with underline); Keywords (no more than six, in width, italics); Annotation (8-12 lines, width, lower case);

– then the text of the article is in Russian or English, size 12, interval one and a half, the recommended total volume of the article should not exceed 10 pages, including tables, illustrations;

– at the end of the article the LIST OF LITERATURE is given, in which the bibliographic list of sources of literature is indicated, drawn up in accordance with the current standards (as a rule, not less than 15 titles);

– after the list of literature is REFERENCES, in which these bibliographic sources should be written in Latin (ie Latin letters).

Rules to write a scientific abstract

Abstract is a source of information about the content of the paper and its research results. The structure of the abstract should correspond to the structure of the paper and should be not less than 100 words, but not more than 250 words.

The abstract includes the following aspects of the paper:

- subject and purpose of the paper;
- method or methodology described in the paper;
- results;
- discussion.

The abstract plays the following role:

- allows you to establish the main content of the paper, determine its relevance and decide whether to read the full text of the paper;
- provides information about the paper and eliminates the need to read the full text of the paper if the paper is of secondary interest to the reader;
- used in information systems, including automated ones, to search for documents and information (title, abstract and keywords are translated into English, and foreign readers judge the content of the paper by them).

The abstract should be informative (not contain general wordings) and original. The information contained in the title of the paper should not be repeated in the text of the abstract. The text of the abstract should not contain an interpretation of the content of the paper, criticisms and the author's point of view, as well as information that is not included in the paper. You should avoid unnecessary introductory phrases (for example, " the author is considering..."). Historical references, if they do not constitute the main content of the paper, the description of previously published works and well-known provisions are not given in the abstract.

The text of the abstract should use syntactic constructions peculiar to the language of scientific and technical documents, avoid complex grammatical structures.

The text of the abstract should use significant (key) words from the text of the paper.

The method or methodology of the work should be described if they are new or of interest from the point of view of this work. In the abstract of the paper describing the experimental work, indicate the data sources and the specific features of their processing.

The results are described very accurately and informative. The main theoretical and experimental results, actual data, discovered interrelations and regularities are presented. At the same time, preference is given to new results and data of long-term importance, important discoveries, conclusions that refute existing theories, as well as data that, in the author's opinion, have practical value.

Conclusions may be accompanied by recommendations, assessments, suggestions, hypotheses described in the paper.

Terms of publication of the article

– the article should be sent by e-mail;

– the editorial board of the journal follows the ethical standards adopted in the international scientific community, relying on the recommendations of the Ethics Committee of scientific publications that do not contradict the norms of Russian legislation in the field of regulation of the activities of the media and copyright;

– articles that do not meet the requirements for presentation and processing are not considered or published;

– in one issue of the journal, as a rule, only one author's article is published, including co-authors;

– authors should provide only original works, if text or graphic information obtained from other persons is used, references to the relevant publications or the author's written permission are necessary;

– the decision to publish the manuscript is made by the editorial board on the basis of the result of peer review and expert evaluation by qualified specialists in the field of information security;

– in the case of receipt of the manuscript for publication, the author must promptly give answers to editorial questions related to comments on the article;

– in case of refusal to publish, the editorial board should provide the author with a copy of the review and justification for refusing the publication;

– submitting an article to more than one journal is simultaneously regarded as unethical behavior and is unacceptable;

– articles are published for free.

Rules for publication of texts

1. Articles must be submitted electronically (* .doc or * .rtf) with a printout (or a file in * .pdf format) - to avoid inaccuracies in reading the formulas.
2. Pictures, graphics, photographs and other types of illustrations should, if possible, not only be included in the text, but also separate files in the original format (not integrated into the Word document).
3. Abbreviations and abbreviations, which are not on the list of abbreviations, should be disclosed (in parentheses or in a footnote).
4. By providing links to formulas, expressions or restrictions in the text of the article, please make sure that the relevant objects in the article are numbered and numbered.
5. References to the literature should be given in the text in square brackets, in the case of citations, with pages.
6. When preparing a list of literature, it is desirable to pay attention to the availability of output data of works and to avoid repeated instructions of the same work under different numbers.
7. References to laws, regulations, confessions and so on should be indicated in the prescribed form: the Law of the Russian Federation "__" of x month xxxx, No. ___. Art. ___.
8. Foreign words, terms and surnames, the spelling of which allows variants, please write within the same article the same way.

Submission Preparation Checklist

As part of the submission process, authors are required to check off their submission's compliance with all of the following items, and submissions may be returned to authors that do not adhere to these guidelines.

1. This article has not been previously published, and not submitted for review and publication in another journal (or a corresponding explanation if otherwise in the Comments to the editor).
2. File with the articles submitted in the one jf the following document format OpenOffice, Microsoft Word, RTF, or WordPerfect.
3. The full web address (URL) for links are given where it is possible.
4. The text is single-spaced; uses a font size of 12 points; to highlight use italics, not underlining (except for URL addresses); all illustrations, graphs and tables located in the appropriate places in the text, not at the end of the document.
5. The text complies with the stylistic and bibliographic the requirements described in the Guide for authors, on the "About the journal" page.
6. If you are submitting an article in a peer reviewed section of the journal then the document meets the requirements to ensure blind peer review.

Privacy Statement

The names and email addresses entered in this journal site page will be used exclusively for the purposes specified by this journal and will not be used for any other purposes or will not be given over to another individuals and organizations.

Адрес редакции: Каширское ш., 31, Москва, 115409, Россия
Тел.: +7 (495) 788 5699, тоновый режим 9216 или 8277

Editorial address: Kashirskoe shosse, 31, Moscow, 115409, Russia
Tel. +7 (495) 788 5699, tone mode set 9216 or 8277
E-mail: BIT@mephi.ru
https://bit.mephi.ru

Периодичность выхода – 4 раза в год / Periodicity – 4 times a year

Подписка на журнал
производится в почтовых отделениях связи
по каталогу «Пресса России»

Подписной индекс 29226

Цена в продаже свободная / Price selling free

Ответственный редактор И.М. Ядыкин
Технический редактор П.А. Золотухина

Подписано в печать 15.09.2020. Формат 60x84 1/8
Печ. л. 13,5. Уч.-изд. л. 13,5. Тираж 500 экз. Изд. № 002 – 3

Национальный исследовательский ядерный университет «МИФИ»
Каширское ш., 31, Москва, 115409, Россия

National Research Nuclear University MEPHI
Kashirskoe shosse, 31, Moscow, 115409, Russia

Типография ООО «ТИПОГРАФИЯ»
ул. Кантемировская, 60, Москва, 115477, Россия