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 05.13.00 – информатика, вычислительная техника и управление, по которой 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

CONTENT

Анатолий А. Малюк, Ольга Ю. Полянская
Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, г. Москва, 115409, Россия
e-mail: AAMalyuk@mephi.ru, https://orcid.org/0000-0002-5746-1508,
e-mail: OYPolyanskaya@mephi.ru, https://orcid.org/0000-0001-9867-3278

ОПЫТ РЕАЛИЗАЦИИ ПИЛОТНОГО ПРОЕКТА ЕВРОПЕЙСКОЙ СИСТЕМЫ ОПОВЕЩЕНИЯ И ОБМЕНА ИНФОРМАЦИЕЙ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ*

DOI: http://dx.doi.org/10.26583/bit.2018.1.01

Аннотация. Формирование глобального информационного общества с особой остротой ставит проблему развития культуры информационной безопасности. В Доктрине информационной безопасности Российской Федерации, принятой в декабре 2016 года, как одна из основных угроз определяется низкая осведомленность граждан в вопросах обеспечения личной информационной безопасности.

Одним из наиболее важных механизмов повышения компетентности и формирования культуры информационной безопасности, помимо массового обучения людей, являются методы пропаганды и создания «горячих линий». Они позволяют широкой общественности брать на себя инициативу в наблюдении и уведомлении о компьютерных инцидентах. Развитие подобных подходов целесообразно осуществлять с учетом накопленного сегодня международного опыта.

С этой целью в статье рассматривается европейский опыт создания системы информационно-консультативной помощи в области предупреждения угроз безопасности использования общедоступных и корпоративных информационных систем, а также ликвидации последствий проявления угроз в информационной сфере. Анализ опыта реализации пилотного проекта европейской системы оповещения и обмена информацией выявил целесообразность проектирования подобных систем на основе модели управления с четырьмя игроками, объединяющей операторов сети, производителей информации (которые являются поставщиками ИТ-продуктов или специалистами в области ИТ-безопасности), локальных информационных посредников и потребителей информации. В качестве модели информационного потока может быть выбран узел, который запускает локальный веб-портал, предоставляющий информацию для конечных пользователей, формирует новую информацию, адаптирует информацию к ограничениям различных каналов распространения и к характеристикам целевых групп конечных пользователей. Методология пилотного проекта может быть использована при проектировании и развертывании системы оповещения и обмена информацией, ориентированной на конечных пользователей нескольких регионов или стран, сотрудничающих в области информационной безопасности.

Ключевые слова: информационная безопасность, осведомленность по вопросам информационной безопасности, система оповещения и обмена информацией, культура информационной безопасности.

Для цитирования. ***МАЛЮК, Анатолий А.; ПОЛЯНСКАЯ, Ольга Ю.*** *ОПЫТ РЕАЛИЗАЦИИ ПИЛОТНОГО ПРОЕКТА ЕВРОПЕЙСКОЙ СИСТЕМЫ ОПОВЕЩЕНИЯ И ОБМЕНА ИНФОРМАЦИЕЙ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. Безопасность информационных технологий, [S.l.], v. 25, n. 1, p. 6-18, 2018. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1089>. Дата доступа: 14 feb. 2018. doi:http://dx.doi.org/10.26583/bit.2018.1.01.*

* ***Благодарности.*** Работа выполнена при финансовой поддержке РФФИ (отделение общественных и гуманитарных наук), проект № 15-03-00248: Проведение научных исследований по направлению «Формирование в обществе культуры информационной безопасности».

Anatoly A. Malyuk, Olga Y. Polyanskaya
National Nuclear Research University MEPHI (Moscow Engineering Physics Institute),
Kashirskoe shosse, 31, Moscow, 115409, Russia
e-mail: AAMalyuk@mephi.ru, https://orcid.org/0000-0002-5746-1508,
e-mail: OYPolyanskaya@mephi.ru, https://orcid.org/0000-0001-9867-3278

Experience of the pilot implementation of the european information sharing and alerting system in the field of information security*

DOI: http://dx.doi.org/10.26583/bit.2018.1.01

Abstract. The formation of a global information society poses a particular challenge to the development of an information security culture. In the Doctrine of Information Security of the Russian Federation, adopted in December 2016, one of the main threats is the low awareness of citizens in matters of ensuring personal information security.

One of the most important mechanisms for increasing competence and forming an in-formation security culture, in addition to mass training of people, are methods of propaganda and creation of "hot lines". They allow the general public to take the initiative in monitoring and reporting computer incidents. The development of such approaches should be carried out taking into account the international experience accumulated today.

To this end, the article examines the European experience of creating a system of information and advisory assistance in the field of preventing threats to the security of public and corporate information systems, primarily information and telecommunications networks, as well as eliminating the consequences of threats in the information sphere. The analysis of the experience of implementing the pilot project of the European Information Sharing and Alert System has revealed the advisability of designing such systems on the basis of a management model with four players that unites network operators, information producers (who are IT product suppliers or IT security specialists); local information intermediaries and consumers of information. As a model of the information flow, a node can be selected that runs a local web portal that provides information to end users, generates new information, adapts information to the constraints of various distribution channels, and to the characteristics of end-user target groups. The methodology of the pilot project can be used in the design and deployment of a notification and information exchange system aimed at end-users of several regions or countries cooperating in the field of information security.

Keywords: information security, information security awareness, information sharing and alerting system, culture of information security.

For citation. ***MALYUK, Anatoly A.; POLYANSKAYA, Olga Y.*** *Experience of the pilot implementation of the european information sharing and alerting system in the field of information security. IT Security (Russia), [S.l.], v. 25, n. 1, p. 6-18, 2018. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1089>. Date accessed: 14 feb. 2018. doi:http://dx.doi.org/10.26583/bit.2018.1.01.*

* ***Acknowledgements:*** This research was executed at financial support of RFBR (Department of social Sciences and Humanities), project No. 15-03-00248: Conducting research in the field of "Formation of a culture of information security"

Введение

Развитие глобального информационного общества выдвигает на передний план задачу формирования специфических общественных отношений и новых форм межличностного и корпоративного взаимодействия. Особенно это касается вопросов обеспечения личной, общественной и государственной безопасности. Новизна поставленной задачи определяется тем, что в настоящее время недостаточно научных работ по принципам формирования культуры информационной безопасности, особенно в России.

По мнению авторов многих научных статей в этой области [1-4], формирование в обществе культуры информационной безопасности предполагает, прежде всего, создание

механизмов, с помощью которых государство может повлиять на процессы развития информационного общества и перейти от декларации основных направлений политики в этой сфере к разработке конкретных программ и массовому обучению широких слоев пользователей. Среди первоочередных задач эксперты в своих работах [5-9] выделяют следующие: расширение вклада средств массовой информации в пропаганду культуры информационной безопасности, совершенствование типовых норм по обеспечению безопасности использования общедоступных и корпоративных информационных систем и информационно-телекоммуникационных сетей, реализация системы массового обучения в области культуры информационной безопасности с использованием возможностей глобальных информационно-телекоммуникационных сетей, разработка основных образовательных программ по формированию культуры информационной безопасности.

В этом перечне задач, как отмечается в ряде работ [10-15], одно из главных мест занимают вопросы создания системы информационно-консультативной помощи в области предупреждения угроз безопасности использования общедоступных и корпоративных информационных систем, в первую очередь информационно-телекоммуникационных сетей, а также ликвидации последствий проявления угроз в информационной сфере. Представляется, что основное внимание при организации такой информационно-консультативной помощи должно быть сосредоточено на ряде следующих ключевых проблем:

- создание порталов и сайтов, содействующих оказанию информационно-консультативной помощи пользователям общедоступных и корпоративных информационных систем, и информационно-телекоммуникационных сетей;
- разработка и реализация перспективных проектов негосударственных организаций, направленных на оказание информационно-консультативной помощи;
- совершенствование правовых механизмов организации широкого обмена информацией и взаимодействия на международном уровне в целях предотвращения новых угроз, приобретающих трансграничный характер;
- совершенствование взаимодействия уполномоченных государственных органов на международном уровне.

На сегодняшний день большой практический интерес представляет зарубежный (прежде всего, европейский) опыт создания такого рода систем информационно-консультативной помощи, который и является предметом дальнейшего нашего рассмотрения.

1. История вопроса (проект FISHA)

До начала 2000-х годов развитые европейские государства не были обеспокоены отсутствием у граждан знаний в области сетевой и информационной безопасности, знаний о том, что такое риски и угрозы в этой сфере и как защитить себя от них. Но, в конце концов, в странах ЕС появилось понимание, что без определенной культуры и надлежащего в смысле информационной безопасности поведения граждане и представители малых и средних предприятий, пользующиеся ИКТ-устройствами, подключенными к Интернету, представляют угрозу для критически важных информационных инфраструктур своих стран. Многие эксперты [16-20] полагают, что без определенного уровня подготовки и информированности работников по вопросам информационной безопасности невозможно обеспечить культуру безопасности в организациях. Основой для формирования культуры информационной безопасности в развитых странах стали рекомендации и аналитические материалы Организации экономического сотрудничества и развития (ОЭСР) [15, 21-23], а также документы и резолюции Европейской комиссии и Европейского Союза [24-26, 28]. В ряде документов [29-32] Европейская комиссия признала важность глобальных мер по повышению уровня информированности домашних пользователей и представителей малых и средних предприятий (МСП) по вопросам информационной безопасности и отвела в этом деле ключевую роль государствам-членам ЕС. В целях повышения европейского потенциала

реагирования на сетевые угрозы безопасности в 2006 году Комиссия в своей «Стратегии для безопасного информационного общества» предложила создать европейскую систему обмена информацией и оповещения (EISAS – European Information Sharing and Alerting System) [27].

Предполагалось, что система EISAS должна:

- способствовать совершенствованию у всех граждан ЕС, а также представителей МСП знаний и навыков, необходимых для защиты своих ИТ-систем и информационных ресурсов;
- сделать доступной информацию по безопасности для всех европейских граждан и представителей МСП на их родном языке;
- опираться на национальные возможности государств-членов ЕС;
- активизировать сотрудничество между национальными/государственными группами реагирования на компьютерные инциденты CERT в государствах-членах ЕС.

Европейская комиссия обратилась к агентству по сетевой и информационной безопасности Европейского союза ENISA с просьбой «изучить вопрос о целесообразности европейской многоязычной системы по обмену информацией и оповещения» [27]. По инициативе Европейской комиссии был начат рассчитанный на долгое время проект EISAS. Он прошел много этапов от первоначального технико-экономического обоснования в 2007 году до первого крупномасштабного пилотного проекта в 2012 году.

В соответствии с рекомендациями EISAS Roadmap [33] в 2009-2011 годах была разработана Структура для обмена информацией и оповещения FISHA (The Framework for Information Sharing and Alerting). Проект FISHA [34] начался в 2009 году с целью реализации модели EISAS. В центре внимания проекта было три основных направления:

- техническое решение для обмена информацией: P2P-сеть и сеть локальных узлов;
- политическая структура, включающая концепцию распространения информации и рекомендации по созданию устойчивой модели управления;
- план коммуникаций, включающий матрицу коммуникаций и характеристику основных целевых групп для информирования.

В настоящее время известны разные подходы и модели систем обмена информацией по информационной безопасности, описанные в ряде научных работ [35- 41]. Консорциум FISHA предложил модель управления для четырех игроков (модель FISHA) [34]:

- организации сетевой безопасности;
- производители информации;
- локальные информационные посредники (брокеры);
- потребители информации (т.е. граждане и представители МСП).

Организации сетевой безопасности занимали центральное место в этой модели, поскольку они стали бы основными сторонами, заинтересованными в запуске национальных систем оповещения и обмена информацией. К категории организаций сетевой безопасности были отнесены национальные государственные группы реагирования на компьютерные инциденты CERT, а также другие организации, занимающиеся подобной деятельностью в государствах-членах ЕС. Производители информации и информационные посредники, безусловно, считались критически важными субъектами, но выполняли лишь дополнительные функции.

Проект FISHA предложил два вида узлов для управления совместной работой этих игроков: центральный узел и несколько базовых узлов [34]. С точки зрения технического администрирования, организация сетевой безопасности, представляющая центральный узел, помимо всего прочего, должна была нести ответственность за управление сетью базовых узлов. С этой целью в проекте FISHA был разработан прототип веб-приложения (система FISHA), который был основан на технологии P2P для обмена информацией в сети. Центральный узел должен был выполнять функции интерфейса с центральными узлами в других странах. Объединенные виды деятельности, осуществляемые центральным узлом и базовыми узлами, описывались как национальная система оповещения и обмена информацией. Независимо от того являлся ли центральный узел

группой CERT, или нет, эта роль предполагала взятие на себя ответственности за работу и координацию национальной системы оповещения и обмена информацией.

Главным результатом проекта FISHA было создание прототипа веб-приложения для оповещения и обмена информацией. Проект FISHA инициировал создание сети групп информационной безопасности, среди тех национальных/государственных групп CERT, которые согласились предоставлять в стандартном формате информацию по безопасности, обычно используемую для информирования и оповещения конечных пользователей. В принципе, каждая группа CERT использует одни и те же источники информации и подписывается на одни и те же списки рассылки и RSS-каналы для того, чтобы следить за инцидентами безопасности в Интернете в целом. Эти виды деятельности предполагалось разделить между несколькими группами CERT, и таким образом достичь синергетического эффекта. В результате проекта была создана модель прототипа системы, согласно которой группы CERT разделяют эти "объекты информации" и публикуют их на родных языках целевой аудитории – граждан и малого и среднего бизнеса.

Проект FISHA стартовал с деятельности EISAS по сбору, обработке (консолидации и форматированию) и распространению информации (предоставлению информации) в рамках процесса передачи информации, имеющей отношение к безопасности, по сети от источника до конечного пользователя. Ряд экспертов отметили, что система FISHA потенциально может быть очень полезной, если используется для «совместного анализа» информации [34]. Проект FISHA был завершен в 2011 году, доказав правильность концепции. Он предложил совместную техническую платформу для обеспечения эффективного обмена и распространения информации по повышению осведомленности граждан и предприятий малого и среднего бизнеса. В качестве пилотного проекта EISAS система FISHA обеспечивала технические средства для распространения информации по информационной безопасности среди производителей и потребителей информации. Это позволило участникам структуры:

- создать общую базу данных имеющихся материалов для повышения осведомленности по вопросам информационной безопасности;
- просматривать информацию в этой базе данных;
- уведомлять друг друга о недавно появившихся материалах;
- обмениваться общедоступными материалами и участвовать в их создании;
- предоставлять локальным информационным посредникам доступ к локально адаптированным материалам.

ENISA представила план системы EISAS, согласно которому основные функциональные возможности и услуги EISAS должны были быть разработаны и внедрены в виде регионального прототипа EISAS Basic Toolset в 2011 году [42]. Затем этот прототип должен был быть распространен на более крупные сообщества в 2012 году в рамках крупномасштабного пилотного проекта европейской системы обмена информацией и оповещения.

В 2011 году агентство ENISA развило подход EISAS в экспериментальном проекте по повышению информационной осведомленности граждан и предприятий малого и среднего бизнеса в рамках одного государства-члена ЕС. Слабая подготовка и информированность этих целевых групп по вопросам информационной безопасности признается многими авторами [43-47] серьезной угрозой для критически важных информационных инфраструктур многих стран. EISAS Basic Toolset разрабатывался как методология, облегчающая информирование целевых групп EISAS об информационной безопасности и расширяющая их возможности за счет предоставления необходимых средств защиты их компьютеров и информационных активов и помощи в овладении необходимыми навыками [42]. Предполагалось связываться с целевыми группами граждан через предприятия, на которых они работали, и распространять среди них:

- оповещения и предупреждения;
- рекомендации;
- передовые практики и информационно-пропагандистские материалы, в виде

листовок, видео, мультфильмов и т.д.

Технико-экономическое исследование развертывания системы EISAS показало, что, используя подход EISAS Basic Toolset, можно значительно повысить информационную безопасность конечных пользователей и их компьютерного оборудования в домашних условиях [48]. Ключевыми факторами успеха стали информирование конечных пользователей об информационной безопасности в соответствии с их потребностями и пониманием, а также предоставление им структуры поддержки для оказания оперативной помощи в случае необходимости.

2. Реализация основных принципов информирования пользователей

Упомянутый выше подход Basic Toolset определил основу более крупного экспериментального развертывания с участием нескольких государств-членов, которое было осуществлено в виде крупномасштабного пилотного проекта EISAS Large-Scale Pilot, реализованного в 2012 году (это было определено в плане EISAS Roadmap [49]). Крупномасштабный пилотный проект развертывания был сосредоточен на двух основных аспектах: сотрудничестве между соответствующими ключевыми игроками, а также совместной обработке и распространении информации (см. рис. 1). В рамках пилотного проекта EISAS национальные правительственные группы реагирования на компьютерные инциденты CERT и другие подобные сообщества в Германии, Венгрии, Португалии, Норвегии, Испании и Польше объединили усилия с целью повышения информированности домашних пользователей и представителей МСП по вопросам информационной безопасности.

Рис. 1. Роли и виды деятельности участников пилотного проекта
(Fig. 1. Roles and activities of participants in the pilot project)

Провайдерами информации были:

- немецкая компания Deutsche Telekom AG (DTAG);
- норвежский центр информационной безопасности NorSIS, государственный орган Норвегии.

В число распространителей информации входили:

- агентство правительства Каталонии, отвечающее за обеспечение безопасности информационно-коммуникационных технологий (ИКТ) CESICAT. (CESICAT также действует как центр реагирования на компьютерные инциденты CERT для каталонского малого и среднего бизнеса, граждан, университетов и органов государственного управления);

- венгерский центр реагирования на компьютерные инциденты CERT Hungary (Biztonsagosinternet hotline);
- польский центр реагирования на компьютерные инциденты CERT Polska;
- одна из крупнейших финансовых организаций Испании la Caixa.

Инновационные информационные материалы были получены от основных участников пилотного проекта. Была создана международная команда для совместной обработки и адаптации материалов к потребностям и особенностям населения каждой из стран-участниц. При поиске и отборе информационных материалов учитывался характер представления материала, поскольку это влияет на его привлекательность для целевой группы населения. Для распространения использовалась высококачественная, предварительно сформированная информация, которая касалась безопасного Интернет-серфинга и ботнетов (веб-справочник), кражи личных данных и фишинга (обучающая викторина), а также и социальной инженерии (интерактивное видео). Все эти материалы распространялись по соответствующим каналам связи (социальные сети, крупные общедоступные веб-сайты, специализированные списки рассылки и т.п.), предназначенным для граждан и представителей малого и среднего бизнеса ЕС.

3. Взаимодействие с участниками информационного общества

Очевидно, что особые условия крупного международного совместного проекта, основанного на добровольной работе разных участников, создавали значительные трудности в управлении проектом (см. табл.1) [50]. Трудности возникали из-за проблем с нахождением «общего языка» (с учетом культуры, часовых поясов, местного контекста, языка общения), а также с координацией групповой работы, мотивацией сотрудников и их готовностью к совместной работе.

Таблица 1. Характеристики взаимодействия участников проекта EISAS Large-Scale Pilot
Table 1. Characteristics of interaction between EISAS Large-Scale Pilot project participants

Влияющие факторы	Количество	Содержание факторов
Страны	6	Дания (2), Германия (11), Греция (2), Венгрия (3), Норвегия (2), Польша (2), Испания и Каталония (3)
Языки	8	каталонский, французский, датский, немецкий, венгерский, норвежский, польский, испанский
Временные зоны	3	GMT+0, GMT+1, GMT+2
Координация групповой работы	Тесная	Планирование выполнения технической настройки, строгое соблюдение последовательности задач (например, программирование выполнялось только после завершения перевода текстов, распространение материалов начиналось только после безошибочного выполнения технической настройки)
Готовность участников к сотрудничеству	Средняя	Отношение к дистанционной коммуникации как к рабочим совещаниям; быстрое установление доверительных отношений
Готовность участников использовать современные технологии для совместной работы	Средняя	Применение традиционных средств коммуникации: электронной почты, конференцсвязи Skype. Платформа управления проектами Web 2.0 использовалась только двумя участниками.

Выводы

Подводя итог, можно констатировать, что на основе трансграничного сотрудничества и государственно-частного партнерства была достигнута цель пилотного проекта EISAS Large-Scale Pilot: шесть различных субъектов в четырех государствах-членах ЕС сотрудничали на постоянной основе в рамках совместной информационно-просветительской кампании. Крупномасштабный пилотный проект работал в течение относительно короткого времени, тем не менее, он позволил выявить ряд факторов, которые необходимо принимать во внимание при развертывании межгосударственной системы обмена информацией и оповещения по вопросам информационной безопасности [50].

Важным фактором в концепции EISAS является наличие материалов по информационной безопасности, которые могут быть использованы для информирования целевых групп. Проект EISAS Large-Scale Pilot ясно продемонстрировал, что участники, готовые предоставить информацию, должны быть поддержаны некоторой структурой центрального управления – информационным посредником, который берет на себя задачу обработки информации после ее получения от поставщика и до ее передачи распространителю, выполняя следующие функции:

- помогает производителям оригинальной информации рекомендациями по поводу создания материалов, распространяемых на международном уровне;
- создает систему стимулов для производителей оригинальной информации, побуждающих их стать поставщиками информации (например, поощряющих государственно-частное партнерство);
- объединяет вместе в команды (группы) партнеров, предоставляющих и распространяющих информацию;
- оказывает услуги по профессиональному переводу и локализации материалов, по решению технических проблем;
- сохраняет передовой опыт, с тем, чтобы со временем отпала необходимость в информационном посреднике.

С учетом затрат времени и усилий участников пилотный проект показал, что координация и посредническая деятельность по обмену информацией между субъектами проекта являются решающими – более 80% работ, необходимых для осуществления EISAS в этом проекте было выполнено информационным посредником [50]. Кроме того, несмотря на то, что трудно было найти высококачественные материалы, пригодные для совместного распространения, именно они являются необходимым условием мотивирования распространителей информации, для того чтобы они взяли на себя необходимую нагрузку по получению материала в Интернете.

Наибольший удельный вес работ пришелся на задачи управления проектом. Управление проектом здесь заключалось не просто в ежедневных административных усилиях по реализации проекта в сжатые сроки, а в поддержании мотивации участников продолжать совместную работу на расстоянии и их убеждении, что стоит идти дальше.

Результаты пилотного проекта свидетельствовали о том, что жизненно важным вопросом в существовании сети EISAS являются устойчивые модели финансирования. Самая большая проблема сотрудничества заключалась в балансе эксплуатационных расходов и стоимости участия в сети. Проект подтвердил, что функционирование EISAS не может быть основано на добровольном участии, особенно тех заинтересованных сторон, основной вид деятельности которых не связан с безопасностью ИКТ. Основным стимулом для участников является предоставление финансовой поддержки. Достаточно высокими оказались расходы на программирование, адаптацию и локализацию информационных материалов [50]. Наиболее затратной по времени активностью в цикле производства информации EISAS была названа обработка имеющейся информации, то есть процесс ее классификации и длительного перевода на европейские языки. Успех EISAS зависит от качества информации, которой обмениваются участники и которая распространяется по целевым группам. Этот показатель должен быть достаточно

высоким, чтобы обеспечить стимулы для участия. Наиболее важным итогом пилотного проекта стало подтверждение того, что система EISAS осуществима в больших масштабах и может быть рекомендована для внедрения по всей Европе.

Результаты этого пилотного проекта свидетельствуют о том, что подход EISAS к европейскому сотрудничеству в области повышения осведомленности в вопросах обеспечения информационной безопасности (и не только, но и в более широком аспекте формирования информационного общества) работает и предлагает экономически эффективное решение для совершенствования знаний и навыков граждан ЕС в условиях постоянно нарастающих киберугроз.

СПИСОК ЛИТЕРАТУРЫ:

1 Малюк А.А., Литинская Л.В., Коваленко С.Ю. Формирование информационной культуры общества – важнейший фактор обеспечения информационной безопасности «Безопасность информационных технологий», вып.4, 2009. сс. 17-24.
2 Ghernouti-Hélie. A National Strategy for an Effective Cybersecurity Approach and Culture. 2010 International Conference on Availability, Reliability and Security, 2010, pp. 370 – 373.
3 Mahfuth Amjad, Yussof Salman, Baker Asmidar Abu, Nor'ashikin Ali. A systematic literature review: Information security culture. 2017 International Conference on Research and Innovation in Information Systems (ICRIIS), 2017, pp.1–6.
4 Martins, A. and Eloff, J. 'Information Security Culture' IFIP TC11 International Conference on Information Security, Cairo, Egypt, 7- 9 May 2002.
5 Малюк, А. А.; Полянская, О. Ю. Зарубежный опыт формирования в обществе культуры информационной безопасности. Безопасность информационных технологий, [S.l.], v. 23, n. 4, p. 25-37, dec. 2016. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/8>. Дата доступа: 12 dec. 2017.
6 Малюк А.А., Полянская О.Ю. Формирование современной культуры информационной безопасности «Инфофорум», журнал «Бизнес и Безопасность в России», октябрь, 2008.
7 Schlienger, T. and S. Teufel 'Analysing Information Security Culture: Increased Trust by an Appropriate Information Security Culture' 14th International Conference on Database and Expert Systems Applications (DEXA 2003), Prague, Czech Republic, September 2003.
8 Schlienger, T. and S. Teufel 'Information Security Culture - From Analysis to Change.' Proceedings of ISSA 2003, Johannesburg, South Africa, 9-11 July 2003.
9 Schlienger, T. and S. Teufel. 'Information Security Culture - The Socio-Cultural Dimension in Information Security Management.' IFIP TC11 International Conference on Information Security, Cairo, Egypt, 7-9 May 2002
10 Alain Esterle, Hanno Ranck, and Burkard Schmitt (edited by Burkard Schmitt). "Information security. A new challenge for the EU". Chaillot Paper no. 76, 2005. [Электронный ресурс] URL: http://www.iss.europa.eu/uploads/media/cp076 .pdf.
11 Popp Robert; Poindexter John. Countering Terrorism through Information and Privacy Protection Technologies. IEEE Security & Privacy. 2006, Volume 4, Issue 6, pp. 18-27.
12 Ryan J. J. C. H. Information security tools and practices: what works? IEEE Transactions on Computers, 2004, Volume: 53, Issue: 8, pp. 1060 – 1063.
13 Schjolberg S., Ghernaouti-Hélie S. A Global Treaty on Cybersecurity and Cybercrime, Second edition, 2011. [Электронный ресурс] URL: http://www.cybercrimelaw.net/documents/.
14 Talib Shuhaili; Clarke Nathan L.; Furnell Steven M. An Analysis of Information Security Awareness within Home and Work Environments. 2010 International Conference on Availability, Reliability and Security, 2010, pp.196-203.
15 The promotion of a culture of security for information systems and networks in OECD countries. [Электронный ресурс] URL: http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/REG(2005)1/FINAL&docLanguage=En.
16 AlHogail Areej, Mirza Abdulrahman. Information security culture: A definition and a literature review. 2014 World Congress on Computer Applications and Information Systems (WCCAIS), 2014, IEEE, pp.1-7.
17 Ngo L. Zhou, W. Warren, M. Understanding transition towards organizational culture change. Proceedings of the 3rd Australian Information Security Management Conference, Perth Australia, 2005.
18 Ruighaver, A.B. & Maynard, S. Organizational Security Culture: More Than Just an End-User Phenomenon. Proceedings of the 21st IFIP TC-11 International Information Security Conference (IFIP/SEC 2006). May 22, 2006, Karlstad, Sweden, pages 425-430.
19 Ruighaver, A.B., Maynard, S. & S. Chang (2006) Organizational Security Culture: Extending the End-User Perspective. Computers & Security, Volume 26, Issue 1, February 2007, Pages 56-62.
20 Sunthoshan Govender; Elmarie Kritzinger; Marianne Loock. The influence of national culture on information security culture.2016 IST-Africa Week Conference, Year: 2016, pp. 1–9.
21 Cybersecurity policy making at a turning point. Analysing a new generation of national cybersecurity strategies

for the Internet Economy. [Электронный ресурс] URL: http://www.oecd.org/officialdocuments/.
22 OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. [Электронный ресурс] URL: http://www.ftc.gov/bcp/conline/edcams/infosecurity/popups/OECD_guidelines.pdf
23 Summary of responses to the survey on the implementation of the OECD guidelines for the security of information systems and networks: towards a culture of security. [Электронный ресурс] URL: http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/REG(2003)8/FINAL&docLanguage=En.
24 Commission of the European Communities "Commission Decision of 22 April 2005 establishing the European Research Advisory" Official Journal of the European Union. Board (2005/516/EC), 2005.
25 Commission of the European Communities. "Critical Infrastructure Protection in the Fight against Terrorism" (COM(2004)702). 2004, [Электронный ресурс] Сайт Европейской комиссии. URL: http://europa.eu.int/comm/justice_home/doc_centre/criminal/terrorism/doc/com_2004_702_en.pdf.
26 Commission of the European Communities. "Green Paper on a European Programme for Critical Infrastructure Protection" (COM(2005) 576), 2005. [Электронный ресурс] Сайт Европейской комиссии. URL: http://www.libertysecurity.org/IMG/pdf/EC_-_Green_Paper_on_CI_-_17.11.2005.pdf.
27 Communication: A strategy for a Secure Information Society. 31.05.2006. [Электронный ресурс] Сайт Европейской комиссии. URL: http://ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=2766 .
28 Council Resolution of 22 March 2007 on a Strategy for a Secure Information Society in Europe. Council of the European Union, Official Journal of the European Union. (C68 /01), 2007. [Электронный ресурс] Сайт Европейского Союза. URL: http://eur-lex.europa.eu/LexUriServ/site/en/oj/2007/c_068/c_06820070324en00010004.pdf.
29 European Commission Information Society. "Availability and Robustness of Electronic Communication Infrastructures (ARECI) Study". [Электронный ресурс] URL: http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/areci_study/index_en.htm .
30 European Commission Justice and Home Affairs. "Freedom, Security and Justice; Protect Infrastructures". [Электронный ресурс] URL: http://ec.europa.eu/justice_home/fsj/terrorism/protection/fsj_terrorism_protection_infrastruct_en.htm.
31 Proposal for a Directive of the Council on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection. European Commission Justice and Home Affairs. 2006. [Электронный ресурс] URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52006PC0787 :EN:NOT.
32 Network and Information Security: Commission seeks to improve network and information security in Europe. 31.05.2006. [Electronic resource] European Commission. URL: http://ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=2679.
33 EISAS Roadmap, ENISA, 2011. [Электронный ресурс] Сайт Агентства по сетевой и информационной безопасности Европейского союза (ENISA). URL: https://www.enisa.europa.eu/act/cert/other-work/eisas_folder/eisas_roadmap .
34 FISHA project, [Электронный ресурс] Сайт проекта по созданию структуры для обмена информацией и оповещения FISHA (The Framework for Information Sharing and Alerting). URL: http://fisha-project.eu /.
35 Dandurand Luc, Serrano Oscar . Towards improved cyber security information sharing. 2013 5th International Conference on Cyber Conflict (CYCON 2013), IEEE Conference Publications, 2013, pp.1-16.
36 Desourdis Robert I., Contestabile John M. Information sharing for situational understanding and command coordination in emergency management and disaster response. 2011 IEEE International Conference on Technologies for Homeland Security(HST), 2011, pp. 26 – 32.
37 Do Hoang Giang, Ng Wee Keong . Privacy-preserving approach for sharing and processing intrusion alert data. 2015 IEEE Tenth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP). 2015, pp.1-6.
38 Feledi Danie, Fenz Stefan. Challenges of Web-Based Information Security Knowledge Sharing. 2012 Seventh International Conference on Availability, Reliability and Security, 2012, pp.514-521.
39 Holgado Pilar; López de Vergara Jorge E.; Villagrá Víctor A.; Sanz Iván; Amaya Antonio. Sharing information about security alerts using semantic web technologies. 2010 International Conference on Network and Service Management, 2010, pp. 270-273.
40 Ivanc Blaž ; Blažič Borka Jerman. Information Security Aspects of the Public Safety Data Interoperability Network. 2016 European Intelligence and Security Informatics Conference (EISIC), 2016, pp. 88–91.
41 Kokkonen Tero ; Hautamäki Jari, Siltanen Jarmo, Hämäläinen Timo. Model for sharing the information of cyber security situation awareness between organizations. 23rd International Conference on Telecommunications (ICT), 2016, IEEE Conference Publications, pp. 1-5.
42 EISAS Basic Toolset report, ENISA, 2011. [Электронный ресурс] Сайт Агентства по сетевой и информационной безопасности Европейского союза (ENISA). URL: https://www.enisa.europa.eu/publications/eisas-basic-toolset.
43 Bishop M. Education in information security. IEEE Concurrency.2000, Volume 8, Issue 4, pp.4-8.
44 Chia, P. Maynard, S., and Ruighaver, A.B. 'Exploring Organisational Security Culture' Sixth Pacific Asia

Conference on Information Systems, Tokyo, Japan, 2-3 September, 2002.
45 Chia, P. Maynard, S., and Ruighaver, A.B. 'Understanding Organisational Security Culture' in Information Systems: The Challenges of Theory and Practice, Hunter, M. G. and Dhanda, K. K. (eds), Information Institute, Las Vegas, USA, 2003, pp. 335 - 365.
46 Dojkovski, S., Lichtenstein, S and Warren, M. Information Security Culture in Small and Medium Sized Enterprises: A Socio-Cultural Framework, Proceedings of 6th Australian Information Warfare & Security Conference, School of Information Systems, Deakin University, Geelong, Australia, 2005.
47 Dojkovski, S., Lichtenstein, S. and Warren, M. Challenges in Fostering an Information Security Culture in Australian Small and Medium Sized Enterprises, Proceedings of the 5th European Conference on Information Warfare and Security, Academic Conference Limited, United Kingdom, 2006.
48 EISAS Deployment Feasibility Study ENISA, 2013. [Электронный ресурс] Сайт Агентства по сетевой и информационной безопасности Европейского союза (ENISA). URL: http://www.enisa.europa.eu/publications/eisas-deployment-feasibility-study.
49 Network and Information Security: Commission seeks to improve network and information security in Europe. 31.05.2006. [Электронный ресурс] European Commission. URL: http://ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=2679.
50 EISAS Large-Scale Pilot, Collaborative Awareness Raising for EU Citizens & SMEs ENISA, 2012. [Электронный ресурс] Сайт Агентства по сетевой и информационной безопасности Европейского союза (ENISA). URL: https://www.enisa.europa.eu/.../eisas-large-scale-pilot.

REFERENCES:

[1] Malyuk A.A., Litinskaya L.V., Kovalenko S.Yu. The information culture formation of the society is the most important factor of information security. Bezopasnost' informacionnyh tehnologij (IT Security). ISSN 2074-7128, №.4, 2009, pp. 17-24. (in Russian).
[2] Ghernouti-Hélie. A National Strategy for an Effective Cybersecurity Approach and Culture. 2010 International Conference on Availability, Reliability and Security, 2010, pp. 370 – 373.
[3] Mahfuth Amjad, Yussof Salman, Baker Asmidar Abu, Nor'ashikin Ali. A systematic literature review: Information security culture. 2017 International Conference on Research and Innovation in Information Systems (ICRIIS), 2017, pp.1–6.
[4] Martins, A. and Eloff, J. 'Information Security Culture' IFIP TC11 International Conference on Information Security, Cairo, Egypt, 7- 9 May 2002.
[5] Malyuk, A. A.; Polyanskaya, O. Y.. Foreign experience of the formation of information security culture in society. IT Security (Russia), [S.l.], v. 23, n. 4, p. 25-37, dec. 2016. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/8>. Date accessed: 22 dec. 2017. (in Russian).
[6] Malyuk AA, Polyanskaya O.Yu. Forming a modern culture of information security / «Infoforum», «Biznes i Bezopasnost' v Rossii», October, 2008 (in Russian).
[7] Schlienger, T. and S. Teufel 'Analysing Information Security Culture: Increased Trust by an Appropriate Information Security Culture' 14th International Conference on Database and Expert Systems Applications (DEXA 2003), Prague, Czech Republic, September 2003.
[8] Schlienger, T. and S. Teufel 'Information Security Culture - From Analysis to Change.' Proceedings of ISSA 2003, Johannesburg, South Africa, 9-11 July 2003.
[9] Schlienger, T. and S. Teufel. 'Information Security Culture - The Socio-Cultural Dimension in Information Security Management.' IFIP TC11 International Conference on Information Security, Cairo, Egypt, 7-9 May 2002
[10] Alain Esterle, Hanno Ranck, and Burkard Schmitt (edited by Burkard Schmitt). "Information security. A new challenge for the EU". Chaillot Paper no. 76, 2005. [Electronic resource] URL: http://www.iss.europa.eu/uploads/media/cp076 .pdf.
[11] Popp Robert; Poindexter John. Countering Terrorism through Information and Privacy Protection Technologies. IEEE Security & Privacy. 2006, Volume 4, Issue 6, pp. 18-27.
[12] Ryan J. J. C. H. Information security tools and practices: what works? IEEE Transactions on Computers, 2004, Volume: 53, Issue: 8, pp. 1060 – 1063.
[13] Schjolberg S., Ghernaouti-Hélie S. A Global Treaty on Cybersecurity and Cybercrime, Second edition, 2011. [Electronic resource] URL: http://www.cybercrimelaw.net/documents/.
[14] Talib Shuhaili; Clarke Nathan L.; Furnell Steven M. An Analysis of Information Security Awareness within Home and Work Environments. 2010 International Conference on Availability, Reliability and Security, 2010, pp.196-203.
[15] The promotion of a culture of security for information systems and networks in OECD countries. [Electronic resource] URL: http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/REG(2005)1/FINAL&docLanguage=En.
[16] AlHogail Areej, Mirza Abdulrahman. Information security culture: A definition and a literature review. 2014 World Congress on Computer Applications and Information Systems (WCCAIS), 2014, IEEE, pp.1-7.
[17] Ngo L. Zhou, W. Warren, M. Understanding transition towards organizational culture change. Proceedings of the 3rd Australian Information Security Management Conference, Perth Australia, 2005.

[18] Ruighaver, A.B. & Maynard, S. Organizational Security Culture: More Than Just an End-User Phenomenon. Proceedings of the 21st IFIP TC-11 International Information Security Conference (IFIP/SEC 2006). May 22, 2006, Karlstad, Sweden, pp. 425-430.
[19] Ruighaver, A.B., Maynard, S. & S. Chang (2006) Organizational Security Culture: Extending the End-User Perspective. Computers & Security, Volume 26, Issue 1, February 2007, pp. 56-62.
[20] Sunthoshan Govender; Elmarie Kritzinger; Marianne Loock. The influence of national culture on information security culture.2016 IST-Africa Week Conference, Year: 2016, pp. 1–9.
[21] Cybersecurity policy making at a turning point. Analysing a new generation of national cybersecurity strategies for the Internet Economy. [Electronic resource] URL: http://www.oecd.org/officialdocuments/.
[22] OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. [Electronic resource] URL: http://www.ftc.gov/bcp/conline/edcams/infosecurity/popups/OECD_guidelines.pdf.
[23] Summary of responses to the survey on the implementation of the OECD guidelines for the security of information systems and networks: towards a culture of security. [Electronic resource] URL: http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/REG(2003)8/FINAL&docLanguage=En.
[24] Commission of the European Communities “Commission Decision of 22 April 2005 establishing the European Research Advisory” Official Journal of the European Union. Board (2005/516/EC), 2005.
[25] Commission of the European Communities. “Critical Infrastructure Protection in the Fight against Terrorism” (COM(2004)702). 2004, [Electronic resource] European Commission. URL: http://europa.eu.int/comm/justice_home/doc_centre/criminal/terrorism/doc/com_2004_702_en.pdf.
[26] Commission of the European Communities. “Green Paper on a European Programme for Critical Infrastructure Protection” (COM(2005) 576), 2005. [Electronic resource] European Commission. URL: http://www.libertysecurity.org/IMG/pdf/EC_-_Green_Paper_on_CI_-_17.11.2005.pdf.
[27] Communication: A strategy for a Secure Information Society. 31.05.2006. [Electronic resource] European Commission. URL: http://ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=2766 .
[28] Council Resolution of 22 March 2007 on a Strategy for a Secure Information Society in Europe. Council of the European Union, Official Journal of the European Union. (C68 /01), 2007. [Electronic resource] EUR-Lex. Access to European Union law. URL: http://eur-lex.europa.eu/LexUriServ/site/en/oj/2007/c_068/c_06820070324en00010004.pdf.
[29] European Commission Information Society. “Availability and Robustness of Electronic Communication Infrastructures (ARECI) Study”. [Electronic resource] URL: http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/areci_study/index_en.htm .
[30] European Commission Justice and Home Affairs. “Freedom, Security and Justice; Protect Infrastructures”. [Electronic resource] URL: http://ec.europa.eu/justice_home/fsj/terrorism/protection/fsj_terrorism_protection_infrastruct_en.htm.
[31] Proposal for a Directive of the Council on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection. European Commission Justice and Home Affairs. 2006. [Electronic resource] URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52006PC0787 :EN:NOT.
[32] Network and Information Security: Commission seeks to improve network and information security in Europe. 31.05.2006. [Electronic resource] European Commission. URL: http://ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=2679.
[33] EISAS Roadmap, ENISA, 2011. [Electronic resource] The European Union Agency for Network and Information Security (ENISA). URL: https://www.enisa.europa.eu/act/cert/other-work/eisas_folder/eisas_roadmap.
[34] FISHA project, [Electronic resource] The Framework for Information Sharing and Alerting (FISHA). URL: http://fisha-project.eu /.
[35] Dandurand Luc, Serrano Oscar . Towards improved cyber security information sharing. 2013 5th International Conference on Cyber Conflict (CYCON 2013), IEEE Conference Publications, 2013, pp.1-16.
[36] Desourdis Robert I., Contestabile John M. Information sharing for situational understanding and command coordination in emergency management and disaster response. 2011 IEEE International Conference on Technologies for Homeland Security(HST), 2011, pp. 26 – 32.
[37] Do Hoang Giang, Ng Wee Keong . Privacy-preserving approach for sharing and processing intrusion alert data. 2015 IEEE Tenth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP). 2015, pp.1-6.
[38] Feledi Danie, Fenz Stefan. Challenges of Web-Based Information Security Knowledge Sharing. 2012 Seventh International Conference on Availability, Reliability and Security, 2012, pp.514-521.
[39] Holgado Pilar; López de Vergara Jorge E.; Villagrá Víctor A.; Sanz Iván; Amaya Antonio. Sharing information about security alerts using semantic web technologies. 2010 International Conference on Network and Service Management, 2010, pp. 270-273.
[40] Ivanc Blaž ; Blažič Borka Jerman. Information Security Aspects of the Public Safety Data Interoperability Network. 2016 European Intelligence and Security Informatics Conference (EISIC), 2016, pp. 88–91.
[41] Kokkonen Tero ; Hautamäki Jari, Siltanen Jarmo, Hämäläinen Timo. Model for sharing the information of

cyber security situation awareness between organizations. 23rd International Conference on Telecommunications (ICT), 2016, IEEE Conference Publications, pp. 1-5.

[42] EISAS Basic Toolset report, ENISA, 2011. [Electronic resource] The European Union Agency for Network and Information Security (ENISA). URL: https://www.enisa.europa.eu/publications/eisas-basic-toolset.

[43] Bishop M. Education in information security. IEEE Concurrency.2000, Volume 8, Issue 4, pp.4-8.

[44] Chia, P. Maynard, S., and Ruighaver, A.B. 'Exploring Organisational Security Culture' Sixth Pacific Asia Conference on Information Systems, Tokyo, Japan, 2-3 September 2002.

[45] Chia, P. Maynard, S., and Ruighaver, A.B. 'Understanding Organisational Security Culture' in Information Systems: The Challenges of Theory and Practice, Hunter, M. G. and Dhanda, K. K. (eds), Information Institute, Las Vegas, USA, 2003, pp. 335 - 365.

[46] Dojkovski, S., Lichtenstein, S and Warren, M. Information Security Culture in Small and Medium Sized Enterprises: A Socio-Cultural Framework, Proceedings of 6th Australian Information Warfare & Security Conference, School of Information Systems, Deakin University, Geelong, Australia, 2005.

[47] Dojkovski, S., Lichtenstein, S. and Warren, M. Challenges in Fostering an Information Security Culture in Australian Small and Medium Sized Enterprises, Proceedings of the 5th European Conference on Information Warfare and Security, Academic Conference Limited, United Kingdom, 2006.

[48] EISAS Deployment Feasibility Study ENISA, 2013. [Electronic resource] The European Union Agency for Network and Information Security (ENISA). URL: http://www.enisa.europa.eu/publications/eisas-deployment-feasibility-study.

[49] Network and Information Security: Commission seeks to improve network and information security in Europe. 31.05.2006. [Электронный ресурс] European Commission. URL: http://ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=2679.

[50] EISAS Large-Scale Pilot, Collaborative Awareness Raising for EU Citizens & SMEs ENISA, 2012. [Electronic resource] The European Union Agency for Network and Information Security (ENISA). URL: https://www.enisa.europa.eu/.../eisas-large-scale-pilot.

Поступила в редакцию – 10 декабря 2017 г. Окончательный вариант – 05 февраля 2018 г.
Received – December 10, 2017. The final version – February 05, 2018.

Jean Y. Astier[1], Igor Y. Zhukov[2], Oleg N. Murashov[3], Alexey P. Bardin[3]
[1]*HyperPanel Lab,*
Saclay 4 Rue Rene Razel Building'azur 91400 Saclay, France
e-mail: jean-yves.astier@hyperpanel.fr, https://orcid.org/0000-0002-7002-1195
[2]*CEO of Ltd. «The National Mobile Portal»,*
Volgogradskiy pr.,2 off.36, Moscow, 109316, Russia
e-mail: i.zhukov@inbox.ru, https://orcid.org/0000-0002-4429-8799
[3]*Joint-stock company «Ramec-VS»,*
Volgogradskiy pr., 2, Moscow, 109316, Russia
e-mail: olegxozbox@yandex.ru, https://orcid.org/0000-0002-4467-2170
e-mail: lovvi@mail.ru, https://orcid.org/0000-0001-8029-6902

A NEW OS ARCHITECTURE FOR IOT

DOI: http://dx.doi.org/10.26583/bit.2018.1.02

Abstract. Current computer operating systems architectures are not well suited for the coming world of connected objects, known as the Internet of Things (IoT) for multiple reasons: poor communication performances in both point-to-point and broadcast cases, poor operational reliability and network security, excessive requirements both in terms of processor power and memory size leading to excessive electrical power consumption. We introduce a new computer operating system architecture well adapted to IoT, from the most modest to the most complex, and more generally able to significantly raise the input/output capacities of any communicating computer. This architecture rests on the principles of the Von Neumann hardware model, and is composed of two types of asymmetric distributed containers, which communicate by message passing. We describe the sub-systems of both of these types of containers, where each sub-system has its own scheduler, and a dedicated execution level.

Keywords: Internet of Things (IoT), architectures, operating systems.
For citation. ***ASTIER, Jean Y. et al.*** *A NEW OS ARCHITECTURE FOR IOT. IT Security (Russia), [S.l.], v. 25, n. 1, p. 19-33, 2018. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1090>. Date accessed: 14 feb. 2018. http://dx.doi.org/10.26583/bit.2018.1.02.*

What is the Architecture of an Operating System?

There are a number of general theories on “systems”, each giving its own definition of what a “system” is. We will be using the simple definition stating that: a “system” is a “set of entities talking through interfaces (and according to protocols)". We will consider here, that in the case of a computer operating system, what are respectively called “entities” and “interfaces” in that definition are what are usually called “sub-systems” and “APIs” in computer speak. What we will be calling “architecture” is a description of these sub-systems and of their APIs. The description of a sub-system will be that of its scheduler, of the scheduler's modes of context switching, of its performance, but also of the services provided by the sub-system. The interfaces between the different sub-systems will be “procedural” or using “message passing” (Fig.1).

Why introduce a new architecture?

The architecture of the Multics system was among the most ambitious computer operating system architectures. Its definition started in 1964, and it can be considered to have finished in 1972, the year of the publication of an article titled *Multics – the first seven years* (we are leaving out the implementation of the system, which went on after the article was published). The following sentence comes from the article's conclusions [1]:

In closing, perhaps we should take note that in the seven years since Multics was proposed, a great many other systems have also been proposed and constructed; many of these have developed similar ideas. In most cases, their designers have developed effective implementations which are directed to a different interpretation of the goals, or to a smaller set of goals than those required for the complete computer utility.

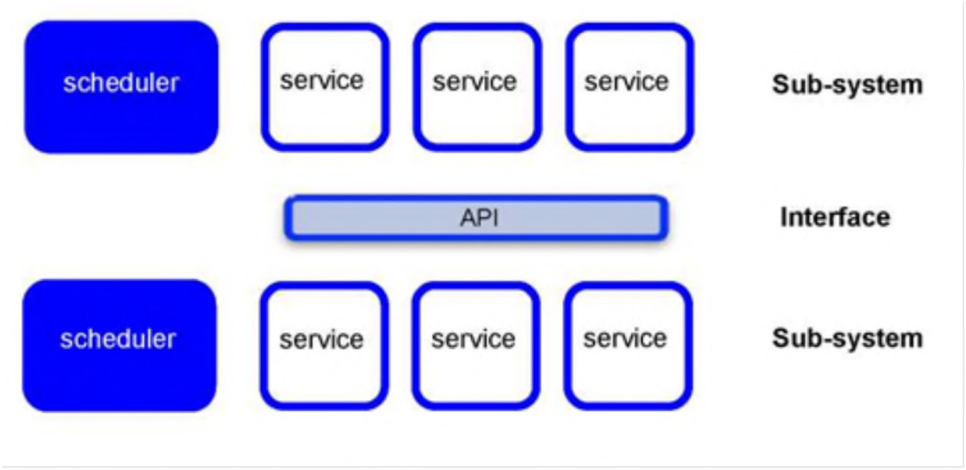

Fig. 1. The "system" API organization

This sentence turned out to be prophetic, because well after 1972, numerous computer operating system architectures were still influenced by Multics, to such a point that certain architectural traits will be passed down from generation to generation, although their use will be long gone due to the evolution of the hardware and of the use of computers.

Recall that the first machine used to develop Multics, the General Electric Model 654, had at most 1024 kilo-words of central memory, with each word being 36 bits (for a total of 4.5 megabytes), had up to 4 processors, each capable of executing 500,000 instructions per second. It was the size of a very large room. By comparison, a modern smartphone has 500 times more memory, and 1000 times more processing power. The smallest systems-on-a-chip for IoT are the size of the smallest coins, have 0.5 megabytes of memory and can run 2,000,000 instructions per second. The use of a smartphone, or of any IoT has therefore nothing to do with that of the General Electric 654, which allowed a few tens of users to perform scientific computing, or to develop Multics using slow and loud teleprinters [2].

In the following paragraphs, we will analyze some of the downsides of the architectural traits inherited from a time long ago, and ill-suited to modern communicating machines. We cannot overemphasize the fact that the consequences are not the result of a particular implementation, but rather of the architectures themselves. The past decade has seen a number of projects coming from developers whose aims were to rewrite part or all of existing architectures, without achieving significant gains. We will end the article by introducing a new operating system architecture meant for IoT and for communicating computer machines. In the following of this text we will use the term of "communicating machine" for machines using richer I/Os than a simple IoT device, that is to say using communication links, but also being able to process and store real time data flows.

Telecommunication and Input/Output Problems

We will distinguish three types of data flows which often exhibit telecommunication performance problems: high bandwidth point-to-point flows, high bandwidth broadcast flows, and low bandwidth flows of infrequent broadcast messages. In a more general manner, all input/outputs of our IoTs and computers are suffering serious performances issues, more specifically in their file systems. We will proceed by pointing out five architectural deficiencies which account for the performance problems. Some of these deficiencies are so prevalent that they have driven the introduction of palliative hardware solutions, which are often expensive.

Almost all existing operating systems exhibit poor performance as soon as protocol stacks such as HTTP/TCP/IP meet sustained flows nearing half of the transmission bandwidth. To see this, one only needs to start streaming an HD video through a broadband Internet connection to a PC. When the streaming is started, a waiting animation is always shown, for up to a few seconds, even though the video should start playing instantly. Then, sometimes the video will pause, which should not occur. When this happens, novices blame the PC, the network or the server of being too slow. Actually, the terminals' operating systems are to blame for these hiccups; that

can easily be proved by replacing the terminal by a device with a suitable operating system. Now, on the same connection, the same files located on the same server can be played without problems. For a number of users however, DSL TV is not good enough, driving the telecommunications operators to replace copper wire infrastructure by fiber too early given the investments made.

Set-top box operating systems also show poor performance when receiving broadcast streams, both by cable or from terrestrial and satellite antennas. If it is possible to record on a hard drive a single TV program, without experiencing too many glitches, recording 7 or 8 is nigh impossible. The total data flow of 8 high definition videos is only 16 megabytes per second, and the slowest of disks, at 5400 rotations/minute, have a data rate of 80 megabytes per second when correctly used. To cope with these deficiencies of the terminal operating systems, hard-drive manufacturers sell highly expensive models whose rotation speed is of 10,000 rotations/minute or more, and whose firmware is specially modified for video recording.

The most energy efficient home-automation radio protocols use small broadcast messages, which are not repeated. For instance, there are small electrical switches which broadcast exactly one small message over the radio. Although the speed is only 115,200 bauds, some systems can sometimes randomly lose a few bytes of the message making it unusable, even though the hardware is fully able to receive them without any loss. Although the radio protocols were specially designed to limit the electronics for a modem directly connected to an asynchronous serial port, the radio modems manufacturers are driven to add a small system-on-a-chip, whose sole purpose is to store the bytes received for the few milliseconds that are sometimes required by the operating systems.

These problems are caused by multiple architectural weaknesses, which combine and add up. Among them, the five most egregious are the high context switching times, the useless data copies, the excessive data buffering, overly general file systems, and lastly, inappropriate hardware interruption handling mechanisms. Once again, these are not implementation problems of these operating systems, but rather problems of the architectures themselves. The five issues are presented in further detail bellow.

Excessive Context Switching Times

The context switching time is the time spent at every transition from one activity to another: the time needed by the operating system to perform ad-hoc actions [3]. The architectural choices of what has to be done at every context switch determines the time it takes: whether to change the address space or not, whether to change the stack or not, and the extent of the modifications to the internal tables of the system. We purposefully use the term of “activity”, rather than “task” or “thread”. In fact – and this is an important architectural design decision –a technique called finite state automaton engine [4] exists but is not very widespread in the software world because it is difficult to master, but which nonetheless allows for context switching in virtually no time by eliminating the notions of task and threads. We will see later how to use it gainfully.

Useless Data Copying

Useless copies in the central memory of the machine can occur with certain operating systems because, as a result of the isolation mechanisms of the tasks and the system itself, copying is the only data transfer method between two tasks or between a task and the system itself. Architectural design decisions are the sole cause.

Excessive Data Buffering

Buffering consists of accumulating an amount of data before even starting processing. Often, these buffers are found to be 200 to 10,000 times too large and are in the megabytes or tens of megabytes rather than kilobytes. That's why users who start streaming must wait multiple seconds before seeing the first image even appear: the data begins to arrive from the server as soon as the request is made, but only when megabytes of video data have arrived does the video

decoding begin. One may ask why such large buffers are used, causing such long wait times. There are in fact two causes for this. The first is the operating system context switching times; using buffers a thousand times smaller means a thousand-fold increase in number of context switches by unit of time, which leads to a system collapse as soon as the activities are organized as tasks, no matter how "lightweight." The second is an implementation issue. Many binary data flow parsers are unable to stop their work at any point in the input flow, but only at certain points, such as at the beginning of a new image. These parsers can only be started when a buffer contains an amount of data at least equal to the largest possible compressed image size. This second point is not an architectural defect in and of itself. The architect having identified that the overly coarse parsers are a cause of system collapse can choose to integrate critical features in the system itself or in its libraries, so that they can be well implemented and optimized. With this, it is clear what the benefit is obtained by specializing an operating system: providing optimized business-specific functionality to developers, which they cannot optimize sufficiently due to a lack of time. Moreover, modern hardware sometimes comes with hardware parsers which developers don't use or under-use because of the complications this entails. The integration of all the parsers for high bit rate flow allows for the use of such hardware support. It is important to realize that using more powerful processors would not solve anything, because it would not diminish the context switching costs by a factor 1000 or 10,000, and would do nothing to reduce the number of bytes needed before starting these parsers. This last point is of utmost importance, because it explains why it is absurd to always increase the processing power of our smartphones: this extra power is of no use, because it was never the source of the sluggishness. And because of it, the battery life goes down. In fact, video decoding is the only reason why there are 8 cores in a cell phone using dedicated processors (DSPs) which can reduce the power requirement by a factor ten compared to software decoding on an eight-core processor.

Ill-Suited File systems

From a strict point of view, the term "file system" refers to the organization of data on a physical support. A file system is labeled "general file system" when it is both capable of containing a large number of small files as well as large files. In its general acceptation, which we will use, "file system" also refers to the operating system components which implement and maintain this organization. For the same disk data organization specification, such as FAT32, there are multiple ways to maintain this organization, and the methods chosen will have impacts greater than the organization itself. Depending on the use-case, file system strategies will favor small files by allow fast creation and destruction, or will benefit the throughput for large files. In the case of communicating machines simultaneously receiving large bit rate data flows, it will be necessary to use file systems that are well adjusted to that use case, where the movements of the disk's read-and-write head are minimized.

Poor interrupt handling

Modern electronics, including the smallest *Systems On a Chip* used for IoT, all have interrupt controllers allowing nested interrupts [5]. Software can configure the priority of each interrupt, and when two interrupts arrive nearly at the same time, the handling code for the first can be interrupted if the priority of the second is greater. The software must assign the greatest priorities to the shortest and most frequent handlers, and the lowest priorities to the longest and rarest handlers. That way a long handler will be interrupted by short ones, and no latency is induced in the handling of the frequent interrupt, which leads to the maximum speeds. A short handler cannot be interrupted by a long one, but this is of no importance. Of course, the short handler codes must be carefully optimized, and will not perform slow calls to the system. No interrupt handling can call a blocking function, such as grabbing a semaphore. Certain architects consider that the considerable power afforded by the modern processors eliminates the need to make use of the interrupt priorities, and that it is not a problem to call slow system procedures from interrupt handlers even though simple order of magnitude computations prove the contrary. This is the reason why certain operating systems, even when run on powerful processors lose the

last bytes of small radio messages transmitted at 115,200 bauds: if a UART has a 16 byte deep FIFO, it can be filled in 1.5 milliseconds, and the following bytes will be lost if the interrupt handler is not run during this time period. In the case of a communicating operating system, which because of its job, is exposed to sustained high interrupt rates, the interrupt handling must be performed swiftly and cannot be postponed and placed on a run queue, because doing so only increases the amount of ineffective activities in the system, increases the latencies, and worsens the problems due to interrupt misses.

Safety problems

In the case of developer workstation operating systems, the system must be fully protected from application bugs during the testing phase, no matter how expensive the protections are. Certain systems go so far as to protect components of the operating system or the drivers by automatically stopping the failing piece of software. An operating system meant for communicating machines is not designed to be used for its own development as was Multics, or to run text editors and compilers. In addition, in embedded communicating objects, it would be absurd to stop the software components allowing the communication itself, thereby isolating the device. It is in fact better to restart the system. Most importantly, what matters in the end is the safety of the operation of the whole communicating machine, which is a combination of hardware, operating system and application software.

As far as the operating system is concerned, the safety of its operation is guaranteed by a large number of automated, off-line checks. Each component of the system must be submitted to checks called “unit tests”; the component is tested alone and in isolation of the other components. A major issue is the comprehensiveness of the test coverage, that is the guarantee that all possible code paths have been explored at least once during the tests. For this last point, the architecture chosen for the operating system is not without consequence. In particular, the use of the previously mentioned finite state automaton engine technique lets one automatically detect if test coverage is complete or not.

As far as the applications are concerned, the choice of suitable architectures can also be essential, especially for the smallest of IoT devices. Let's consider two examples: when the language used to implement an application is compiled to machine code, it is impossible to prevent the application from inappropriately accessing its own data, and it is expensive to limit its address space in order to isolate the code, the system data and the peripheral registers. With “language-based computers” architecture [6], the combination of the hardware and its operating system do not offer any other choice than a single interpreted language for the development of the applications. It becomes impossible for an application to overwrite its own data, the code or data of the system, and it cannot access the peripheral registers.

Security problems

The protection of the data collected or stored on IoT devices, but also the integrity of the software of the object makes up what we will call the “security”. Surprisingly, certain architects consider that security is not an architectural concern. It is as if it were possible to secure an operating system after the fact, by adding “security layers” whose implementation as also outside the scope of the architect's responsibility. To illustrate, it is as if it were possible to draw up the plans for a building without taking account its security, to finish the construction, and only then try and achieve a high level of security by adding surveillance systems and access controls. When building a bunker or simply a locker room, the architect must from the design stage ban windows, add sufficiently thick walls, and use strong materials.

It behooves the architect to design a system which can start without relying on a shell. The architecture should by design prevent the execution of unauthenticated contents, prevent a user from consenting to disable the security mechanisms. And of course, the architecture should allow for the replacement of open source telecommunications stacks by proprietary codes, all of which must be required to come with automated test with extensive coverage.

Frugality and Scaling Problems

IoT must be frugal, both in terms of its energy consumption as well as its communication bandwidth. The architecture of the operating system impacts the power consumption, from the moment it allows a reduction in required memory sizes, and when it lets the processor clock remain low and even stop completely, which is only possible if the system can restart quickly, typically in less than a millisecond. For IoT of the smaller kind, communicating using a low bandwidth radio, software updates can be realized on a component by component basis in order to reduce the update sizes, which is only possible if the architecture was designed for this. From this point of view, the Language-based Computer architecture is particularly well suited. Indeed, the natural functional decoupling is strong in that case: the interpreter itself is an independent component, each library is an independent component, and the interpreted application is another. It is easy to add an independent version number to each of the blocs, allowing true upgrade of a single component, without needing to upgrade the others, which tends to happen with compiled languages. Because of a single function address table, it is possible to upgrade the functions of a library one by one, without needing to change more than one address in all the code, the address in the function table of the interpreter.

The capability of an operating system to both shrink in the smallest of objects and make use of the most complex is what we call its “scalability”. The amount of necessary code must be minimal, while allowing more code be added so as to provide more features. For this also, a Language-Based Computer architecture turns out to be very efficient. The interpreter code is only a few tens of kilobytes, and the number of functions it can call can be updated thanks to the use of an indirect call table. This then requires the P-codes of the instructions be at least 16 bits long, ruling out those whose instruction size is only 8 bits.

Fleet of Objects Management Problems

The deployment of large quantities of small objects in homes poses three problems of fleet management: the management of the fleet of objects inside one home, the management of objects of the same type across homes, and finally the management of the data which we allow to leave the premises.

Management of the Objects in one Home

The reason for adding communication abilities to small objects is first and foremost a local one: the objects in one home must interact with and receive commands from the residents. Some standards such as EnOcean [7] allow controller type objects to discover locally sensors and actuators, and to create links with them. Specific IP protocols such as Simple Service Discovery Protocol (SSDP) also allow the discovery of local equipment [8]. Even if they are simple compared to TCP/IP, these protocols are nonetheless too complex to be used by application software. It is therefore desirable to integrate them in the operating system.

Object Maintenance

The software upgrades in the case of IoT, where we only have low bandwidth radio channels occurs through gateways which have an Internet connection as well a connection to the radio channel. If we compare the total embedded code sizes, with the bandwidths of the radio channels, it become obvious why partial updates are required for code embedded in objects. From this point of view also, Language-based Computer type approaches are beneficial because the part of the application most often upgraded, the application, is wholly separated from the rest of the code, because it is written in a different language. It is highly desirable, and it may be required that all modifications to the code be authenticated by the operating system.

Exported Data Management and Permissions

The personal data collection and their mining has become a source of profit. Google for instance, to better sell targeted advertising, is increasing the sources of collection and cross-matching of our personal data, in particular the contents of our mails (Gmail) which are

systematically analyzed by artificial intelligence software called "bots." All of the manufacturers of IoT products also wish to collect and store the data collected in our homes for their own benefit. To do so, the collected data are directly transmitted using the Internet to back-end servers under the control of the manufacturers of objects, and only through these servers can users access their own data. Even if end users are doubtlessly ready to let this silent data collection happen, if they even realize it is going on at all, the same cannot be said of the managers of industrial sites, or of housing domains, who are justifiably afraid of security breaches. The operating systems of IoT controllers will have to offer the means to encrypt the transmitted data, but also to block confidential data from getting out.

Hardware input/output architectures

Historians generally consider that the first machine deserving to be called a computer is the ENIAC (Electronic Numerical Integrator and Computer) [9]. This computer was designed at the Ballistic Research Laboratory of the US Army, at Aberdeen in Maryland. This machine was designed by John Presper Eckert, based on ideas of John William Mauchly professor of physics, who had realized that computation of ballistic tables could be performed electronically. Before the ENIAC was fully functional, a second project called EDVAC (Electronic Discrete Variable Automatic Computer) [6] was launched in 1946 also under the direction of Eckert and Mauchly, based on a document written in 1945 by John Von Neumann: First Draft of a Report on the EDVAC. As the name suggests, the document is a first draft, and is very incomplete. The subject of the document is in no way the description of a computer architecture, but does have an explanation of how to use vacuum tubes to increase the speed of computation. The central chapter in this document, *6.0 E-Elements* provides a model of the "elementary electronic neuron", and the following chapters describe how to build an adder, a multiplier, and a subtractor, binary floating points, and central memory using this elementary building block. By way of introduction, the document starts with a paragraph called *2.0 Main subdivisions of the system*, which is, without saying so, a simplified functional description of the ENIAC. But because this article was published in 1945, before the 1948 article "The ENIAC", and because achievements were considered more important than publications in these final years of World War II, the historians mistakenly both attribute the invention of the architecture to John Von Neumann and tie it to the EDVAC [9].

The two fundamental points of the architecture of a computer are on one hand the description of its buses and of its instruction set, the two being closely tied. The 1945 article by Von Neumann does not address the notion of a bus at all, and only defines the different classes and sub-classes of instructions. Bear in mind that the article contains no architectural diagram. Nonetheless on-line literature is filled with diagrams entitled "Von Neumann architecture," most of which do not contain a bus, which is a central element without which the understanding of a computer is impossible, and which both the ENIAC and the EDVAC had. The following architectural diagram was draw by ourselves from the February 1948 article. *The ENIAC* (J.G. Brainerd et T.K. Sharpless), in particular the chapter *Machine Components* (Fig.2):

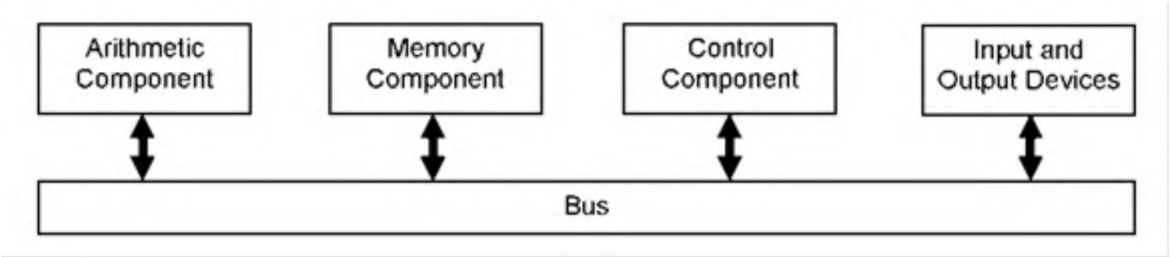

Fig. 2. A universal bus of ENIAC Machine

It is important to realize that the four rectangles at the top of this diagram have little to do with the physical architecture of the ENIAC which is found in *Figure 2 ENIAC Floor Layout* of the same article. What is called Arithmetic Component is a set of electronic bays which deal with

addition, subtraction, and division, but also include some memory; 20 accumulators and 3 function tables. The set of bays corresponding to the Memory Component also contains 20 other accumulators and 3 function tables identical to the previous ones. The *Input and Output Devices* rectangle represents a set of various hardware setups among which are card readers, a card puncher, indicator and button panels, each of them directly connected to the bus, which is made up of coaxial cables.

It is essential to remember that both the ENIAC and the EDVAC were machines meant for performing computation - for ballistic trajectory computation to be precise. In no way were these machines meant for data processing in the modern sense of the term. They were computers in the sense of automatic electronic calculators. Only ten years later would the distinction between computer and calculator disappear for good. All the attention and energy of the ten or so engineers working on building the ENIAC was concentrated on the creation of the electronic bays of the *Arithmetic Component*, *Memory Component*, and *Control Component*. All the *Input and Output Devices* were well tested devices bought "off the shelf" from different companies. For example, the card readers and punches were from IBM, these types of devices having been used for 30 years at that point (IBM was founded in 1911) [10]. Plugging these devices to the computer was a minor issue: little thought and effort was given to the problem. In 1948, in a famous article called *The Eniac*, two engineers who took part in the project, J.G. Brainerd and T.K. Sharpless, wrote the following: "Current developments in large-scale general-purpose digital computing devices are devoted to a considerable extent to obtaining speedier input and output mechanisms."

These developments bore fruit. In 1978, Hewlett-Packard started selling a machine considered to be one of the first "workstations", meant for a single user [11]. The HP 9845A comprises a graphical screen, a keyboard, a printer, and a tape reader. Like all Hewlett-Packard hardware, it is very easy to use and perfectly well built, making it a subject of envy and admiration. In the design of its architecture, the effort spent on input/output goes far beyond what was done for the program execution sub-system (Fig. 3).

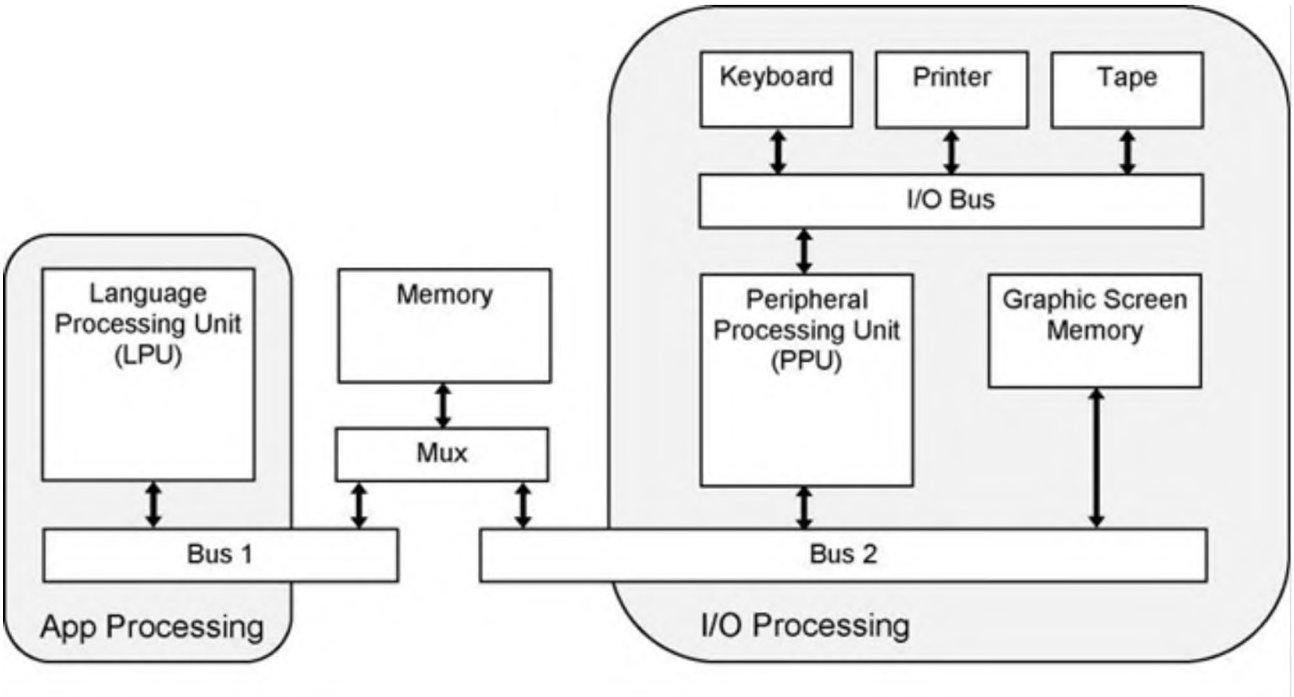

Fig. 3. The first "workstation" principal construction

The LPU executes a BASIC interpreter. The BASIC program is stored in memory with two access ports for the LPU and PPU. When the BASIC program requests an input/output, a request is written in the two port memory, and is executed by the PPU. While the PPU executes the input/output, the LPU can proceed with the execution of its BASIC program.

A new architecture for communicating machines

The remarkable hardware architecture of the HP 9845A of 1978 described above had only one important problem, and that was its cost because it used two 16 bit processors, the LPU and PPU running at 5.7 MHz. By comparison, the first micro-computers IBM PC 5150 of 1981 only had a single Intel 8088 processor running at 4.77 MHz. But both the removal of the processor dedicated to the input/output and the design of the BIOS low-level software layers which did not expose the hardware interruptions, gave the IBM PC 5150 poor input/output performance. Only with OS/2 (1987) and Windows NT (1993) did decent input/output handling systems emerge, and they were still far from the true capabilities of the hardware devices. In 1999, in an article entitled *Introduction to "The Eniac"* (referencing the 1948 article *The Eniac*), W. Burks (one of the main designer of the electronics of the ENIAC) and E. Davidson wrote:

"... and once again, as with the ENIAC, computation rate is not the performance-limiting factor, rather it is still the communication, the I/O, the setup for the computation. It seems that communication science may be at the heart of the problem after all."

In reference to this still relevant observation, we introduce a new distributed operating system architecture meant for IoT and communicating machines. It is based on the notion of "containers", that is a set of self-sufficient codes that can either run on bare metal without any other software, or on top of any third-party operating system. The architecture introduced is composed of two types of containers which talk only by messages, the app containers and the I/O containers.

Every time it needs to perform input/output an app container sends one and only one request message to the I/O container, which will return exactly one response message. We have a client/server relationship, the app container being the client, and the I/O container being the server. A single machine can host either only an app container, only an I/O container, or both. Every machine in the same local network has a unique number called its node number.

The request and response messages have exactly the same structure, called an event. An event carries two addresses, one for the recipient and one for the sender. An address is a triple of integer numbers: node number, automaton number, and way number. The automaton number designates a functionality of a container, while way numbers distinguish the different instances of the same software functionality.

An app container can contain an RTOS, C applications, interpreters, an HTML renderer or even another operating system. In the latter case, the container must include a software component for that system to convert all the input/output commands to request messages.

An I/O container contains drivers, protocols, services, and file systems. When a message reception requested, it can stack a protocol or a file system on top of a driver. It is also able to create pipes which are unidirectional data flow within the container. It has two schedulers called VMIT and VMIO. The first preempts the second with no latency, with the very next instruction running the VMIT.

The following diagram represents one communicating machine and two IoT devices on the same local network, typically Ethernet and WiFi (Fig.4).

Node 1 will typically be a router, or a NAS (Network Array Storage) file server. It can have a display, such a TV or a set-top box. It contains four sub-operating systems, each having their use and a different latency. The VMIT responds to hardware interrupts, with a response time much less than the microsecond. The VMIO receives I/O requests, and has an average response time of less than 100 microseconds. The VMK is a non-preemptive RTOS which allocates time to the Linux kernel. The Linux kernel is stripped of any driver, protocol, network service or file system. All of the input/output requests coming from the Linux applications are transformed into request events which are directly deposited to an I/O container, which can be in any of the nodes 1, 2, or 3. For a Linux binary, all the devices of the three nodes are seen as local devices. Without any modification, the Linux kernel benefits from distributed system features. We therefore have four sub-systems, where each has a specific role for which it is specialized, and from the architecture of its scheduler has a different response time.

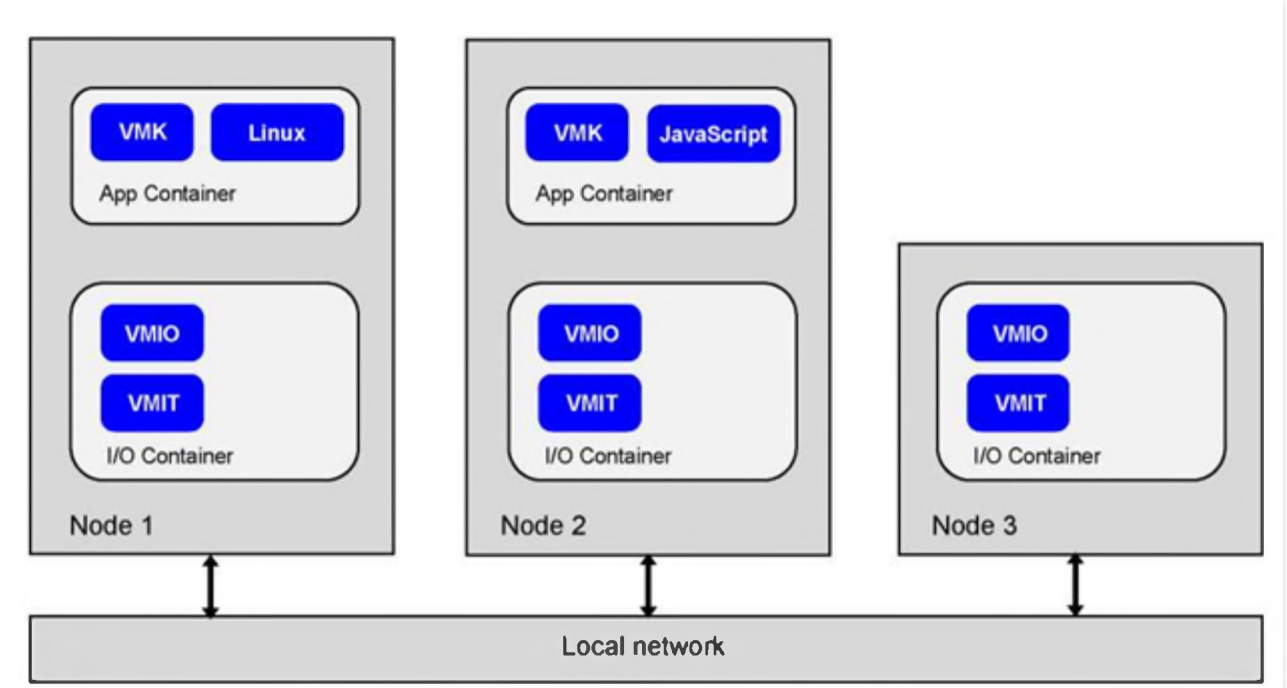

Fig. 4. Communication of several IoT devices

Of course, the most feature-rich sub-system will be the slowest, and conversely the most lightweight will be the fastest.

Node 2 will typically be equipped with a 4 MHz processor, with 16 kilobytes of RAM and 128 kilobytes of code, which gives it capabilities equivalent to that of the 1978 HP 9845A. Like this machine, node 2 is a *Language-based Computer*; its programming language, in this case ECMA 262 (also called JavaScript) is interpreted. Like the HP 9845A, it is responsible for all the input/output. Unlike the 9845A, a single processor is used. The VMIT preempts the VMIO and the VMK with zero latency, and the VMIO preempts the VMK with zero latency.

Node 3 is a small sensor which does not contain an application container. It behaves like an input/output server; it handles requests which can come from the other nodes.

Application Containers

Like the Language processing Unit of the HP 9845A, an application container contains everything that allows an application to run, except for the input/output. What constitutes the application itself will be there, be it C code, JavaScript code, but there is also be HTML files. The container also includes the necessary code for that code, such as mathematical functions, an JavaScript interpreter or an HTML renderer. It contains an RTOS which will support the application written in C, the interpreter or the HTML renderer.

The VMK

The features that the RTOS must provide are very limited, because all of the input/output will be transferred to the I/O container. We call VMK this simplified RTOS. It must provide primitives for task handling, for semaphores, and for event queues. Every task of the VMK has a stack, and a message queue of its own events, and optionally its address space. Finally, the VMK must have the means to send events to the nodes, so that the I/O requests can reach the various recipient container nodes.

HTML renderer

The code bases of many large software projects such as HTML renderers usually have abstraction layers for all of their input/output: telecommunications, files, and graphics. They are therefore easily embeddable in application containers, using a conversion layer that transforms all procedural input/output calls to request events. Furthermore, experience shows that 90% of

what is believed to be part of the HTML rendering in itself is actually code used by the various abstraction layers meant for the various operating systems, and the remaining size will go down from 200 to 20 megabytes of code.

Application-Oriented Operating System

An application-oriented operating system such as Unix or Linux can easily be embedded in an app container. It is easy to strip them of all of their drivers, protocols, network services, and file systems and to create once and for all, a conversion layer like with the HTML renderer, which turns the procedural input/output requests to request event deposits. Having done this, the size of the kernel is only a few hundreds of kilobytes. In this way, we have as a single VMK task, a Unix/Linux kernel where almost all security flaws have disappeared, because the weakest components have been replaced. Previously unobtainable throughputs are achieved, and the data flows inside pipes within the I/O containers. Finally, the strict separation between the kernel and the I/O located in distinct containers and communicating by passing messages, makes using hardware peripheral register access controls (a trusted zone) easy, further increasing the security of the data.

One should note that the client/server model used between applications and for input/output means that the requests made by the application does not need to go through the VMK, and are directly sent to the recipient input/output container. The same is true for the response events.

Input/Output Containers

An input/output container is the equivalent of the Peripheral Processing Unit of the HP 9845A. It receives input/output and pipe configuration requests. It contains drivers, protocols, network services, and file systems. It is composed of two subsystems which are: VMIT, an interrupt handler, and VMIO, a monolithic input/output monitor.

Interrupt handler

At the lowest level is a sub-system called VMIT, whose role is to handle hardware interrupts with different priorities and which can therefore be nested. To each hardware interrupt priority corresponds one and only one stack. The address space in unique, and is that of the input/output monitor. This sub-system handles the low-level drivers, that is all the code which depends on the peripherals. For every type of device or peripheral, there is a specific *Hardware Abstraction Layer*, that is a specification of both the interface of the procedure meant to control the type of device, and the events submitted by the interrupt handlers. These messages can only be deposited to the local input/output monitor, located in the same address space. All of the code of the VMIT depends on the specific hardware, including the scheduler which depends on the CPU and the interrupt crossbar wiring.

Monolithic Input/Output Monitor

Above the VMIT is a monolithic input/output monitor called the VMIO, which executes high-level drivers, the protocols, the services, and the file systems, all implemented as automaton transition tables. There is no notion of a task at this level, nor of semaphores which makes going from one function to the next a latency-free operation, which in turn allows for high bit rates even with multiple concurrent flows. In order to achieve zero-latency, the VMIO uses a single stack for itself and all its automatons, a single address space and a single set of registers. Every driver, protocol, service or file system component is composed of a transition table (state, event) and of a set of C procedures, which are all transactional handlers for a transition. These C procedures, these automaton transition handlers, when they need to send commands to a device under their control, will use directly call without any context switching the C procedures which implement the *Hardware Abstraction Layer* for the device. There is a one to one correspondence between high-level drivers and the specifications of the low-level drivers. All of the code for the VMIO, including the scheduler, is written in C, and is strictly portable without any modification

or conditional compilation. The VMIO has a pipe mechanism, which allows a unidirectional data transfer from automaton to automaton. A pipe is configured and started using request events, and then the client does not need to intervene anymore for the data to flow from automaton to automaton. Thus, the various data flows occur without any context switching, and in particular no copy and no address space change. If for instance the application configures a pipe ETHERNET → TCP → HTTP → FAT32, a high speed download feature is realized.

In this example, the TCP protocol, the HTTP service and the FAT32 file system are executed within the monolithic monitor, and not within the RTOS, which runs in the app container. This is a major trait of the architecture we introduce. Some have noted that the RTOSes are two slow for demanding I/O tasks and have tried to develop faster RTOSes by reducing the context switching time. This is pointless, as it reduces the functionality of the RTOS, without even truly reaching the goal of a sufficient speed-up. By having both an input/output monitor and separately an RTOS, we can both perform I/O faster than an RTOS would, while also having a feature-rich RTOS if needed.

Media Home Gateway Example

A Media Home Gateway will typically have a hard-drive, and an Internet connection be it Ethernet or WiFi. It hosts an application container and an input/output container (Fig.5).

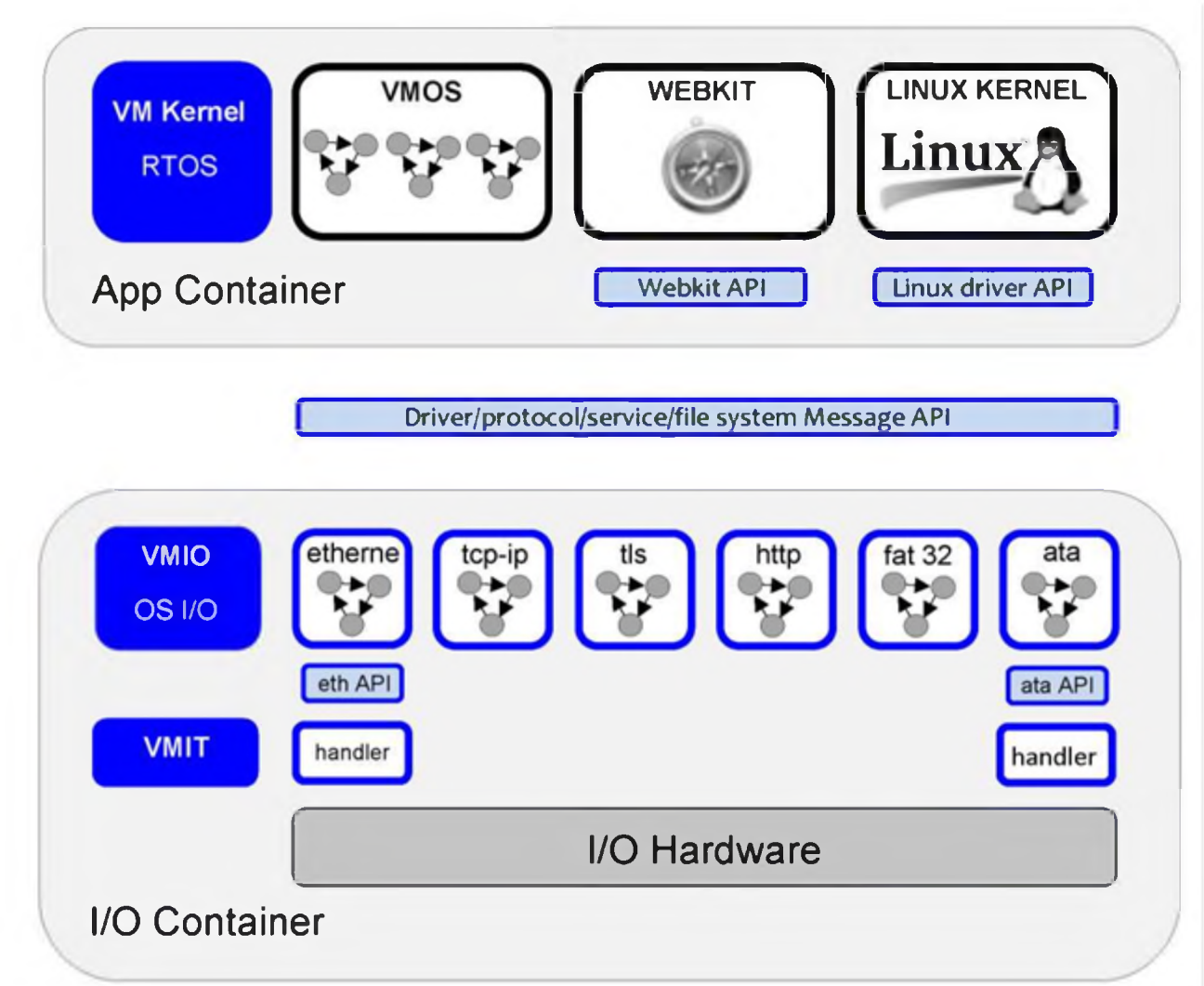

Fig. 5. Home media Gateway device software organization

The application container embeds a first application operating system VMOS which contains interpreters built as finite state automatons. The VMOS executes the *middleware* of the *Media Home Gateway*. Second, there is a HTML renderer, for which an abstraction layer was

implemented, which the input/output requests of the renderer are converted in events deposited to the I/O container. Third is a Linux kernel stripped of all of its drivers, protocols, services, and file systems. An abstraction layer converts all Linux input/output requests to request event deposits.

The I/O container has two low-level drivers, that is hardware-specific code, one for the Ethernet controller and one for the ATA disk. The two interrupt handlers are called by the VMIT. Each low-level drivers needs to follow the specification for the type of hardware, the low-level Ethernet driver must implement an *Ethernet API* which is not the same as the *ATA API*. The VMIO input/output monitor is a finite state automaton engine, which executes the automatons that are independent of the hardware. It contains the "high-level" drivers for Ethernet and ATA, but also the TCP/IP and TLS protocols, the HTTP service, and the FAT32 file system.

An IoT with Application Example

An IoT *Language Based Computer* will typically have an Ethernet connection and multiple radio modems such as Bluetooth Low Energy or EnOcean. It hosts an application container and an I/O container (Fig.6).

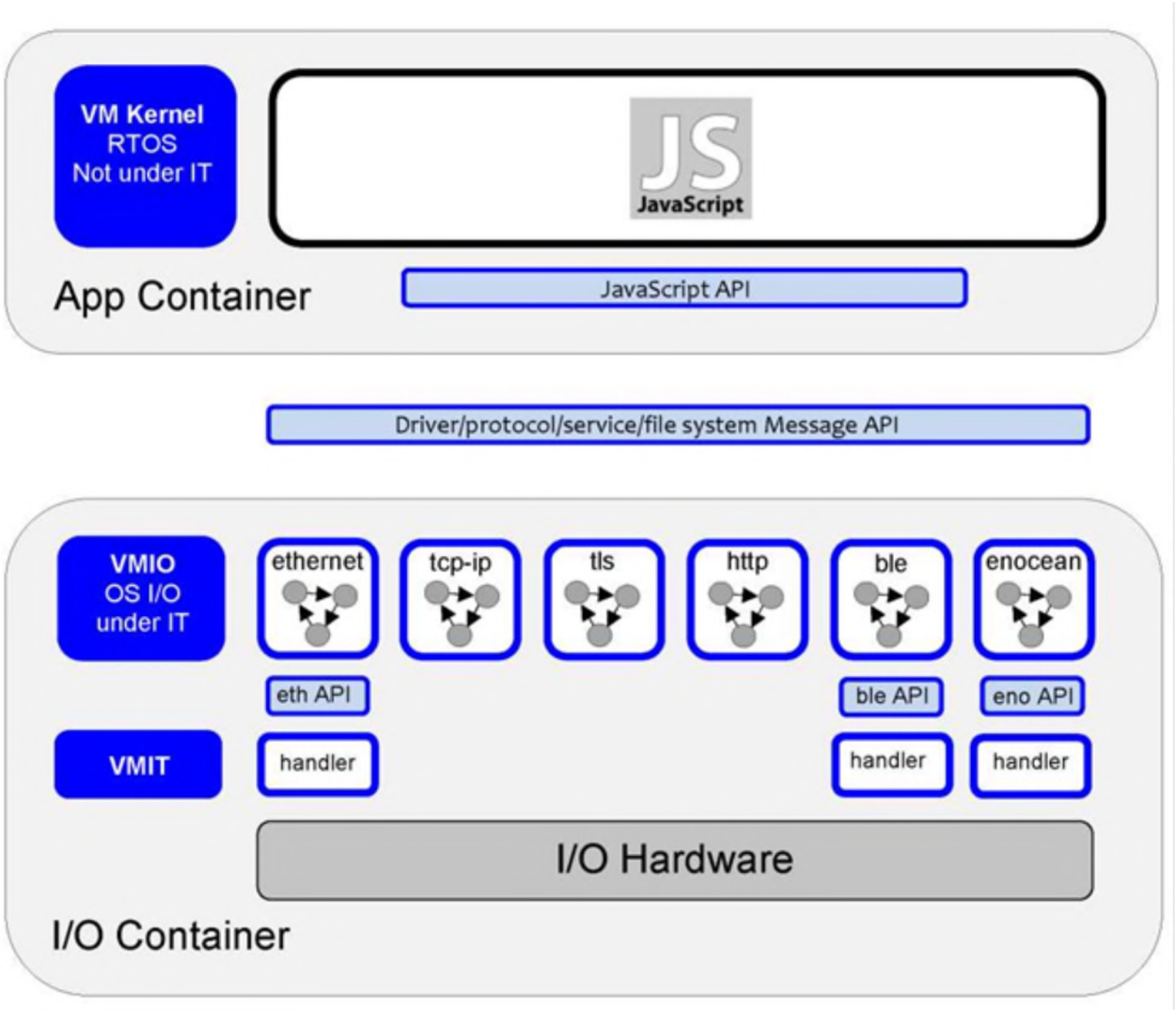

Fig. 6. The example of IoT device software with Application level

The app container embeds a JavaScript interpreter and an application written in JavaScript. An abstraction layer converts the JavaScript input/output request to request events.

The input/output container has three low-level drivers, that is hardware dependent code, the one for the Ethernet controller, the one for the Bluetooth Low Energy modem and the one for the EnOcean modem. All three interrupt handlers are called by the VMIT. Each low-level driver

must implement a specification specific to the nature of the hardware, the low-level Ethernet driver must follow the *ethernetAPI*, which is not the same as the *bleAPI* (Bluetooth API), or the *enoAPI* (EnOcean API). The VMIO I/O monitor executes six automatons which are independent of the hardware: the high-level drivers for Ethernet, BLE and EnOcean, but also TCP/IP and TLS, the the HTTP service.

A Basic IoT Example

A basic IoT device will typically have an EnOcean radio modem, and binary I/O using GPIOs. It only contains an I/O container (Fig.7).

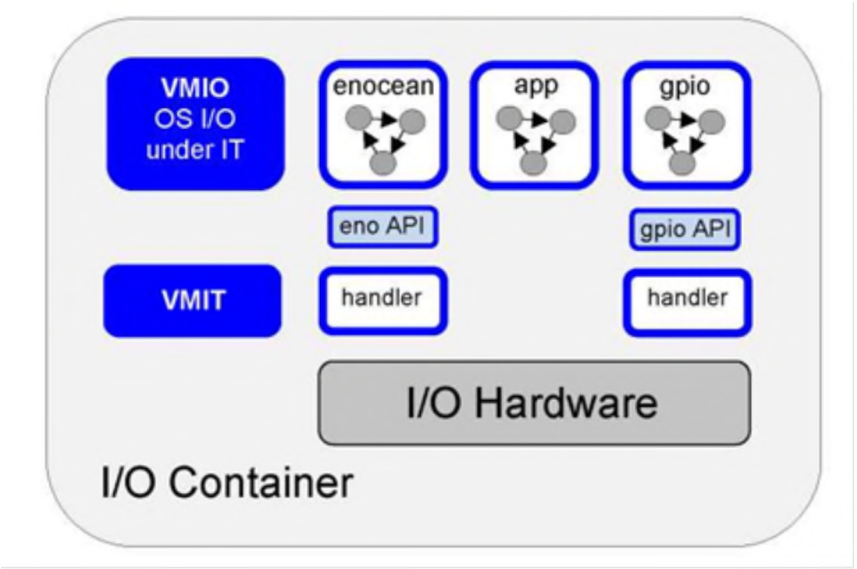

Fig.7. The basic software set for IoT device

The input/output container has two low-level drivers, one for the EnOcean radio modem, another one for the digital and analog GPIOs. The two interrupt handlers are called by the VMIT. The VMIO input/output monitor executes three automatons which are independent of the hardware; the high-level EnOcean and GPIO drivers, but also a micro-application called app.

The small application called app is written as a finite state automaton and is inside of the input/output container. Typically, the app automaton receives remote requests and exerts elementary command control logic. This is an additional feature afforded by this architecture, allowing to further shrink of the code by eliminating the application container and the VMK.

The basic IoT can simultaneously behave like a remove device in the case of a distributed system, being an input/output server, but also as an IoT able to handle messages which are not events thanks to the small app automaton which can contain a small message parser of another format, and simple application logic.

Conclusions

In a world where hardware technologies have long followed Moore's law, the principles of operating system design evolve at an entirely different pace, where the major traits of the architectures of the systems such as Windows, iOS, and Linux are derived from three decades of work dating back to 1964 (Multics architecture).

The study of the new architecture introduced here started with the need to implement a distributed satellite image processing system. In order to chain transparently, processing performed on one hand on a mini computer running FORTRAN code, and on the other on a image processing machine (the two being connected by a high speed interface) the software was split in an application container, and two image processing containers. The first container comprised a FORTRAN interpreter, which made requests to the image processing software located on the same computer and also to the container for the image processing machine.

All of the architectural traits described here have been validated separately through the implementation of various projects between 1986 and 1999. From 1999 to 2008, an operating system has been implemented following all of the architecture, proving that it is indeed a very efficient solution to all of the problems identified at the start of this article. This culminated in real projects, delivering consumer electronics that reached the market.

The architecture is based on concepts and ideas which all existed previously. We did not invent the notions of container, of *Language-based Computer*, of finite state machine engine, of input/output monitor, of interrupt dispatcher, of abstraction layers, of sub-system separation, of preemption, or of execution levels. We did not invent a model for hardware architecture such as the one attributed to Von Neumann, nor did we discover the importance of logical automatons of which Alan Turing has shown are a model of any machine capable of computation.

We did combine all of these concepts and have thus obtained a new architecture and thanks to this we believe we have solved the major problem of input/output for which W. Burks observed (as late as 1999) a lot remained to do from a conceptual point of view. Moreover, this architecture allows improvements in *machine to machine* relationships, in operational safety, in security, in frugality with regards to hardware resources and electrical power, in scalability, and in deployed fleet management. The use of finite state automaton in the input/output container, allowing both greatly improved performances and the comprehensiveness of unit tests, is an essential aspect.

This architecture can be used fully or partially according to need. It is first and foremost meant for true IoT. It is also applicable to all systems doing input/ouput whatever they are. But it can also be used in hybrid objects, that is objects which both communicate while also performing more complex software functionality: control systems, data collection and storage, or local artificial intelligence.

The integration of small rule-based programming, also called “artificial intelligence”, inside our home clouds seems essential in order to use all the hardware capabilities of our communicating machines. These will have to be installed and configured in as fully automated manner as possible, be able to perform “reflex arc” type actions and request assistance from the outside when needed.

REFERENCES:

[1] F. J. Corbató, C. T. Clingen, J. H. Saltzer (1972), *Multics — The First Seven Years* (AFIPS). Accessed November 20, 2017 at: http://web.mit.edu/Saltzer/www/publications/f7y/f7y.html (This is an excellent review, written after a considerable perioAd of use and improvement over the initial efforts.)
[2] GE-645. System manual. GE information system. Large System Department, January 1968.
[3] Haldar, Sibsankar and Aravind, Alex A. (1962) – *Operating systems* London: Pearson Education. ISBN 978-8131730225.
[4] Hopcroft, John E. and Ullman, Jeffrey D. (1979). Introduction to Automata Theory, Languages, and Computation. Reading, MA: Addison-Wesley. ISBN 0-201-02988-X.
[5] Badawy, Wael, and Julien, Graham A. (2003) – System-on-Chip for Real-Time Applications. Springer Science & Business Media. ISBN 1-4020-7254-6.
[6] McKeeman, William M., Language directed computer design. Stanford University Stanford, California 1968.
[7] Interantional Organization for Standardization (2012) ISO/IEC 14543-3-10. https://www.iso.org/standard/59865.html.
[8] UPnP Device Architecture 1.1. UpnP Forum 2008.
[9] Rojas, Raúl and Hashagen, Ulf (2002) *The First Computers—History and Architectures.* Boston MA: MIT Press. ISBN-10: 0262681374.
[10] Web site: https://en.wikipedia.org/wiki/IBM.
[11] Kückes, A. (2010) *The HP 7845 Project*. Accessed November 20, 2017 at: http://www.hp9845.net/9845.

Поступила в редакцию – 10 сентября 2017 г. Окончательный вариант – 05 февраля 2018 г.
Received – September 10, 2017. The final version – February 05, 2018.

Вячеслав М. Барбашов, Николай С. Трушкин
[1]*Национальный исследовательский ядерный университет «МИФИ»,*
115409, Москва, Каширское шоссе, 31, Россия
e-mail: VMBarbashov@mephi.ru, https://orcid.org/0000-0001-7136-415X
e-mail: NSTrushkin@mephi.ru, https://orcid.org/0000-0003-2407-084X

ОСОБЕННОСТИ МОДЕЛИРОВАНИЯ ИНФОРМАЦИОННЫХ ОТКАЗОВ ЦИФРОВЫХ КМОП СБИС ПРИ ВОЗДЕЙСТВИИ РАДИАЦИИ

DOI: http://dx.doi.org/10.26583/bit.2018.1.03

Аннотация. Рассмотрены методы обеспечения информационной безопасности, которые основаны на применении функционально-логического моделирования больших цифровых интегральных схем (СБИС) при воздействии ионизирующего излучения. Показано, что кратность узла и мощность спектра более точно описывается при использовании понятия нечеткой кратности. Предложены методы прогнозирования информационной безопасности БИС при воздействии ионизирующего излучения, которые основаны на модели нечеткого цифрового и вероятностного надежностного автоматов. Причем характер их изменения при облучении зависит от многих факторов, включая тип излучения, его интенсивность и спектр, вид критериального параметра характеризующего радиационную стойкость ИС, режим работы микросхем. Поэтому в разных диапазонах уровней или интенсивностей воздействия модель ИС может носить как нечеткий, так и вероятностный характер. Проведения такого сопоставления является необходимым этапом общей процедуры анализа радиационной стойкости ИС.

Ключевые слова: топологические вероятностные модели, нечеткие вероятности, зоны неопределенности.

Для цитирования. ***БАРБАШОВ, Вячеслав М.; ТРУШКИН, Николай С.*** *ОСОБЕННОСТИ МОДЕЛИРОВАНИЯ ИНФОРМАЦИОННЫХ ОТКАЗОВ ЦИФРОВЫХ КМОП СБИС ПРИ ВОЗДЕЙСТВИИ РАДИАЦИИ. Безопасность информационных технологий, [S.l.], v. 25, n. 1, p. 34-40, 2018. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1091>. Дата доступа: 14 feb. 2018. doi: http://dx.doi.org/10.26583/bit.2018.1.03.*

Vyacheslav M. Barbashov, Nikolai S. Trushkin
National Research Nuclear University MEPHI
Kashirskoe shosse, 31, Moscow, 115409, Russia
e-mail: VMBarbashov@mephi.ru, https://orcid.org/0000-0001-7136-415X
e-mail: NSTrushkin@mephi.ru, https://orcid.org/0000-0003-2407-084X

Features of the model of main information failures in digital CMOS VLSI at impact of the radiation

DOI: http://dx.doi.org/10.26583/bit.2018.1.03

Abstract. The methods of information security, which are based on the use of functional-logical modeling of very large digital integrated circuits (VLSI) under the influence of ionizing radiation are considered. It is shown that the multiplicity of the node and the power of the spectrum are more accurately described when using the concept of fuzzy multiplicity. Methods are proposed for predicting LSI failures when exposed to ionizing radiation, which are based on the model of fuzzy digital and probabilistic reliability automata. Moreover, the nature of their changes during irradiation depends on many factors, including the type of radiation, its intensity and range, type a criteria parameter characterizing the radiation resistance of ICs and work mode. Therefore, in different ranges of levels or intensities of the impact of the IC model can be either of fuzzy or probabilistic nature. Carrying out such a comparison is an essential step in the overall analysis of the IC radiation resistance.

Keywords: topological probabilistic models, fuzzy probability, areas of uncertainty.

For citation. ***BARBASHOV, Vyacheslav M.; TRUSHKIN, Nikolai S.*** *Features of the model of main information failures in digital CMOS VLSI at impact of the radiation.IT Security (Russia), [S.l.], v. 25, n. 1, p. 34-40, 2018. ISSN*

2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1091>. Date accessed: 14 feb. 2018. doi: http://dx.doi.org/10.26583/bit.2018.1.03.

Введение

Как, правило, в условиях воздействия радиации используется модель цифрового автомата с привлечением аппарата теории вероятности. В случае, когда необходим учет физических механизмов отказа СБИС, то построение функционально-логической модели такого класса предполагает использования нечеткого цифрового автомата Брауэра и переход от аксиоматики булевой решетки к аксиоматике векторной решетки для каждого $x \in X$ [1, 2]. Реальный характер радиационного поведения СБИС определяется соотношением радиационно-чувствительных параметров ее элементов с учетом кратности узла и мощности спектра СБИС. В этом случае более точная оценка возможна при использовании понятия нечеткой кратности. Соотношение между функцией распределения плотности вероятности и критериальной функцией принадлежности (КФП) определяет, в конечном итоге, целесообразность использования функционально-логических моделей радиационного поведения СБИС применительно к каждому конкретному случаю. Такое сопоставление является необходимым этапом при анализе радиационной стойкости СБИС.

Дерево топологии моделирующей среды

Для оценки мощности спектра дерева топологии КМОП СБИС с применением нечетких чисел при радиационном воздействии в работе [2] были даны определения кратности узла и мощности спектра дерева СБИС. В этом случае более точная оценка стойкости БИС возможна при использовании понятия нечеткой кратности.

Как правило, с увеличением поглощенной дозы ионизирующего излучения амплитуда импульса логического элемента $l \in [0,1]$ уменьшается [3, 4], и собственная вероятность переключения элемента тоже уменьшается. Это уменьшение вероятности можно интерпретировать как бы увеличением порога срабатывания $l_{П} \in [0,1]$.

В качестве примера на рис. 1 приведены экспериментальные результаты разброса $U^0_{вых}$ чипов КМОП цифровых интегральных микросхем оперативного запоминающего устройства (ЦИМС ОЗУ) серии 1617РУ6 и их транзисторных структур, которые соответствуют нормальному распределения Гаусса. Поскольку дисперсия σ^2 зависят от поглощенной дозы облучения, то по верхней оценки (6) можно установить и максимальную дозу облучения.

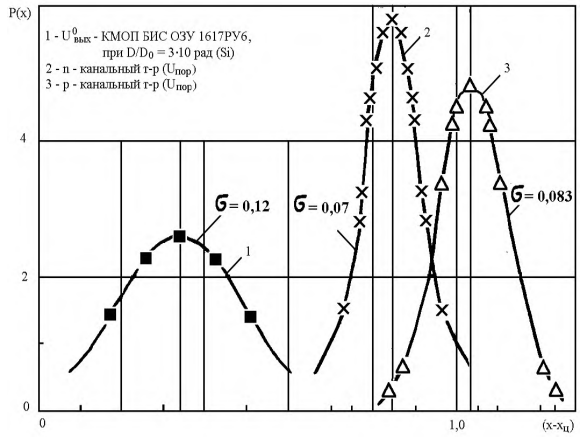

Рис. 1. Распределения усредненных по пластине $U^0_{вых}$ чипов КМОП ЦИМС ОЗУ 1617РУ6 от дозы (1), Uпор n- и p- канальных МОП транзисторов (2, 3), полученные на ускорителе электронов с Ee – 130

(Fig. 1. Distributions of averaged over the chip logical zero output voltage CMOS VSLI RAM 1617RU6 from the dose (1), threshold voltage of n-channel and p-channel MOS transistors (2, 3) obtained at an electron accelerator with Ee = 130 keV)

Пусть из узла соединений логических элементов выходит n ветвей. Узел выбирается с максимальным количеством связей (критический узел). Кратность узла в случае $m = n$ реализуется при нормальной работе. При этом, если $l_П$ начинает приближаться к l, возникает зона неустойчивости, в которой элементы переключаются случайным образом и кратность узла становится неопределенной. Ее величина, как известно [5 - 7], может быть выражена нечетким числом. Для упрощения оценок в данной работе используются треугольные $(L-R)$ нечеткие числа.

В тоже время величины порогов $l_П$ распределены по некоторому закону $f(x)$ такому, что $f(x) \underset{\substack{x\to 0\\ x\to 1}}{\to} 0$ (Рис. 2). Так как математическое ожидание $\xi = l_П$, то увеличение дозы облучения $\xi \to l$ и распределение смещается вправо (пунктир на Рис. 2).

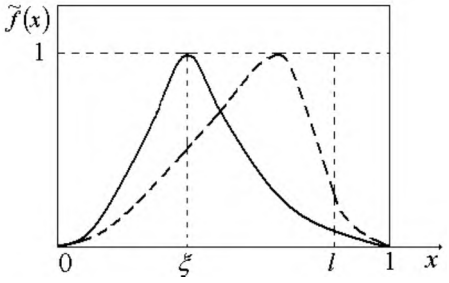

Рис. 2. Функция распределения порогового напряжения переключения логических элементов – $\tilde{f}(x) = \dfrac{f(x)}{f(\xi)}$

(Fig. 2. Logic threshold switching threshold function - $\tilde{f}(x) = \dfrac{f(x)}{f(\xi)}$)

Мода нечеткого числа, очевидно, зависит от величины:

$$S = \int_0^l f(x)dx,$$

а размытие от минимальной разности выражается соотношением [8]:

$$\min\{(S(\xi) - S(l)),\ (S_m(\xi) - S(l))\},$$

где S_m - максимальное значение S.

В этом случае рассмотрим нечеткие числа кратности узлов для двух функций распределения $l_П$ - Гаусса и Лапласа.

Для нормального закона распределения Гаусса справедливо равенство:

$$S_G = \frac{1}{\sqrt{2\pi}\cdot\sigma}\int_0^l e^{-\frac{(x-\xi)^2}{2\sigma^2}}dx = \Phi\left(\frac{\xi}{\sigma}\right) + \Phi\left(\frac{l-\xi}{\sigma}\right), \qquad (1)$$

где $\Phi(z)$ - интеграл вероятностей.

Справа в (1) функция симметричная относительно $\xi = \dfrac{l}{2}$ и при соотношении $\dfrac{l}{\sigma} > 4$ в этой точке имеется слабый максимум, равный $2\Phi\dfrac{l}{2\sigma}$.

Такая особенность функции позволяет использовать простую трапецеидальную аппроксимацию $\tilde{S}_G$ (Рис. 3) [9], где $\alpha = \dfrac{l}{\sigma}$, $x = \dfrac{\xi}{\sigma}$, $\alpha > 4$, $0 \le x \le \alpha$.

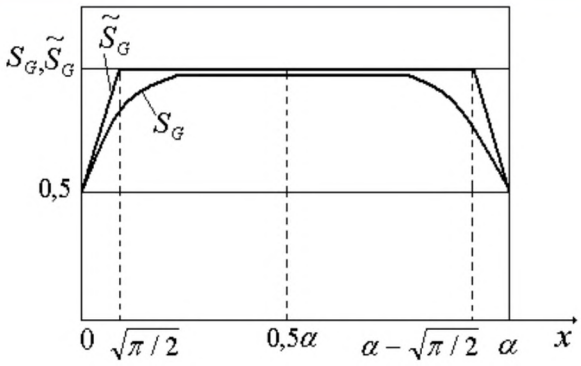

Рис. 3. Трапецеидальная аппроксимация величины S_G для нормального закона распределения Гаусса
(Fig. 3. Trapezoidal fitting of S_G for the normal Gaussian distribution law)

В этом случае моду нечеткого числа можно записать в виде выражения:

$$M_G = [n \cdot \widetilde{S}_G(x)], \tag{2}$$

Полученная размытая функция (2) имеет следующий вид:

$$\Delta_G = 2[n \cdot \min\{(\widetilde{S}_G(x) - 0{,}5), \ (1 - \widetilde{S}_G(x))\}], \tag{3}$$

где $\alpha - \sqrt{\pi/2} < x < \alpha$.

В выражениях (2) и (3) $[Z]$ - целая часть $[Z]$.

Тогда из формул (2) и (3) получим, $(L - R)$ нечеткое число, которое представляется в виде равнобедренной функции с основанием Δ_G (Рис. 4).

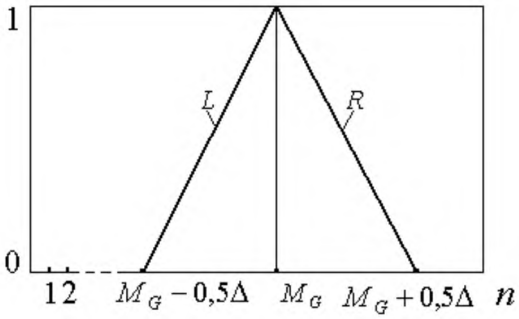

Рис. 4. Нечеткое число кратности узла соединения логических элементов
(Fig. 4. Multiplicity fuzzy number of the node connecting the logical elements)

Если $x < \alpha - \frac{1}{2}\sqrt{\frac{\pi}{2}}$, то размытие не включает n.параметров и соответствующая этому случаю, поглощенная доза ионизирующего излучения считается катастрофической. В этом случае, предельная поглощенная доза определяется следующим равенствами:

$$x_{\max} = \alpha - \frac{1}{2}\sqrt{\frac{\pi}{2}} \text{ или } \xi_{\max} = l - \frac{\sigma}{2}\sqrt{\frac{\pi}{2}} \approx l - 063\sigma. \tag{4}$$

Полученные выражения (4) справедливы для одного узла.

Для большого количества узлов дерева распределение Лапласа имеет:

$$S_L = \frac{1}{2\beta}\int_0^l e^{-\frac{|t-\xi|}{\beta}}\,dt = 1 - \frac{e^{x-\alpha} + e^{-x}}{2}, \tag{5}$$

где $x = \frac{\xi}{\beta}$, $\alpha = \frac{l}{\beta}$, $\alpha > x$, $\alpha > 4$.

Функция распределения Лапласа (5) аналогично распределению Гаусса (1) и ее можно аппроксимировать также трапецеидальной функцией $\widetilde{S}_L$ (Рис. 5).

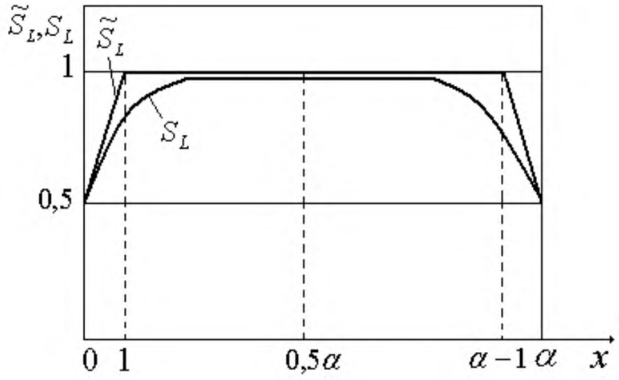

Рис. 5. Трапецеидальная аппроксимация S_L для распределения Лапласа
(Fig.5. Trapezoidal fitting S_L for Laplace distribution)

При этом мода и размытие нечеткого числа соответственно равно соотношениям [10]:

$$M_L = [n \cdot \widetilde{S}_L(x)], \tag{6}$$

$$\Delta_L = 2[n \cdot \min\{(\widetilde{S}_L(x) - 0{,}5),\ (1 - \widetilde{S}_L(x))\}], \tag{7}$$

где $[Z]$ - целая часть Z, $\alpha - 1 < x < \alpha$.

Использование распределение функции Лапласа предпочтительнее, так как в области математического ожидания имеет значительно меньший разброс.

Для несимметричных законов распределения формулы (2) – (7) остаются справедливыми, но с другими пределами изменения обобщенного параметра x. Нормировка x осуществляется по некоторому характерному параметру размытия распределения [11].

Для оценки мощности дерева необходимо суммировать нечеткие числа, но среднее значения, как определено в работе [3], вычисляются через среднее значение мод и размытости.

В этом случае, средняя величина моды равна:

$$M_\Sigma = \frac{\sum_{i=1}^{K} M_i}{K}, \tag{8}$$

где K - число узлов в дереве, M_i - мода нечеткого числа $i-го$ узла.

Средняя размытость определяется из соотношения:

$$\Delta_\Sigma = \frac{\sum_{i}^{K} \Delta_i}{K}, \tag{9}$$

где Δ_i - размытость нечеткого числа $i-го$ узла.

Таким образом, мощность дерева выражается также нечетким числом, но мода и размытость которого, определяемые по формулам (8) и (9), не обязательно целые. Ели размытость не захватывает максимальные значения мощности, приведенные в [3], то соответствующая поглощенная доза излучения считается катастрофической, причем меньше чем для одного узла [12].

Однако, данная оценка остается завышенной, так как не учитывается тот факт, что для узлов промежуточного уровня дерева, при не переключении какого-то элемента, кратность соответствующего узла считается равной 0.

Заключение

Обеспечение информационной безопасности КМОП СБИС в условиях ионизирующего излучения определяется конкретным спектром дерева топологии СБИС и соотношением радиационно-чувствительных параметров: кратности узлов, мощности спектра дерева, моды нечеткого числа. В этом случае соотношение между функцией распределения разброса и моды нечеткого числа определяет, в конечном итоге, целесообразность использования функционально-логических моделей радиационного поведения СБИС применительно к каждому конкретному случаю. Проведение такого сопоставления является необходимым этапом общей процедуры анализа радиационной стойкости СБИС. При этом следует отметить, что в разных диапазонах уровней или интенсивностей воздействия оценка мощности спектра дерева топологии СБИС может носить как нечеткий, так и вероятностный характер. При этом нечеткая кратность может задаваться в n-мерном пространстве с сохранением базовых параметров модели, а радиационные эффекты, возникающие в СБИС, при различных уровнях облучения, оцениваются в ней по изменению одного и того же параметра системы. Такая структура модели является вероятностно-нечеткой с операторами вероятностного типа, а критериальная функция принадлежности является суперпозицией статистической и детерминированной критериальной функцией принадлежности. При этом, определена взаимосвязь нечеткой кратности и вероятностной логик, позволяющая наиболее точно оценивать качество функционирования СБИС при воздействии радиации.

СПИСОК ЛИТЕРАТУРЫ:

1 Frank M.J. Associativity in a class of operations on spaces of distribution functions. Aeguationes Math 12 (1975), 121-144.
2 V.M. Barbashov, N.S. Trushkin Evaluation performance of digital integrated circuits while exposed to radiation. 2016 IOP Conf. Ser.: Mater. Sci. Eng. 151 012011.
3 В.М. Барбашов, Б.И. Подлепецкий, Н.С. Трушкин Моделирование радиационной надежности цифровых устройств на функционально-логическом уровне. Датчики и системы. – 2016.– №4, с. 54-57.
4 Гретцер Г. Общая теория решеток. М.: Мир, 1982. 456 с.
5 Нечеткие множества и теория возможностей. Под ред. Р.Р. Ягера. М.: Радио и связь, 1986. 408 с.
6 Нечеткие множества в моделях управления и искусственного интеллекта. Под ред. Д.А.Поспелова. М.: Наука, 1986. 312 с.
7 Денисенко В.В. Компактные модели МОП – транзисторов для SPICE в микро- и наноэлектронике.М.: ФИЗМАТЛИТ, 2010. – 408 с.
8 Барбашов В.М., Трушкин Н.С. Функционально-логическое моделирование качества функционирования ИС при воздействии радиационных и электромагнитных излучений. Микроэлектроника. 2009, том 38, № 1, с. 34-47.
9 A.V. Sogoyan, A.I. Chumakov, A.Yu. Nikiforov Method for Predicting CMOS Parameter Degradation Due to Ionizing Radiation with Regard to Operating Time and Conditions. Russian Microelectronics. 1999. V. 28. № 4. P. 224-235.
10 V. M. Barbashov, N.S. Trushkin, and O. A. Kalashnikov “Deterministic and nondeterministic failure models of LSI circuits exposed to radiation. Russian Microelectronics, vol. 44, no. 5, pp. 312-315, 2015.
11 A. V. Sogoyan, and V. A. Polunin, “A model for the formation of leakage currents in the dielectrics of MOS structures under the effect of heavy charged particles. Russian Microelectronics, vol. 44, no. 1, pp. 54-59, 2015.
12 Барбашов В.М. Моделирование функциональных отказов цифровых систем при воздействии радиации. Датчики и системы. – 2011. - № 6. – С. 29-34.

REFERENCES:

[1] Frank M.J. Associativity in a class of operations on spaces of distribution functions. Aeguationes Math 12 (1975), 121-144.
[2] V.M. Barbashov, N.S. Trushkin Evaluation performance of digital integrated circuits while exposed to radiation. 2016 IOP Conf. Ser.: Mater. Sci. Eng. 151 012011.
[3] V.M. Barbashov, B.I. Podlepetsky, N.S. Trushkin Modeling the Radiation Reliability of Digital Devices at a Functional-Logical Level. Sensors and Systems. - 2016, no. 4, pp. 54-57. (in Russian).
[4] Gratzer G. the General theory of lattices. M.: Mir, 1982. 456 p. (in Russian).
[5] Fuzzy sets and the theory of possibilities, Ed. R.R. Yager. M.: Radio and Communication, 1986, p.408. (in Russian).
[6] Fuzzy sets in control and artificial intelligence models. edited by D. A. Pospelov. M.: Nauka, 1986. 312 p. (in Russian).
[7] Denisenko V. V. Compact models of MOS - transistors for SPICE in micro - and nanoelectronics.M.: FIZMATLIT, 2010. - 408 p. (in Russian).
[8] VM Barbashov, NS Trushkin Functional-logical modeling of the quality of IS functioning under the influence of radiation and electromagnetic radiation. Microelectronics. 2009, Vol. 38, No. 1, pp. 34-47. (in Russian).
[9] A.V. Sogoyan, A.I. Chumakov, A.Yu. NikiforovMethod for Predicting CMOS Parameter Degradation Due to Ionizing Radiation with Regard to Operating Time and Conditions. Russian Microelectronics. 1999. V. 28. № 4. P. 224-235.
[10] V. M. Barbashov, N.S. Trushkin, and O. A. Kalashnikov “Deterministic and nondeterministic failure models of LSI circuits exposed to radiation. Russian Microelectronics, vol. 44, no. 5, pp. 312-315, 2015.
[11] A. V. Sogoyan, and V. A. Polunin, “A model for the formation of leakage currents in the dielectrics of MOS structures under the effect of heavy charged particles. Russian Microelectronics, vol. 44, no. 1, pp. 54-59, 2015.
[12] VM Barbashov Modeling of functional failures of digital systems under the influence of radiation. Sensors and systems. - 2011. - No. 6. - pp. 29-34. (in Russian).

Поступила в редакцию – 16 Октября 2017 г. Окончательный вариант – 05 февраля 2018 г.
Received – October 16, 2017. The final version – February 05, 2018.

Алексей А. Гавришев, Александр П. Жук
Северо-Кавказский федеральный университет,
ул. Пушкина, 1, г. Ставрополь, 355009, Россия
e-mail: alexxx.2008@inbox.ru, https://orcid.org/0000-0002-4242-6152
e-mail: alekszhuk@mail.ru, https://orcid.org/0000-0002-0168-8391

РАЗРАБОТКА БЕСПРОВОДНОЙ ИМИТОЗАЩИЩЕННОЙ СИСТЕМЫ ИДЕНТИФИКАЦИЯ И КОНТРОЛЯ ДОСТУПА ТРАНСПОРТНЫХ СРЕДСТВ

DOI: http://dx.doi.org/10.26583/bit.2018.1.04

Аннотация. В данной статье рассматриваются беспроводные системы идентификации и контроля доступа транспортных средств на охраняемые объекты. Рассмотрены известные системы. В результате установлено, что одним из перспективных подходов к идентификации и контролю доступа транспортных средств на охраняемые объекты является использование систем на основе принципа «свой-чужой». Среди данных систем выделяются «однонаправленные» и «двунаправленные» системы идентификации и контроля доступа. «Двунаправленные» системы являются более предпочтительными для вопросов идентификации и контроля доступа. Однако, в настоящее время, данные системы должны иметь уменьшенную вероятность распознавания структуры запросных и ответных сигналов в силу того, что потенциальный злоумышленник может достаточно легко выполнить несанкционированный доступ к радиоканалу системы. На основании этого разработана беспроводная система идентификации и контроля доступа транспортных средств на охраняемые объекты на основе принципа «свой-чужой», отличающаяся повышенной защищенностью от несанкционированного доступа и подавления помехами за счет использования перезаписываемых накопителей хаотических последовательностей. Дополнительно к этому предлагается использовать для идентификации транспортного средства RFID-метку, содержащую дополнительную информацию о нем. Приведены некоторые технические характеристики разработанной системы (возможный частотный диапазон запросно-ответных сигналов, дальность связи, скорость передачи данных, объем передаваемых данных, рекомендации по выбору RFID-меток). Так же, с помощью аппарата нечеткой логики, была произведена оценка защищенности от несанкционированного доступа запросно-ответных сигналов на основе системы «свой-чужой», передаваемых по радиоканалу, разработанной системы и аналогов. Оценка защищенности разработанной системы показывает достаточный уровень ее защищенности от комплексных угроз (просмотр, подмена, перехват и радиоэлектронное подавление трафика) по сравнению с известными системами данного класса. Среди основных преимуществ разработанной системы следует упомянуть повышенную защищенность от несанкционированного доступа и подавления помехами за счет использования перезаписываемых накопителей хаотических последовательностей, в которых потенциально можно использовать широкий класс хаотических сигналов. Так же следует отметить повышенную вероятность идентификации проверяемых транспортных средств за счет использования принципа «свой-чужой» и RFID-меток. Среди основных недостатков предложенной системы следует отметить необходимость наличия точной синхронизации между передающей и приемной сторонами.

Ключевые слова: идентификация, контроль доступа, транспортные средства, радиоканал, имитозащищенность, хаотические сигналы.

Для цитирования. ***ГАВРИШЕВ, Алексей А.; ЖУК, Александр П.*** *РАЗРАБОТКА БЕСПРОВОДНОЙ ИМИТОЗАЩИЩЕННОЙ СИСТЕМЫ ИДЕНТИФИКАЦИЯ И КОНТРОЛЯ ДОСТУПА ТРАНСПОРТНЫХ СРЕДСТВ. Безопасность информационных технологий, [S.l.], v. 25, n. 1, p. 41-51, 2018. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1092>. Дата доступа: 14 feb. 2018. doi:http://dx.doi.org/10.26583/bit.2018.1.04.*

Aleksei A. Gavrishev, Aleksandr P. Zhuk
North Caucasus Federal University,
Pushkin St., 1, Stavropol, 355009, Russia
e-mail: alexxx.2008@inbox.ru, https://orcid.org/0000-0002-4242-6152
e-mail: alekszhuk@mail.ru, https://orcid.org/0000-0002-0168-8391

Development of a wireless protection against imitation system for identification and control of vehicle access

DOI: http://dx.doi.org/10.26583/bit.2018.1.04

Abstract. This article deals with wireless systems for identification and control of vehicle access to protected objects. Known systems are considered. As a result, it has been established that one of the most promising approaches to identifying and controlling vehicle access to protected objects is the use of systems based on the "friend or foe" principle. Among these systems, there are "one-directional" and "bedirectional" identification and access control systems. "Bidirectional" systems are more preferable for questions of identification and access control. However, at present, these systems should have a reduced probability of recognizing the structure of the request and response signals because the potential attacker can easily perform unauthorized access to the radio channel of the system. On this basis, developed a wireless system identification and control vehicle access to protected objects based on the principle of "friend or foe", featuring increased protection from unauthorized access and jamming through the use of rewritable drives chaotic sequences. In addition, it's proposed to use to identify the vehicle's RFID tag containing additional information about it. Are some specifications of the developed system (the possible frequency range of the request-response signals, the communication range, data rate, the size of the transmitted data, guidelines for choosing RFID). Also, with the help of fuzzy logic, was made the security assessment from unauthorized access request-response signals based on the system of "friend or foe", which are transferred via radio channel, developed systems and analogues. The security assessment of the developed system shows an adequate degree of protection against complex threats (view, spoofing, interception and jamming of traffic) in comparison with known systems of this class. Among the main advantages of the developed system it's necessary to mention increased security from unauthorized access and jamming through the use of rewritable drives chaotic sequences, in which you can potentially use a wide class of chaotic signals. It should also be noted the increased likelihood of identification check the vehicle through the use of the principle of "friend or foe" and RFID. Among the main disadvantages of the proposed system it should be noted the need for precise synchronization between transmitting and receiving sides.

Keywords: identification, access control, vehicles, radio channel, protection against imitation, chaotic signals.

For citation. ***GAVRISHEV, Aleksei A.; ZHUK, Aleksandr P.*** *Development of a wireless protection against imitation system for identification and control of vehicle access. IT Security (Russia), [S.l.], v. 25, n. 1, p. 41-51, 2018. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1092>. Date accessed: 14 feb. 2018. doi:http://dx.doi.org/10.26583/bit.2018.1.04.*

Введение

В настоящее время для охраны и защиты различных важных объектов и людей применяются различные системы безопасности. В последнее время большое развитие получили беспроводные системы безопасности. Целесообразность использования радиоканала в системах безопасности объясняется несколькими факторами [1, 2], среди которых выделяют простоту организации, меньшие затраты на построение и эксплуатацию, возможность применения при отсутствии проводных линий связи и в чрезвычайных ситуациях, возможность оперативного изменения структуры и параметров систем при наращивании объектов охраны.

Одной из самых распространенных беспроводных систем безопасности в настоящее время являются системы автомобильной безопасности. Среди областей ее применения

можно выделить, например, охрану транспортных средств (ТС) от угонов [3], идентификацию и контроль доступа ТС на охраняемые объекты [4]. Разработка новых методов и технологий идентификации и контроля доступа ТС на охраняемые объекты является актуальной задачей [4].

Целью данной статьи является разработка беспроводной имитозащищенной системы идентификации и контроля доступа транспортных средств на охраняемые объекты на основе принципа «свой-чужой».

Основная часть

Анализ предметной области

Как известно [5], на любом важном охраняемом объекте обычно присутствует внутренняя зона, территория объекта, а также проходная для ТС (легковые и грузовые автомобили, специальная и военная техника и т.д.) и персонала. С целью исключить несанкционированный доступ на территорию объекта, предотвращения терактов и прочее, проходная для ТС обычно ограждается с помощью различных инженерных сооружений, например, заграждения (заборы, шлагбаумы, ворота), противотаранные заграждения (надолбы, металлические ежи, бетонные блоки) и т.д. [6].

В настоящее время интерес представляют автоматизированные системы контроля доступа, которые могут провести дистанционную идентификацию и контроль доступа людей и ТС [5]. Остановимся подробнее на известных методах и технологиях идентификации и контроля доступа ТС. Так в работе [7] описываются известные системы идентификации и контроля доступа ТС: антитеррористическая система контроля доступа и въезда на социально-значимые объекты «Барьер», автоматизированная система контроля подъездных путей к охраняемым объектам «Блокхост-КСКПП», а также система контроля доступа ТС (Полезная модель РФ № 144117, опубл. 10.08.2014). Среди их основных недостатков отмечается тот факт, что функция автоматического распознавания регистрационных номеров не дает 100 % вероятности распознавания, и нет возможности отличить поддельные номера [7]. Кроме того, отмечается, что применяемые в них типы заграждений не являются достаточной защитой от несанкционированного доступа. Так же следует отметить, что, как в данных системах, так и в аналогичных системах, предусмотрена возможность исключительно ручного контроля проезжающих ТС, однако это не является удачным вариантом [4].

Другим примером системы идентификации и контроля доступа ТС является использование каких-либо уникальных идентификаторов, например, систем на основе принципа «свой-чужой». Примером использования уникальных идентификаторов является система контроля проезда автомобилей [8]. В ее основу положено использование RFID-меток (далее «Т1»). Для RFID-меток можно предусмотреть защиту от клонирования, а также криптографическую защиту передаваемой информации. Принцип функционирования системы прост [8]: при обнаружении метки считыватель сопоставляет её данные с внутренней таблицей доступа и после этого системой принимается решение о допуске/не допуске ТС на охраняемую территорию. Так же в работе [4] предлагается многоэтапная радиочастотная идентификация ТС, заключающаяся в разделении уникальных идентификационных данных (далее «Т2»). Так на первом этапе информационного обмена между меткой и считывателем запрашивается государственный регистрационный номер ТС, высота ТС и т.д. (этот процесс идет без шифрования). Затем по дополнительному запросу выдаются специальные регистрационные, конструкторские или технологические данные (в этом случае требуется шифрование с минимальной криптографической стойкостью). После этого по специальному запросу должны выдаваться наиболее секретные данные о ТС, а также его VIN (идентификационный номер транспортного средства). В этом случае необходимо шифрование с максимальной криптографической стойкостью.

Пример технологии на основе принципа «свой-чужой» приведен так же в работе [9]. Отличительной чертой данного подхода является использование в стационарном блоке управления и в мобильном брелоке управления одинаковых генераторов псевдослучайных последовательностей (ПСП), которые инициализируются общим генератором случайных чисел, находящимся в стационарном блоке управления (далее «Т3»). Таким образом, в случае легального пользователя оба генератора ПСП должны выдать одинаковые последовательности и, наоборот, в случае нелегального пользователя, выдать различные последовательности, о чем будет выдано уведомление. Данная технология хоть и заточена для охраны автомобилей от несанкционированного доступа, однако легко может быть перенесена на случай систем идентификации и контроля доступа ТС.

Так же известна система, в которой, среди прочего, применяются радиочастотные метки (содержат уникальные идентификаторы транспортного средства), сканирующее устройство и сложные сигналы с фазовой модуляцией (ФМС) [10]. Уникальные идентификаторы ТС вносятся в базу данных и могут легко быть считаны сканирующим устройством с радиочастотных меток через защищенный от несанкционированного доступа радиоканал (далее «Т4»). В качестве дополнительного уникального идентификатора может использоваться несмываемый тайнописный краситель (например, на ветровом стекле), обнаруживаемый в ультрафиолетовых лучах.

Далее рассмотрим систему автомобильной сигнализации, предложенную в работе [11]. В ней предлагается использовать автокорреляционную широкополосную систему связи на основе модуляции фазы передаваемого сигнала. Данная система позволяет значительно повысить защищенность от несанкционированного доступа. При соответствующей адаптации данная технология может найти применение для систем идентификации и контроля доступа ТС (далее «Т5»).

Как видно из приведенного анализа, одним из самых перспективных подходов к идентификации и контролю доступа ТС на охраняемую территорию является использование систем на основе принципа «свой-чужой». Здесь следует отметить, что система на основе принципа «свой-чужой» может быть как «однонаправленная», когда уникальный идентификатор передается на блок контроля и сравнивается с эталонным списком, например, [8], так и «двунаправленная», когда присутствуют как запросные, так и ответные сигналы [9]. Второй вид системы на основе принципа «свой-чужой» является более предпочтительным для вопросов идентификации и контроля доступа ТС [4, 9]. Однако, в настоящее время отмечается, что такие «двунаправленные» системы на основе принципа «свой-чужой» должны иметь уменьшенную вероятность распознавания структуры запросных и ответных сигналов злоумышленником за счет высокой скрытности структуры передаваемой информации [12]. Это следует из того, что в настоящее время достаточно легко выполнить несанкционированный доступ к радиоканалу систем безопасности для злоумышленных действий (например, просмотр, подмена, перехват и подавление помехами) [13]. Методами защиты от данных угроз в беспроводных системах автомобильной безопасности потенциально могут стать криптографические методы защиты информации (КМЗИ) [3, 13], а также технологии на основе шумоподобных сигналов (ШПС) [3, 13].

Одним из самых перспективных методов одновременной защиты радиоканала от несанкционированного доступа (просмотр, подмена, перехват) и подавления помехами в системах автомобильной безопасности в настоящее время могут стать технологии на основе шумоподобных сигналов, например, использование хаотических сигналов (ХС) [3, 13, 14]. Так в работе [14] рассматривается использование сверхширокополосных сигналов на основе хаотических сигналов в системе автомобильной безопасности, в частности сигнализация, идентификация и т.д. (далее «Т6»). Отмечается, что сигналы данного вида обеспечивают защиту от помех и повышенную защищенность от несанкционированного доступа [14]. В частности, известно [15], что ХС позволяют добиться повышенной защищённости от несанкционированного доступа за счёт повышенной структурной скрытности по сравнению с «классическими» видами ШПС. Так структурная скрытность

«классических» видов ШПС сначала увеличивается, а потом, по мере увеличения базы, уменьшается, в то время, как структурная скрытность ХС быстро возрастает [15].

Разработаем на основе хаотических сигналов беспроводную имитозащищенную систему идентификации и контроля доступа ТС на охраняемые объекты на основе принципа «свой-чужой» (далее «Т7»).

Разработка беспроводной имитозащищенной системы идентификации и контроля доступа транспортных средств на охраняемые объекты

Для этих целей рассмотрим рис. 1, на котором приведена структурная схема устройства имитозащиты контролируемых объектов с повышенной структурной скрытностью сигналов-переносчиков [16]. Данная технология предназначена для защиты информационного обмена между блоком контроля и оконечными датчиками в охранно-пожарных системах за счет использования перезаписываемых накопителей хаотических последовательностей [17]. Концептуально данное устройство имитозащиты контролируемых объектов состоит из блока контроля, включающего в себя генератор первой псевдослучайной последовательности (ПСП-1), генератор второй псевдослучайной последовательности (ПСП-2), накопитель хаотической последовательности (НХП), накопитель копии хаотической последовательности (НКХП), устройство сравнения (УС) и контролируемого объекта (датчика), включающего в себя генератор ПСП-2, НХП, НКХП [16].

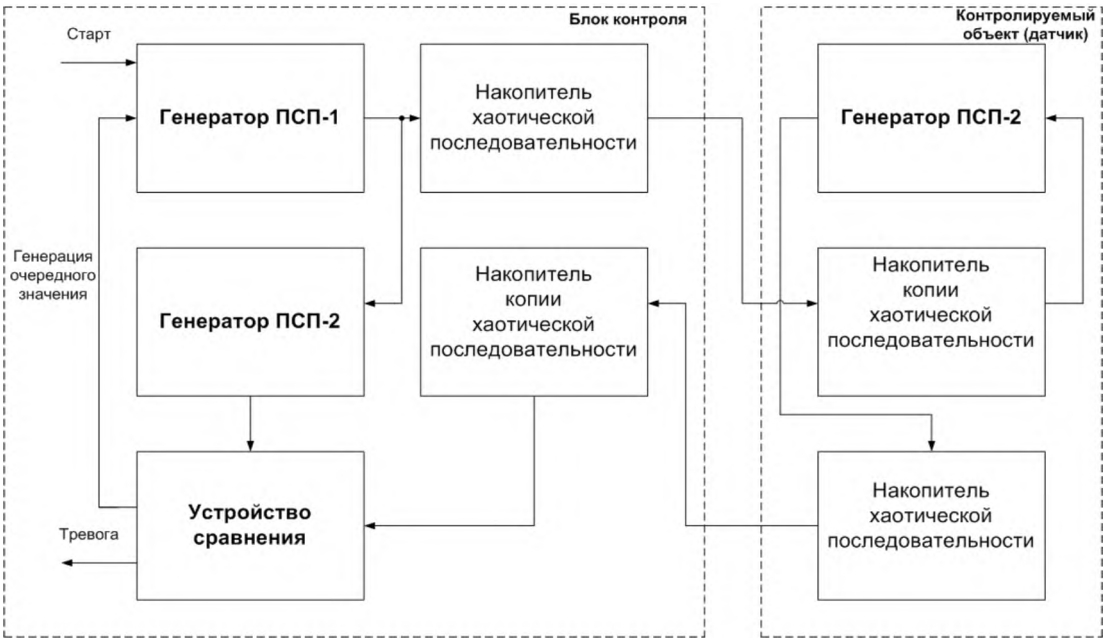

Рис.1. Структурная схема устройства имитозащиты контролируемых объектов с повышенной структурной скрытностью сигналов-переносчиков
(Fig. 1. Block diagram of apparatus for protection against imitation of controlled objects with high structural security of carrier signals)

Рассматриваемое устройство имитозащиты контролируемых объектов функционирует следующим образом [16]. Для запуска блока контроля на вход генератора ПСП-1 подаётся стартовая команда. Затем генератор ПСП-1 вырабатывает первую ПСП. Полученное значение отправляется на генератор ПСП-2 блока контроля и одновременно с этим в НХП перемножается с ХС и, после вхождения в режим синхронизации, через линию связи передается на контролируемый объект (датчик). После этого в НКХП происходит декодирование полученного сигнала с помощью копии ХС, идентичной ХС в блоке контроля, и далее декодированный сигнал в виде последовательности поступает в генератор ПСП-2, функция генерации последовательности которого идентична функции генератора ПСП-2 блока контроля. Затем в НХП происходит перемножение

последовательности ПСП-2 контролируемого объекта (датчика) с ХС и, после вхождения в режим синхронизации, через линию связи передаётся на блок контроля. Далее в НКХП происходит декодирование полученного сигнала с помощью копии ХС, идентичной ХС в контролируемом объекте (датчике), и после чего декодированный сигнал в виде последовательности поступает на УС, в котором проверяется отклик ранее пришедшего значения генератора ПСП-2 блока контроля и отклик генератора ПСП-2 контролируемого объекта (датчика). В случае совпадения значений, пришедших от контролируемого объекта (датчика) и блока контроля, вырабатывается сигнал «Норма», который служит для генерации следующего псевдослучайного числа генератором ПСП-1. При несовпадении значений, устройство сравнения выдает команду «Тревога».

Отдельно отметим, что более подробное описание данного подхода, в том числе, подробное описание процесса умножения информационного сигнала на ХС на передающей стороне и его восстановление на приемной стороне, приведено в работе [17].

Используем данный подход для разработки беспроводной имитозащищенной системы идентификации и контроля доступа ТС на охраняемые объекты на основе принципа «свой-чужой». Для этого воспользуемся структурной схемой (рис. 1) с изменениями и уточнениями: правую часть вместо «контролируемого объекта (датчика)» обозначим как «транспортное средство». Кроме того, заметим, что ТС так же должно иметь RFID-метку (например, на ветровом стекле), в которой должна содержаться некоторая секретная информация о ТС, например, его VIN (идентификационный номер транспортного средства). Она служит для дополнительной идентификации ТС. Так же в перезаписываемых накопителях (перезаписываемые запоминающие устройства) ТС и блока контроля должны быть записаны одинаковые наборы хаотических последовательностей (при необходимости они могут периодически перезаписываться на новые последовательности [17; 18]).

Таким образом, при въезде/выезде ТС на территорию охраняемого объекта в автономном режиме, оно находится на некотором расстоянии перед внешними воротами шлюза (для упрощения на рис. не показано). В данном варианте исполнения шлюз оборудован управляемыми преградами, выполненными в виде ворот (для упрощения на рис. не показано). Исходное состояние – внешние ворота закрыты. Могут гореть красные светофоры, запрещающие движение [7]. После этого, блок контроля вырабатывает первую ПСП, которую одновременно отправляет в свой генератор ПСП-2 и в НХП, где она перемножается с ХС, и при вхождении в режим синхронизации, отправляется в ТС. Далее ТС декодирует переданный сигнал с помощью НКХП и вырабатывает свою вторую ПСП, которая перемножается с ХС в НХП, и при вхождении в режим синхронизации, отправляется в блок контроля. Блок контроля декодирует ее в НКХП и отправляет в свое устройство сравнения, в которое так же должна прийти ранее им выработанная вторая ПСП. Таким образом, в устройстве сравнения блока контроля сравниваются вторая ПСП ТС и вторая ПСП блока контроля (рис. 1). В случае верного сравнения блоком контроля дается команда на генерацию нового значения первой ПСП (для следующего случая въезда/выезда), открываются внешние ворота, и ТС может въехать в шлюз. В этом случае могут гореть зеленые сигналы светофора, разрешающие въезд [7]. Затем внешние ворота за ТС закрываются. В случае неверного сравнения или невозможности войти в режим синхронизации ворота не открываются (дальнейшие действия зависят от должностных лиц). После этого, в шлюзе считыватель должен считать информацию с RFID-метки ТС и сравнить полученную информацию (VIN ТС) с таблицей доступа (для упрощения на рис. не показано). В случае совпадения VIN ТС с таблицей доступа, открываются внутренние ворота, и ТС может въехать на охраняемую территорию. В случае несовпадения VIN ТС с таблицей доступа, внутренние ворота не открываются (дальнейшие действия зависят от должностных лиц). Так же возможно предусмотреть процедуру досмотра ТС, а также его видеосъемку: в таком случае открытие внутренних ворот будет определяться должностными лицами в ручном режиме. Процедура выезда с территории объекта

аналогична процедуре въезда. Для упрощения процедуры выезда можно предусмотреть выезд с территории объекта исключительно с помощью RFID-метки.

Рассмотрим некоторые технические характеристики разработанной системы идентификации и контроля ТС. К одной из основных характеристик таких систем относится частотный диапазон запросно-ответных сигналов. В настоящее время в России для беспроводных систем безопасности самыми распространенными не лицензируемыми диапазонами частот являются 2,4 ГГц, 433 МГц, 868 МГц [19]. Как известно [19], в диапазоне 2,4 ГГц работают такие известные популярные стандарты связи, как Bluetooth, Wi-Fi и ZigBee, что очень сильно зашумляет эфир. Основными характеристиками диапазона 2,4 ГГц являются относительно большая скорость передачи данных (до десятков Мбит/с), малая дальность связи (до 100 м) и отсутствие способности волны огибать препятствия [19]. Субгигагерцевые диапазоны 433 МГц и 868 МГц, по сравнению с диапазоном 2,4 ГГц, обладают следующими характеристиками: обеспечивают приемлемую дальность связи (до 1000 м), обладают пониженным энергопотреблением, способностью волны огибать препятствия (дифракция), скоростью передачи данных свыше 200 Кбит/с [19]. Одним из главных условий их использования, является соответствие радиопередающих устройств техническим требованиям, утвержденным решением Государственной комиссии по радиочастотам [20]. Поэтому в разработанной системе идентификации и контроля ТС, в силу функционирования, в том числе, и на открытой местности, а также необходимости удаленной идентификации ТС, предлагается использовать субгигагерцевые диапазоны.

Другим важным вопросом является объем передаваемых данных между ТС и блоком контроля. Так как в данной системе идентификации и контроля доступа ТС не передаются «тяжелые» данные (например, видеоизображения), а также нет постоянного непрерывного радиообмена, то объем передаваемых данных будет незначительным. Для рассматриваемых условий можно предположить, что длина используемой ПСП будет равна 128 бит, такую же длину будет иметь ХС, с которым ПСП перемножается. Дополнительно к этому, для различных служебных данных, можно предусмотреть несколько 8-битных полей. В этом случае длина ХС будет чуть больше. В итоге, общий объем передаваемых данных между ТС и блоком контроля не будет выходить за значения максимальной скорости передаваемых данных, которая определена для субгигагерцевых диапазонов (200 Кбит/с).

Среди основных технических недостатков разработанной системы следует отметить необходимость наличия точной синхронизации между передающей и приемной сторонами. Поэтому для создания точной синхронизации в системах данного класса целесообразно использовать внешние средства, например, на основе концепции программно-конфигурируемого радио [18].

Далее рассмотрим требования к RFID-метке, служащую в качестве дополнительного метода идентификации ТС. В качестве RFID-метки можно применять, например, пассивные метки (без питания и аккумуляторов), содержащие только уникальный идентификационный номер и функционирующие только на малом расстоянии от считывателя [8], или применять более сложные радиочастотные метки, например, на основе сложных сигналов с фазовой модуляцией [10]. Их частотный диапазон может быть разнообразными, например, 13,553-13,567 МГц (нелицензируемый диапазон частот) или 866-868 МГц (лицензируемый диапазон частот) [20].

Далее проведем оценку защищенности рассмотренных систем идентификации и контроля доступа ТС от комплексных угроз (просмотр, подмена, перехват и подавление помехами), применяемых одновременно. Оценку защищенности будет проводить для запросно-ответных сигналов на основе системы «свой-чужой», передаваемых по радиоканалу. В случае разработанной системы, оценку защищенности проведем для этапа, когда ТС находится перед воротами. Оценку защищенности проведем на основе методики, изложенной в работе [21]. Ее основные этапы изложены ниже:

1) задание кортежа «*Параметры ИБ АвС*»={*At*, *P*}, где «*At*» – уровень атаки, «*P*» – уровень защиты;

2) преобразование нечетких значений переменных «очень низкий», «низкий», «средний», «высокий», «очень высокий» в числовые значения [1, 5];

3) задание важности инцидента ИБ $I_{АвС} = k(m) \times At \times P$;

4) задание численной оценки защищенности радиоканала сигнализации в целом $P_{АвС} = 1 - I_{АвС}$;

5) вычисление обобщенных показателей уровня атаки $At_O = \sum_{i=1}^{n} A_i$ и уровня защиты $P_O = \sum_{i=1}^{n} P_i$;

6) вычисление коэффициента нормирования *k(m)*;

7) вычисление оценки защищенности $P_{АвС} = 1 - k(m) \times At_O \times P_O$;

8) перевод количественной оценки в качественную оценку с помощью таблицы сопоставления.

Более подробно с данной методикой оценки защищенности, в том числе с начальными условиями, примерами расчетов, таблицей перевода количественных оценок защищенности в качественные, можно ознакомиться в работах [13, 21].

Проведем необходимые подготовительные вычисления (таблица 1). Условимся [13], что угроза «просмотр» обозначается как «У1», угроза «подмена» – как «У2», угроза «перехват» – как «У3», угроза «подавление помехами» – как «У4».

В таблице 2 приведен ранжированный список количественных и качественных оценок защищенности беспроводных систем идентификации и контроля доступа ТС, описанных в данной статье. Анализ таблицы 2 показывает, что наиболее защищенными запросно-ответными сигналами в системах идентификации и контроля доступа ТС обладают технологии на основе хаотических сигналов, а наименее защищенными – технологии на основе КМЗИ.

Таблица 1. Результаты подготовительных расчетов

Угрозы	*P*-уровень защиты							*At*-уровень атаки						
	T1	*T2*	*T3*	*T4*	*T5*	*T6*	*T7*	*T1*	*T2*	*T3*	*T4*	*T5*	*T6*	*T7*
У1	3	3	5	3	3	2	2	4	4	5	4	4	4	4
У2	3	3	2	2	2	2	2	4	4	4	4	4	4	4
У3	5	5	5	3	3	2	2	5	5	5	5	5	4	4
У4	5	5	5	3	3	2	2	5	5	5	5	5	4	4

Таблица 2. Количественные и качественные оценки защищенности

№	Устройство (способ)	Метод защиты радиоканала	Количественная оценка защищенности	Качественная оценка защищенности
1	Т7	ШПС (ХС)	0,6800	Высокая
2	Т6	ШПС (ХС)	0,6800	Высокая
3	Т5	ШПС (ФМС)	0,5050	Средняя
4	Т4	ШПС (ФМС)	0,5050	Средняя
5	Т2	КМЗИ	0,2800	Низкая
6	Т1	КМЗИ	0,2800	Низкая
7	Т3	КМЗИ	0,1925	Очень низкая

Заключение

Таким образом, в данной работе проведен анализ известных систем идентификации и контроля доступа ТС на охраняемый объект. Установлено, что одним из самых

предпочтительных вариантов реализации данных систем является использование «двунаправленных» систем на основе принципа «свой-чужой». Однако, в настоящее время отмечается, что такие «двунаправленные» системы на основе принципа «свой-чужой» должны иметь уменьшенную вероятность распознавания структуры запросных и ответных сигналов злоумышленником за счет высокой скрытности структуры передаваемой информации [12]. Это следует из того, что в настоящее время достаточно легко выполнить несанкционированный доступ к радиоканалу систем безопасности для злоумышленных действий (например, просмотр, подмена, перехват и радиоэлектронное подавление передаваемых по радиоканалу данных) [13]. В качестве возможного метода защиты от данных угроз рассматриваются технологии на основе шумоподобных сигналов, а именно – хаотические сигналы [3, 13, 14].

На основании этого была разработана беспроводная имитозащищенная система идентификации и контроля доступа транспортных средств на охраняемые объекты на основе принципа «свой-чужой», отличающаяся повышенной защищенностью от несанкционированного доступа и подавления помехами за счет использования перезаписываемых накопителей хаотических последовательностей. Дополнительно к этому предлагается использовать для идентификации ТС RFID-метку, содержащую VIN ТС.

Были приведены некоторые технические характеристики разработанной системы (возможный частотный диапазон запросно-ответных сигналов, дальность связи, скорость передачи данных, объем передаваемых данных, рекомендации по выбору RFID-меток).

Так же, с помощью аппарата нечеткой логики [21], была произведена оценка защищенности от несанкционированного доступа запросно-ответных сигналов на основе системы «свой-чужой», передаваемых по радиоканалу, разработанной системы и аналогов. Оценка защищенности разработанной системы показывает ее достаточный уровень защищенности от комплексных угроз (просмотр, подмена, перехват и радиоэлектронное подавление трафика) по сравнению с известными системами данного класса.

Среди основных преимуществ разработанной системы следует упомянуть повышенную защищенность от несанкционированного доступа и подавления помехами за счет использования перезаписываемых накопителей хаотических последовательностей, в которых потенциально можно использовать широкий класс хаотических сигналов. Так же следует отметить повышенную вероятность идентификации проверяемых транспортных средств за счет использования принципа «свой-чужой» и RFID-меток. Среди основных недостатков предложенной системы следует отметить необходимость наличия точной синхронизации между передающей и приемной сторонами. Для ее создания в системах данного класса предложено использовать внешние средства, например, на основе концепции программно-конфигурируемого радио [18].

СПИСОК ЛИТЕРАТУРЫ:

1 Эсауленко А. В. Моделирование и обеспечение надежности радиоканала в системах безопасности: автореферат дисс. канд. тех. наук. Воронеж. 2015. 19 с.
2 Драгун С. Организация беспроводных охранно-пожарных систем на базе радиосистемы «Стрелец» Технологии безопасности. 2011. № 6. С. 14-15.
3 Жук А. П., Гавришев А. А., Осипов Д. Л., Бурмистров В. А. Анализ методов защиты беспроводных каналов связи автомобильных сигнализаций от несанкционированного доступа Интернет-журнал «Технологии техносферной безопасности». 2016. № 5 (69). С. 173-177.
4 Пономарев В. А., Мороз С. М. Обоснование применения радиочастотной идентификации транспортных средств Журнал автомобильных инженеров. 2017. № 1(102). С. 32-36.
5 Бондарев П. В., Измайлов А. В., Толстой А. И. Физическая защита ядерных объектов: Учебное пособие для вузов. М.: МИФИ, 2008. 584 с.
6 Тарасов Р. А., Упрунина А. А. Основы профессиональной деятельности: учебное пособие для самостоятельной подготовки слушателей. Волжский: ФКОУ ДПО МУЦ УФСИН России по Волгоградской области. 2014. 76 с.
7 Полевой В. Г., Грачев С. Н. Григорьев С. А. Система автоматизированного управления пропуском транспорта Патент РФ № 2610925. 2017. 11 С.

8 Автономная система контроля и управления проездом автомобилей URL: http://www.isbc-rfid.ru/_solutions/id_9/ (дата обращения: 28.11.2017).
9 Гавришев А. А., Бурмистров В. А., Анзин И. В. К вопросу об использовании псевдослучайных последовательностей для предотвращения несанкционированного доступа к радиоканалу автомобильной сигнализации Новые информационные технологии и системы: сб. науч. ст. XI Междунар. науч.-техн. конф. Пенза: изд-во ПГУ. 2014. С. 270-272.
10 Дикарев В. И., Шубарев В. А., Калинин В. А., Мельников В. А. Способ маркировки автотранспорта Патент РФ № 2464644. 2012. 8 С.
11 Фролов В. Я., Ковтунов Ю. А., Кубата В. Г. Методы обеспечения помехоустойчивости при управлении автомобильной противоугонной сигнализацией Автомобильный транспорт. 2013. Вып. 33. С. 105-109.
12 Бельтов А. Г., Попов А. Р., Жуков И. Ю., Левицкий Н. Е. Способ передачи информации шумоподобными сигналами в системе опознавания «свой-чужой» Патент РФ № 2532085. 2014. 12 С.
13 Гавришев А. А., Жук А. П., Осипов Д. Л. Анализ технологий защиты радиоканала охранно-пожарных сигнализаций от несанкционированного доступа Труды СПИИРАН. 2016. Вып. 4(47). С. 28-45.
14 Мохсени Т. И., Рыжов А. И., Лазарев В. А. Эксперименты по применению СШП средств связи в автомобиле Труды 55-й научной конференции МФТИ. Радиотехника и кибернетика. Том 2. М.: МФТИ. 2012. С. 103.
15 Сиващенко С. И. Скрытность радиосистем со сложными и хаотическими сигналами Системи управління, навігації та зв'язку. 2009. № 3(11). С. 56-58.
16 Жук А. П., Гавришев А. А. Альтернативный подход повышения структурной скрытности сигналов-переносчиков устройства имитозащиты контролируемых объектов Спецтехника и связь. 2015. № 2. С. 59-63.
17 Осипов Д. Л., Жук А. П., Гавришев А. А. Устройство имитозащиты контролируемых объектов с повышенной структурной скрытностью сигналов-переносчиков Патент РФ № 2560824. 2015. 15 с.
18 Мохсени Т. И., Кикот А. М. Когерентная передача цифровой информации с двоичной модуляцией хаотического импульса Журнал радиоэлектроники. 2015. № 6. 24 с.
19 Пушкарев О. Использование диапазонов 433 И 868 МГц в системах промышленной телеметрии Беспроводные технологии. 2012. № 2. С. 42-48.
20 Решение ГКРЧ при Мининформсвязи России от 07.05.2007 N 07-20-03-001 (ред. от 04.07.2017) «О выделении полос радиочастот устройствам малого радиуса действия». 2007. 35 с.
21 Гавришев А. А., Бурмистров В. А., Осипов Д. Л. Оценка защищенности беспроводной сигнализации от несанкционированного доступа на основе понятий нечеткой логики Прикладная информатика. 2015. Т. 10. № 4(58). С. 62–69.

REFERENCES:

[1] Jesaulenko A. V. Modelirovanie i obespechenie nadezhnosti radiokanala v sistemah bezopasnosti [Modeling and ensure the reliability of the radio channel security systems]. Ph.D. Thesis. Voronezh Institute of the Ministry of Interior of Russia. Voronezh. Russia. 2015. 19 p. (in Russian).
[2] Dragun S. Organizacija besprovodnyh ohranno-pozharnyh sistem na baze radiosistemy «Strelec» [Organization of wireless fire and security systems based on radio systems «Strelec»]. Tehnologii bezopasnosti. 2011, no. 6, pp. 14–15. (in Russian).
[3] Zhuk A. P., Gavrishev A. A., Osipov D. L., Burmistrov V. A. Analysis of methods of protection of wireless communication channels of car alarm systems from unauthorized access. Tehnologii tehnosfernoj bezopasnosti – Technology of technosphere safety. 2016, no. 5 (69), pp. 173-177. (in Russian).
[4] Ponomarev V. A., Moroz S. M. Obosnovanie primenenija radiochastotnoj identifikacii transportnyh sredstv [The rationale for the use of radio frequency identification of vehicles]. Zurnal AAI. 2017, no. 1(102), pp. 32-36. (in Russian).
[5] Bondarev P. V., Izmajlov A. V., Tolstoj A. I. Fizicheskaja zashhita jadernyh ob'ektov: Uchebnoe posobie dlja vuzov [Physical protection of nuclear facilities: textbook]. Moscow. MIFI Publ. 2008, 584 p. (in Russian).
[6] Tarasov R. A., Uprunina A. A. Osnovy professional'noj dejatel'nosti: uchebnoe posobie dlja samostojatel'noj podgotovki slushatelej [Fundamentals of professional activity: teaching aid for independent preparation of students.]. Volzhskij. FSE IAPE "Interregional training centre of the Department of Federal service of execution of punishments across the Volgograd region". 2014. 76 p. (in Russian).
[7] Grigorev S. A., Grachev S. N., Polevoj V. G. Transport passage automated control system. Patent RF, no. 2610925, 2017, 11 p. (in Russian).
[8] Avtonomnaja sistema kontrolja i upravlenija proezdom avtomobilej [Autonomous system of control and management of passing cars]. URL: http://www.isbc-rfid.ru/_solutions/id_9/ (access: 28.11.2017) (in Russian).
[9] Gavrishev A. A., Burmistrov V. A., Anzin I. V. K voprosu ob ispol'zovanii psevdosluchainykh posledovatel'nostei dlya predotvrashcheniya nesanktsionirovannogo dostupa k radiokanalu avtomobil'noi signalizatsii [To question about the use of pseudo-random sequences to prevent unauthorized access to the radio car alarm]. Sbornik nauch-nykh statei XI Mezhdunarodnoi nauchno-tekhniches-koi konferentsii «Novye informatsionnye tekhnologii i sistemy» [Proceeding of the Eleventh International Conference of Science and Technology «New information technology and systems» (2014, Penza, Russia)]. Penza, PGU Publ., 2014, pp. 270-272. (in Russian).

[10] Dikarev V. I., Shubarev V. A., Kalinin V. A., Mel'nikov V. A. Method of labelling vehicles. Patent RF, no. 2464644, 2012, 8 p. (in Russian).
[11] Frolov V., Kovtunov J., Kubata V. Methods of providing noise immunity in automobile anti-theft system control. Road transport. 2013, i. 33, pp. 105-109. (in Ukrainian).
[12] Bel'tov A. G., Popov A. R., Zhukov I. J., Levitskij N. E. Method to transmit information by noise-like signals in friend-or-foe detection system. Patent RF, no. 2532085, 2014, 8 p. (in Russian).
[13] Gavrishev A. A., Zhuk A. P., Osipov D. L. Analysis of protection technologies radio fire alarm systems against unauthorized access. SPIIRAS Proceedings. 2016, i. 4(47), pp. 28-45. (in Russian).
[14] Mohseni T. I., Ryzhov A. I., Lazarev V. A. Jeksperimenty po primeneniju SShP sredstv svjazi v avtomobile [Experiments on the use of UWB communications in the car]. Trudy 55-j nauchnoj konferencii MFTI. Radiotehnika i kibernetika [Proceedings of the 55th scientific conference of MIPT. Radio engineering and Cybernetics]. V. 2. Moscow. MIPT Publ. 2012, P. 103. (in Russian).
[15] Sivashchenko S. I. Secrecy of radio system with difficult and chaotic signals. Systemy upravlinnja, navigacii' ta zv'jazku – Systems of control, navigation and communication. 2009, v. 3(11), pp. 56–58 (in Russian).
[16] Zhuk A. P., Gavrishev A. A. Alternative approach of increased structural stealth signal-carrying device simulation protection of the controlled objects. Spetstekhnika i svyaz' – Specialized machinery and communication. 2015, v. 2, pp. 59–63. (in Russian).
[17] Osipov D. L., Zhuk A.P., Gavrishev A. A. Apparatus for protection against imitation of controlled objects with high structural security of carrier signals. Patent RF, no. 2560824, 2015, 15 p. (in Russian).
[18] Mohseni T. I., Kikot A. M. Kogerentnaya peredacha tsifrovoi informatsii s dvoichnoi modulyatsiei khaoticheskogo impul'sa [Coherent transfer of digital information with binary modulation of the chaotic pulse]. Zhurnal radioelektroniki. 2015, no. 6, 24 p. (in Russian).
[19] Pushkarev O. Ispol'zovanie diapazonov 433 I 868 MGc v sistemah promyshlennoj telemetrii [The use of ranges 433 And 868 MHz systems industrial telemetry]. Wireless Technologies. 2012, no. 2, pp. 42-48. (in Russian).
[20] Reshenie GKRCh pri Mininformsvjazi Rossii N 07-20-03-001 (red. ot 04.07.2017) «O vydelenii polos radiochastot ustrojstvam malogo radiusa dejstvija» [The decision of SCRF the Ministry of communications of Russia No. 07-20-03-001 (ed. by 04.07.2017) "On the allocation of radio frequencies to devices of small radius of action"]. 2007, 35 p. (in Russian).
[21] Gavrishev A. A., Burmistrov V. A., Osipov D. L. Assessment the security of wireless alarm from unauthorized access based on the concepts of fuzzy logic. Prikladnaya informatika – Journal of Applied Informatics. 2015, v. 10, no. 4(58), pp. 62–69. (in Russian).

Поступила в редакцию – 01 декабря 2017 г. Окончательный вариант –05 февраля2018 г.
Received – December 01, 2017. The final version – February 05, 2018.

Ксения Г. Сизова[1], Петр К. Скоробогатов[2], Максим О. Прыгунов[3]
[1]Общество с ограниченной ответственностью «НПЦ «Топаз»,
Учительская улица, 23, литера А, оф. 533, г. Санкт-Петербург, 195269, Россия
e-mail: ksizova@microtopaz.ru, https://orcid.org/0000-0003-0922-3430
[2]Национальный исследовательский ядерный университет «МИФИ»,
Каширское шоссе, 31, г. Москва, 115409, Россия
e-mail: pkskor@spels.ru, https://orcid.org/0000-0002-3146-0304
[3]Общество с ограниченной ответственностью «О2 Световые Системы»,
Новорощинская улица, 4, литера А, г. Санкт-Петербург, 196084, Россия
e-mail: maxim.prygunov@o2svet.ru, https://orcid.org/0000-0002-7895-3536

ПРИМЕНЕНИЕ МЕТОДОВ АНАЛИЗА НАДЕЖНОСТИ И РИСКА ПРИ ОБЕСПЕЧЕНИИ, ПРОГНОЗИРОВАНИИ И ОЦЕНКЕ РАДИАЦИОННОЙ СТОЙКОСТИ РЭА

DOI: http://dx.doi.org/10.26583/bit.2018.1.05

Аннотация. Установлено соотношение понятий «качества», «надежности», «стойкости» продукции и «риска». Рассмотрен отечественный и зарубежный опыт, а также международные, национальные и отраслевые стандарты в области обеспечения качества технологических систем различного назначения. Выявлено, что зарубежные отраслевые стандарты в области обеспечения качества космических систем оперируют термином «dependability» (в отечественной терминологии сходен с понятием «надежности»), включая в него понятие радиационной стойкости. Определена взаимосвязь между зарубежными отраслевыми, международными и национальными стандартами. Приведены общие сведения по основным методам анализа и оценки надежности и риска, представленным в отечественных и зарубежных нормативных документах. Предлагается применить имеющуюся развитую методологию анализа и оценки надежности и риска для задач обеспечения, прогнозирования и оценки радиационной стойкости РЭА космической техники на всех этапах жизненного цикла.

Ключевые слова: качество, надежность, радиационная стойкость, радиоэлектронная аппаратура, риск.

Для цитирования. ***СИЗОВА, Ксения Г.; СКОРОБОГАТОВ, Петр К.; ПРЫГУНОВ, Максим О.*** *ПРИМЕНЕНИЕ МЕТОДОВ АНАЛИЗА НАДЕЖНОСТИ И РИСКА ПРИ ОБЕСПЕЧЕНИИ, ПРОГНОЗИРОВАНИИ И ОЦЕНКЕ РАДИАЦИОННОЙ СТОЙКОСТИ РЭА. Безопасность информационных технологий, [S.l.], v. 25, n. 1, p. 52-64, 2018. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1093>. Дата доступа: 15 feb. 2018. doi:http://dx.doi.org/10.26583/bit.2018.1.05.*

Ksenia G. Sizova[1], Petr K. Skorobogatov[2], Maksim O. Prygunov[3]
[1]Limited liability company "NPC "Topaz",
23 Uchitelskaya str., letter A, Saint-Petersburg, 195269, Russian Federation
e-mail: ksizova@microtopaz.ru, https://orcid.org/0000-0003-0922-3430
[2]National Research Nuclear University MEPHI (Moscow Engineering Physics Institute),
31, Kashirskoe sh., Moscow, 114509, Russian Federation
e-mail: pkskor@spels.ru, https://orcid.org/0000-0002-3146-0304
[3]Limited liability company "O2 Light Systems",
4 Novoroshhinskaja str., letter A, Saint-Petersburg, 196084, Russian Federation
e-mail: maxim.prygunov@o2svet.ru, https://orcid.org/0000-0002-7895-3536

Application of dependability and risk analysis methods in the process of implementation, prediction and evaluation of electronic equipment radiation hardness

DOI: http://dx.doi.org/10.26583/bit.2018.1.05

Abstract. The relationship between the concepts of "quality", "dependability", "hardness" of products and "risk" is established. The domestic and foreign experience, as well as international,

national and industry standards in the field of quality assurance of electrotechnical systems for various purposes are considered. It was revealed that the foreign industry standards in the field of quality assurance of space systems use the term "dependability" (in the domestic terminology it is similar to the notion of "reliability"), including the concept of radiation resistance. The correlation among foreign industry, international and national standards is defined. General information on the main methods of analysis and assessment of dependability and risk, presented in domestic and foreign documents, are considered. The authors of the paper propose to apply the existing developed methodology of analysis and evaluation of dependability and risk for the tasks of ensuring, predicting and assessing the radiation hardness of space systems at all stages of the life cycle.

Keywords: quality, dependability, radiation hardness, electronic equipment, risk.

For citation. ***SIZOVA, Ksenia G.; SKOROBOGATOV, Petr K.; PRYGUNOV, Maksim O.*** *Application of dependability and risk analysis methods in the process of implementation, prediction and evaluation of electronic equipment radiation hardness. IT Security (Russia), [S.l.], v. 25, n. 1, p. 52-64, 2018. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1093>. Date accessed: 15 feb. 2018. doi:http://dx.doi.org/10.26583/bit.2018.1.05.*

ВВЕДЕНИЕ

Под качеством продукции подразумевается совокупность свойств, обусловливающих ее способность удовлетворять своему назначению. Для оценки качества используются показатели, которые представляют собой количественные характеристики одного или нескольких свойств продукции, рассматриваемые применительно к определенным условиям ее эксплуатации. Каждая продукция обладает своей номенклатурой показателей качества.

Надежность является одним из основных свойств продукции, характеризующего способность выполнять требуемые функции в заданных режимах и условиях применения при сохранении во времени значений параметров в установленных пределах. Надежность продукции согласно отечественной терминологии – сложное свойство качества, которое зависит от безотказности, долговечности, ремонтопригодности и сохраняемости. Оценка показателей надежности дает достаточно полное представление о качестве функционирования продукции в нормальных условиях эксплуатации. Однако, при эксплуатации продукции в условиях воздействия внешних факторов окружающей среды свойство выполнять требуемые функции и сохранять во времени значения параметров в установленных пределах характеризуется показателями стойкости. Таким образом, надежность и стойкость являются показателями качества продукции по характеризуемым свойствам. А исходя из определений, стойкость является «частным случаем» понятия надежности, рассматриваемого в условиях внешних воздействий [1].

Показатели стойкости, как и показатели надежности, имеют вероятностный характер и отражают риск возникновения того или иного события. Понятие риска представляет собой сочетание вероятности события и его последствий. Таким образом, решение задач надежности и стойкости, а значит и задач в области качества продукции, происходит через определение риска. Соотношение понятий «качества», «надежности», «стойкости» и «риска» приведено на рисунке 1 [2].

При эксплуатации в условиях космического пространства (КП) радиоэлектронная аппаратура (РЭА) космического аппарата (КА) находится под воздействием большого количества внешних факторов. К числу наиболее опасных относится ионизирующее излучение (ИИ) КП. Для оценки способности РЭА выполнять свои функции и сохранять параметры в пределах установленных норм в процессе и после воздействия ИИ применяются показатели радиационной стойкости. Основной функцией РЭА является обработка данных, прием и (или) передача информации. В результате воздействия ИИ КП в РЭА возникают радиационные эффекты, которые снижают качество передаваемой информации, а также нарушают методы ее обработки. К показателям качества информации относятся понятия: достоверность, точность, устойчивость, своевременность, актуальность, доступность, достаточность, содержательность и репрезентативность. На

качество передаваемой информации существенно влияет характер функционирования РЭА КА, в первую очередь ее надежность и радиационная стойкость. Однако, исторически сложилось так, что в ракетно-космической отрасли страны данные аспекты рассматриваются обособленно.

Целью данной работы является анализ зарубежного и отечественного опыта в области обеспечения качества продукции (в частности, военной и космической техники), а также обзор нормативной базы в области менеджмента надежности и риска в процессе жизненного цикла технических устройств для рассмотрения возможности применения данных наработок в части развития методологии обеспечения, прогнозирования и оценки радиационной стойкости РЭА КА.

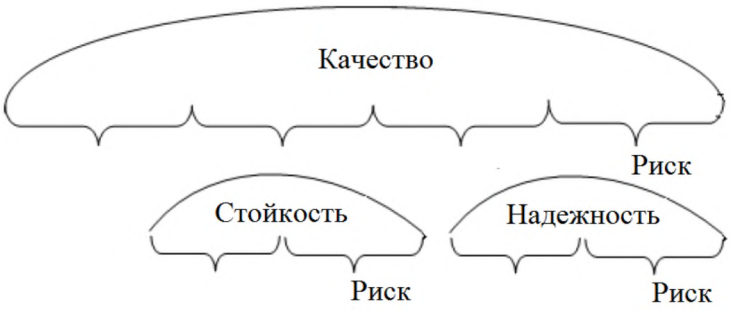

Рис. 1. Соотношение понятий «качества», «надежности», «стойкости» и «риска»
(Fig.1. Correlation of the concepts "quality", "dependability", "hardness" and "risk")

АНАЛИЗ ЗАРУБЕЖНЫХ СТАНДАРТОВ

За рубежом существует множество документов, регламентирующих процесс разработки, проектирования, производства, эксплуатации и технического обслуживания продукции различного назначения с целью обеспечения заданных уровней качества. К примеру, Европейская кооперация по стандартизации в области космической техники (англ. *European Cooperation for Space Standardization*, *ECSS*) сформировала систему стандартов, охватывающую все аспекты создания и эксплуатации космических систем, включая разработку, управление и обеспечение качества продукции. На рисунке 2 приведена структура системы стандартов *ECSS* [3].

Данная система стандартов не разделяет аспекты надежности и радиационной стойкости, а оперирует одним понятием – «*dependability*». «*Dependability*» в стандартах *ECSS* приводится как собирательный термин, применяемый для описания комплексного свойства готовности (*availability*) и влияющих на него свойств безотказности (*reliability*), ремонтопригодности (*maintainability*), а также обеспеченности технического обслуживания и ремонта (*maintenance support*). Термин «*dependability*» в отечественной терминологии сходен с понятием «надежности» и используется в данной работе для качественного описания свойств продукции, а не как количественный параметр. Поэтому далее по тексту авторы будут оперировать именно понятием «надежности».

Стандарты *ECSS* гармонизированы с международными стандартами, в том числе со стандартами Международной электротехнической комиссии (англ. *International Electrotechnical Commission, IEC*), и регулярно актуализируются в соответствии с опытом практического применения [4-10]. *IEC* в свою очередь разрабатывает стандарты для управления системами оценки соответствия продуктов, систем и услуг в области электротехники, электроники и сопутствующих отраслей.

Стоит отметить, что зарубежные отраслевые стандарты, гармонизированные с международными, не ограничиваются только определением радиационной стойкости, как составляющей более общего понятия надежности, но также используют одни и те же методы для анализа и оценки надежности и радиационной стойкости. Такой подход обосновывается тем, что решение этих двух задач в целом происходит через определение рисков.

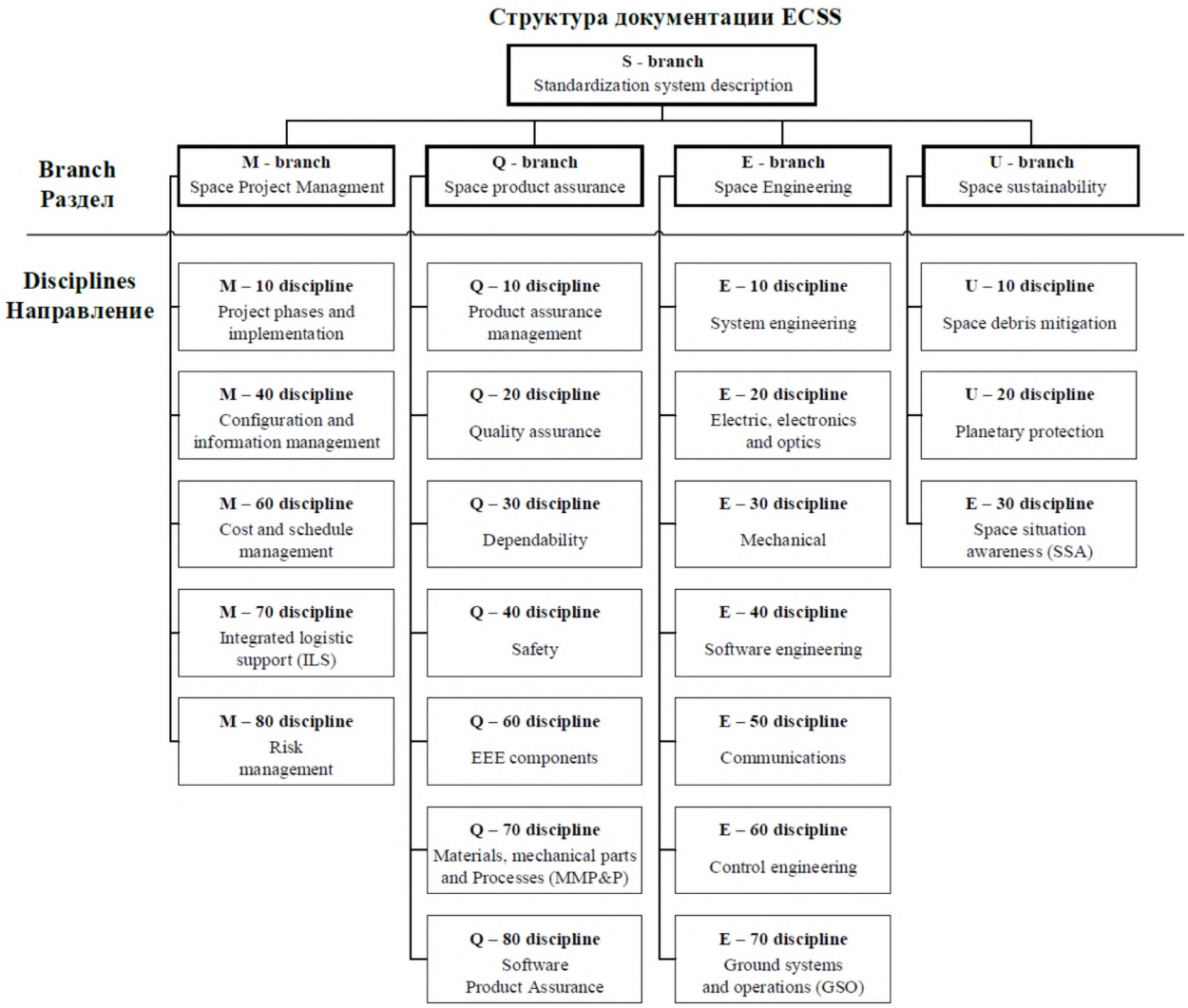

Рис. 2. Структура системы стандартов ECSS
(Fig.2. ECSS standards system structure)

АНАЛИЗ НАЦИОНАЛЬНЫХ СТАНДАРТОВ РФ

Лучшая практика применения методов анализа и оценки рисков нашла отражение в международных стандартах *IEC* по управлению риском, многие из которых приняты в РФ как национальные стандарты. Национальным комитетом *IEC* от Российской Федерации (РФ) является Федеральное агентство по техническому регулированию и метрологии (ФАТРиМ), одной из задач которого является определение норм и требований по обеспечению качества электротехники, электроники отечественного производства.

В структуре национальных стандартов РФ можно выделить две группы стандартов общего назначения «Менеджмент риска» и «Надежность в технике», которые имеют развитую структуру и проверенную методологию. Группа стандартов «Менеджмент риска» описывает процесс управления риском, охватывая при этом различные аспекты работы с ним: от идентификации и анализа риска до оценки его допустимости и определения потенциальных возможностей снижения риска посредством выбора, реализации и контроля соответствующих управляющих действий. В свою очередь группа стандартов «Надежность в технике» предназначена для нормативного обеспечения методов, мероприятий и средств, направленных на достижение уровня надежности объектов, тем самым устанавливает общие методические принципы управления надежностью.

Необходимо подчеркнуть, что в данной работе проанализированы именно те национальные стандарты, которые идентичны/гармонизированы с международными

стандартами *IEC*, поскольку целью авторов являлось рассмотрение возможности обоснованного применения зарубежного опыта для обеспечения и повышения качества отечественной продукции различного назначения. В таблице 1 представлен перечень основных национальных и соответствующих им международных стандартов по менеджменту надежности и риска.

Таблица 1. Перечень основных национальных и соответствующих им международных стандартов по менеджменту надежности и риска.

Обозначение национального стандарта РФ	Наименование национального стандарта РФ	Обозначение соответствующего международного стандарта	Наименование международного стандарта
Основополагающие стандарты			
ГОСТ Р 51901.1-2002	Менеджмент риска. Анализ риска технологических систем	IEC 60300-3-9:1995	Dependability management - Part 3: Application guide - section 9: Risk analysis of technological systems
ГОСТ Р 51901.2-2005 (отменен без замены)	Менеджмент риска. Системы менеджмента надежности	IEC 60300-1:2003	Dependability management – Part 1: Dependability management systems
ГОСТ Р 51901.3-2007	Менеджмент риска. Руководство по менеджменту надежности	IEC 60300-2:2004	Dependability management - Part 2: Guidelines for dependability management
ГОСТ Р МЭК 62198-2015 (на замену ГОСТ Р 51901.4-2005)	Проектный менеджмент. Руководство по применению менеджмента риска при проектировании	IEC 62198:2013	Project risk management - Application guidelines
ГОСТ Р 51901.5-2005	Менеджмент риска. Руководство по применению методов анализа надежности	IEC 60300-3-1:2003	Dependability management – Part 3-1: Application guide - Analysis techniques for dependability – Guide on methodology

Продолжение таблицы 1

Обозначение национального стандарта РФ	Наименование национального стандарта РФ	Обозначение соответствующего международного стандарта	Наименование международного стандарта
ГОСТ Р 51901.6-2005	Менеджмент риска. Программа повышения надежности	IEC 61014:2003	Programmes for reliability growth
ГОСТ Р 27.301-2011	Надежность в технике. Управление надежностью. Техника анализа безотказности. Основные положения	IEC 60300-3-1:2003	Dependability management – Part 3-1: Application guide - Analysis techniques for dependability – Guide on methodology
Руководящие положения и инструменты			
ГОСТ Р 51901.11-2005	Менеджмент риска. Исследование опасности и работоспособности. Прикладное руководство	IEC 61882:2001	Hazard and operability studies (HAZOP studies) – Application guide
ГОСТ Р 51901.12-2007	Менеджмент риска. Метод анализа видов и	IEC 60812:2006	Analysis techniques for system

	последствий отказов		reliability - Procedure for failure mode and effects analysis (FMEA)
ГОСТ Р 27.302-2009 (ГОСТ Р 51901.13-2005 отменен без замены)	Надежность в технике. Анализ дерева неисправностей	IEC 61025:2006	Fault tree analysis (FTA)
ГОСТ Р 51901.14-2007	Менеджмент риска. Структурная схема надежности и булевы методы	IEC 61078:2006	Analysis techniques for dependability - Reliability block diagram and Boolean methods
ГОСТ Р 51901.15-2005	Менеджмент риска. Применение марковских методов	IEC 61165:2006	Application of Markov techniques
ГОСТ Р 51901.16-2005	Менеджмент риска. Повышение надежности. Статистические критерии и методы оценки	IEC 61164:2004	Reliability growth - Statistical test and estimation methods
ГОСТ 27.310-95	Надежность в технике. Анализ видов, последствий и критичности отказов. Основные положения	IEC 60812:2006 в части определений, общих положений и методов анализа	Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)

Среди основополагающих стандартов особо следует выделить ГОСТ Р 51901.1 [11] и ГОСТ Р 51901.5 [11], отражающие в себе современный практический опыт выбора и применения методов анализа и оценки надежности и риска. Методы, содержащиеся в данных нормативных документах, разнообразны и включают в себя как качественные, так и количественные средства для анализа и оценки, а их применение регламентируется однозначно и детализировано. Во введении к стандарту [12] также отмечается, что приведенные в нем методы анализа и оценки надежности могут быть использованы для определения вероятностных характеристик риска.

В таблице 2 приведены сведения по основным методам анализа надежности и риска, представленные в отечественных и зарубежных документах, а также обозначены рекомендации по их применению на различных этапах проекта. В столбце «Название метода» таблицы 2 приведено краткое название метода и его английская аббревиатура. В столбце «Согласно ГОСТ Р 51901.1 (таблица 1)» приведены краткие характеристики методов, используемых при анализе и оценке риска в соответствии с [11]. В столбцах «Согласно ГОСТ Р 51901.5 (таблица 1)» приведены краткие описания методов, используемых для решения общих задач анализа и оценки надежности в соответствии с [11], как качественного, так и количественного характера. При этом, если метод рекомендован для решения поставленной задачи, в последнем столбце таблицы 2 содержится отметка - «применим». В случае если метод рекомендован для решения только некоторой части задачи или может использоваться для решения всей задачи только в комбинации с другими методами, то в столбце ставилась отметка - «поддержка».

Таблица 2. Сведения по основным методам анализа надежности и риска

Название метода	Согласно ГОСТ Р 51901.1 (таблица 1)	Согласно ГОСТ Р 51901.5 (таблица 1)		Рекомендации по применению
		Качественный характер	Количественный характер	
Исследование опасности и работоспособности/ HAZOP (ГОСТ Р 51901.11)	Идентификация опасности и анализ показателей	Анализ причин и последствий отклонений	-	Поддержка на поздних этапах разработки

Название метода	Согласно ГОСТ Р 51901.1 (таблица 1)	Согласно ГОСТ Р 51901.5 (таблица 1)		Рекомендации по применению
		Качественный характер	Количественный характер	
Анализ видов и последствий (критичности) отказов/ FME(C)A (ГОСТ Р 51901.12, ГОСТ 27.310)	Идентификации главных источников опасности и анализ показателей	Анализ воздействия отказов	Вычисление интенсивностей отказов (и критичности) системы	Применим (для систем, у которых преобладают единичные отказы) на стадиях определения, проектирования и разработки
Анализ дерева неисправностей/ FTA (ГОСТ Р 51901.13, ГОСТ Р 27.302)	Идентификации опасности и анализ показателей	Анализ комбинации неисправностей	Вычисление показателей безотказности, работоспособности относительного вклада подсистем в системы	Применим (если поведение системы зависит от времени или последовательности событий) на стадиях определения, проектирования и разработки
Анализ дерева событий/ ETA (ГОСТ Р 54142)	Идентификация опасности и анализ показателей	Анализ последовательности отказов	Вычисление интенсивностей отказов	Применим на стадиях определения, проектирования и разработки
Анализ структурной схемы надежности/ RBD (ГОСТ Р 51901.14)	Совокупность приемов анализа показателей	Анализ путей работоспособности	Вычисление показателей безотказности и комплексных показателей надежности	Применим (для систем, у которых можно выделить независимые блоки) на стадиях определения, проектирования и разработки
Марковский анализ (ГОСТ Р 51901.14)	Идентификация опасности и анализ показателей	Анализ последовательности отказов	Вычисление показателей безотказности и комплексных показателей надежности	Применим для функционально сложных систем на стадиях проектирования и разработки
Статистические методы надежности (ГОСТ Р 51901.6)	Совокупность приемов анализа показателей	Анализ воздействия неисправностей	Определение количественных оценок показателей безотказности с неопределенностью	Поддержка

Продолжение таблицы 2

Название метода	Согласно ГОСТ Р 51901.1 (таблица 1)	Согласно ГОСТ Р 51901.5 (таблица 1)		Рекомендации по применению
		Качественный характер	Количественный характер	
Прогнозирование интенсивности отказов (ГОСТ Р 51901.16)	Совокупность приемов анализа показателей	Возможно применение для анализа стратегии технического обслуживания	Вычисление интенсивностей отказов и наработки на отказ (MTTF)	Применим (для последовательных систем без резервирования) на ранних стадиях проектирования и на стадии производства при необходимости улучшения качества
Анализ сети Петри (ГОСТ Р 51901.5)	Идентификация опасности	Анализ последовательности отказов	Подготовка описания системы для марковского анализа	Применим
Анализ человеческого фактора (ГОСТ Р 51901.5)	Идентификация опасности и анализ показателей	Анализ воздействия действий эффективности человека на работу системы	Вычисление вероятностей ошибок человека	Поддержка на всех стадиях разработки системы
Анализ прочности и напряжений (ГОСТ Р 51901.5)	Анализ вероятностей отказа	Применим как средство для предотвращения неисправности	Вычисление показателей безотказности	Поддержка (для электромеханических компонентов)
Таблица истинности (анализ функциональной структуры) (ГОСТ Р 51901.5)	Идентификация опасности и анализ вероятностей событий	Возможен	Вычисление показателей безотказности и комплексных показателей надежности	Поддержка на ранних этапах разработки

Из представленных выше данных видно, что на сегодняшний день существует достаточное число национальных нормативных документов, гармонизированных с международными стандартами, имеющих хорошо развитые и опробованные инструменты для оценки и анализа надежности и риска [13, 14]. Сами по себе группы стандартов общего назначения «Менеджмент риска» и «Надежность в технике» содержат отработанный механизм обеспечения заданного уровня качества продукции на различных уровнях детализации системы и этапах ее жизненного цикла.

ПРОМЕЖУТОЧНЫЕ ВЫВОДЫ

Несмотря на наличие развитой методологии анализа и оценки надежности и риска на уровне национальных стандартов, а также мировой опыт применения данной методологии к решению задач обеспечения, прогнозирования и оценки в целом качества продукции, понятие радиационной стойкости в отечественной ракетно-космической отрасли до сих пор рассматриваются обособленно и независимо. При этом для развития области радиационной стойкости не используются существующие наработки в смежных областях знаний, а в части стандартизации вопросы обеспечения, прогнозирования и оценки надежности и радиационной стойкости рассматриваются как отдельные независимые направления.

ПРИМЕНИМОСТЬ

Подходы к изучению проблемы надежности основываются на теории вероятностей (сочетание вероятности события и его последствий характеризует риск), одним из центральных понятий которой являются понятия случайного события и случайной величины. Бытовое представление о случайности, как о недетерминированной

переменной провоцирует неверное предположение о сущности определяемых процессов или величин. Главной характеристикой упомянутых событий и величин является их вероятностная сущность, а не случайность (недетерминированность).

Основным фактором, влияющим на работу космической техники, являются радиационные эффекты, вызываемые воздействием ОЯЧ КП. Эти эффекты являются детерминированными по своей природе, но случайными по области их возникновения. Таким образом, полагая, что одиночные сбои и отказы, вызванные воздействием ОЯЧ КП в отдельно взятых элементах системы, имеют случайный и независимый характер, допустимо применять отработанный понятийный и математический аппарат теории надежности, подходящий для описания подобного рода событий и характера реакций на эти события системы в целом.

Порядок и методы оценки стойкости бортовой РЭА космических аппаратов (КА) к воздействию ОЯЧ КП по одиночным сбоям и отказам регламентирован в отраслевом нормативном документе [15]. В соответствии с положениями данного документа, вывод о стойкости РЭА к воздействию ОЯЧ КП по одиночным эффектам производится на основе:

1 этапа – качественного анализа – анализа возможности возникновения сбоев и отказов элементов системы и последствий их влияния на работоспособность и функционирование РЭА с учетом применения средств защиты, алгоритмов и программ, используемых для обнаружения и устранения сбоев, срыва тиристорного эффекта и пробоя, времени восстановления штатного функционирования, влияния перерыва в работе составных частей РЭА на работоспособность и функционирование КА;

2 этапа – количественного анализа – результатов расчета частоты сбоев РЭА и вероятности ее отказа по данным о параметрах чувствительности элементов системы к одиночным эффектам.

Сначала подробнее остановимся на рассмотрении инструментов, приведенных в документе [15], для решения задач 2 этапа. Расчетно-экспериментальный метод, предлагаемый к использованию в [15] для проведения количественного анализа, корректен при определении стойкости функционально простых, нерезервированных систем без учета восстановления их работоспособности. При этом ни сам документ [12], ни документы, на которые он ссылается не располагает в своем составе необходимыми методологией и математическим аппаратом для оценки стойкости современной РЭА, представляющей собой, многофункциональную систему со сложными стратегиями восстановления.

Для преодоления этих трудностей в работе [16] было реализовано применение количественных методов оценки надежности для определения показателей стойкости к воздействию отдельных ядерных частиц (ОЯЧ) КП по сбоям и отказам. Как упоминалось выше, возможность применения такого подхода обуславливалась тем, что области надежности и радиационной стойкости в части решения прикладных задач опираются на одни и те же фундаментальные математические и естественнонаучные принципы, а именно на определение вероятности события и его последствий - риска. Это дало основание для использования при решении задач теории стойкости хорошо развитого теории надежности и позволило сосредоточить основные усилия на учете особенностей возникновения сбоев и отказов в РЭА, вызываемых воздействием ОЯЧ КП, и их последствиях. Таким образом, применение данного подхода позволило в полной мере учесть современные тенденции в проектировании РЭА и получить более полную характеристику ее стойкости.

Возвращаясь к условиям выполнения требований нормативного документа [15] в части 1 этапа оценки, стоит отметить, что несмотря на указание о необходимости проведения качественного анализа, документ не включает в себя конкретные методы и подходы к реализации, а также не ссылается на иные инструменты для решения данной задачи. Таким образом, данный этап остается не формализован. Как и в случае с проведением количественного анализа, проводимого в работе [16], возможно предположить использование показанной аналогии между надежностью и радиационной

стойкостью, распространяя ее на методы качественного анализа, приведенные в таблице 2. Такой подход позволит формализовать процесс и в полной мере соблюсти требования [15] при помощи использования основ, заложенных в действующих национальных стандартах, не прибегая при этом к усложнению и увеличению количества отраслевой нормативной базы.

Таким образом, имеющиеся наработки в области надежности и риска могут быть использованы при решении частных задач стойкости к воздействию ОЯЧ КП по эффектам сбоя и отказа. При этом их использование позволяет получать более полную характеристику стойкости РЭА.

Кроме того, дальнейший анализ национальных и международных стандартов показал, что имеющаяся методология, может применяться не только при анализе систем, где события носят случайный характер, но и, как минимум, рассматривать другие виды радиационных эффектов, имеющих «накопительный» характер (например, дозовые эффекты ионизации и структурных повреждений) в процессе качественного анализа с помощью понятия риска. А при более глубоком изучении вопроса применения понятийного и математического аппарата теории надежности было обнаружено, что можно провести параллель между механизмами определения показателей стойкости к дозовым эффектам и характеристиками прочности, т.е. использовать данную аналогию также в процессе количественного анализа. Данное предположение основывается на том, что как и в случае с дозовыми эффектами отказ элемента по параметрам прочности возникает тогда, когда уровень внешних воздействий (механических, климатических, электрических и т.д.) превысит запас его прочности. На данный момент подробный анализ этого предположения не производился, но в РФ достаточно давно принят комплекс нормативно-технических и руководящих документов по расчетам и испытаниям на прочность в отрасли машиностроения, общие положения которого приведены в [14]. Это говорит о солидной методической базе в данной области знаний и предоставляет возможность к рассмотрению указанной взаимосвязи. Таким образом, имеющиеся наработки в области прочностной надежности могут быть использованы для дополнения и развития методологии в части количественного анализа и оценки показателей радиационной стойкости к воздействию ИИ КП по дозовым эффектам.

Помимо всего прочего, развитие национальных стандартов группы «Надежность в технике» шло параллельно и во взаимосвязи с развитием нормативных документов, разработанных для изделий военной техники - комплексов государственных военных стандартов (КГВС) «Мороз», «Климат» и руководящих военных документов в области надежности. Разработка такой нормативной базы была направлена на совершенствование методологии нормирования надежности и оценки соответствия требованиям надежности по всем уровням разукрупнения вооружения и военной техники (ВВТ): от электрорадиоизделий (ЭРИ) и РЭА военного назначения до целых комплексов и образцов ВВТ. Также с 2005 года в РФ появились нормативные документы системы стандартизации «Надежность военной техники», которая позиционирует себя, как подсистема системы стандартов «Надежность в технике». Система стандартов «Надежность военной технике» имеет много общего с нормативными документами группы «Надежность в технике» и элементами КГВС «Мороз» [18].

Важно отметить, что отраслевая нормативная документация по стойкости в целом, нацелена на подтверждение соответствия РЭА заданным требованиям уже на последних стадиях проектирования и разработки, исключая начальные этапы жизненного цикла. Тем не менее развитие технологий и электронной техники требуют того, чтобы анализ и оценка радиационной стойкости РЭА выполнялась непрерывно, начиная с самых ранних этапов разработки [6, 7]. Таким образом, существующие национальные стандарты в области управления надежностью и риском (в том числе и в части ВВТ) могут быть использованы в качестве базиса в процессе обеспечения, прогнозирования и оценки радиационной стойкости изделий космической техники на стадиях определения,

проектирования, разработки, производства, эксплуатации и технического обслуживания различных уровней системы и в условиях разной детализации проекта.

ЗАКЛЮЧЕНИЕ

Для решения задач обеспечения радиационной стойкости технических систем, предназначенных для ответственных применений, одинаково важны и глубокие теоретические исследования, наличие алгоритмов и методов, их программная реализация, а также эффективная система стандартизации продукции и организации взаимодействия при ее разработке и производстве. Отечественные отраслевые документы в области радиационной стойкости рассматривают отдельные этапы жизненного цикла РЭА, но при этом в них отсутствует система, сопровождающая процессы разработки, проектирования, производства, эксплуатации и технического обслуживания продукции. К сожалению, на данный момент нет прямого способа применения имеющихся отработанных инструментов теории надежности и риска, а также их методов и программных средств, для развития методологии анализа и оценки радиационной стойкости. Тем не менее международные и национальные стандарты РФ по менеджменту надежности и риска технологических систем с оглядкой на зарубежный опыт могут применяться при выборе и обосновании решений, позволяющих обеспечить выполнение обязательных требований, в том числе и по радиационной стойкости РЭА. Это особенно важно при наличии в отраслевых нормативных документах решений не эффективных или не применимых к новым технологиям.

Таким образом, предлагается:

- допуская возможность разумного применения методов анализа и оценки надежности и риска при решении задач обеспечения, прогнозирования и оценки радиационной стойкости РЭА космической техники, проецировать имеющуюся методологию на весь жизненный цикл РЭА, что позволит не просто определять радиационную стойкость, а также и управлять ею;

- использовать, дополнять и развивать теорию радиационной стойкости в части решения прикладных задач методологией и имеющимися программными средствами теории надежности и риска;

Важным представляется производить дальнейший анализ международных, национальных, зарубежных и отечественных отраслевых стандартов, а также мирового опыта в области обеспечения качества технологических систем различного назначения, с целью актуализации или разработки новой отечественной нормативной базы для формирования системы стандартов в области обеспечения, прогнозирования и оценки радиационной стойкости на всех этапах жизненного цикла продукции с учетом опыта, полученного в смежных областях.

СПИСОК ЛИТЕРАТУРЫ:

1 Управление обеспечением стойкости сложных технических систем В. Н. Бакулин, С. Ю. Малков, В. В. Гончаров, В. И. Ковалев. — Москва, 2006. — С. 304.
2 Струков А.В. Анализ международных и российских стандартов в области надежности, риска и безопасности [Электронный ресурс]. – Режим доступа: -http://szma.com/standarts_analysis.pdf (дата обращения 01.10.2017).
3 ECSS, “Description, implementation and general requirements”, ECSS-S-ST-00C, ECSS Secretariat, ESTEC, The Netherlands (July 2008).
4 ECSS, “Standardization objectives, policies and organization”, ECSS-P-00C, ECSS Secretariat, ESTEC, The Netherlands (March 2013).
5 Standards for Space Radiation Environments and Effects” E. Daly, P. Nieminen, A. Mohammadzadeh et al.|RADECS Proceedings of the 7th European Conference on Radiation and Its Effects on Components and Systems, 2003.
6 Poivey C. Radiation Hardness Assurance for Space Systems Component Selection, System Hardening and Counter-Measures/RADECS-2003 Short Course notes (2003).
7 Emerging Radiation Hardness Assurance (RHA) issues: A NASA Approach for Space Flight Programs K. A.

LaBel, A. H. Johnston, J. L. Barth, R. A. Reed et al. IEEE Trans. Nucl. Sci., vol. 45, n 6, pp. 2727-2736, Dec. 1998.
8 Radiation assurance for the space environment. J.L. Barth, K.A. LaBel, C. Poivey IEEE Cat. No.04EX866, International Conference on Integrated Circuit Design and Technology, May 2004.
9 Radiation Hardness Assurance for Space Systems C. Poivey IEEE NSREC Short Course, Phoenix, July 2002.
10 Hardness assurance for space system microelectronic. R. L. Pease, D. R. Alexander. Rad. Phys. Chem., vol. 43, n ½, pp. 191 – 204, Jan. 1994.
11 ГОСТ Р 51901.1-2002. «Менеджмент риска. Анализ риска технологических систем».
12 ГОСТ Р 51901.5-2005 «Менеджмент риска. Руководство по применению методов анализа надежности».
13 Improving failure analysis efficiency by combining FTA and FMEA in a recursive manner J. F. W. Peeters, R. J. I. Basten, T. Tinga. Reliability Engineering & System Safety, vol. 172, pp. 36-44, December 2017.
14 Reliability of non-repairable phased-mission systems with propogated failures G. Levitin, L. Xing, S. V. Amari, Y. Dai. Reliability Engineering & System Safety, vol. 119, pp. 218-228, November 2013.
15 РД 134-0139-2005. Методы оценки стойкости аппаратуры к воздействию заряженных частиц по одиночным сбоям и отказам.
16 Сизова К.Г., Скоробогатов П.К., Ветринский Ю.А. Методология оценки стойкости радиоэлектронной аппаратуры к воздействию отдельных заряженных частиц космического пространства по одиночным сбоям и отказам. ВАНТ. Сер.: Физика радиационного воздействия на радиоэлектронную аппаратуру. 2017. Вып. 1.
17 ГОСТ 25.001-78 «Расчеты и испытания на прочность в машиностроении».
18 Писарев В.Н. К вопросу о стандартизации в области надежности военной техники. Труды международного симпозиума надежность и качество, 2016, с. 293-295.

REFERENCES:

[1] Upravlenie obespecheniem stojkosti slozhnyh tehnicheskih sistem [Management of the durability of complex technical systems] V. N. Bakulin, S. Ju. Malkov, V. V. Goncharov, V. I. Kovalev, Moscow: FIZMATLIT, 2005, 304 p. (in Russian).
[2] Strukov A.V. Analiz mezhdunarodnyh i rossijskih standartov v oblasti nadezhnosti, riska i bezopasnosti [Analysis of international and Russian standards in the field of reliability, risk and safety]. – URL: - http://szma.com/standarts_analysis.pdf (access time 01.10.2017). (in Russian).
[3] ECSS, “Description, implementation and general requirements”, ECSS-S-ST-00C, ECSS Secretariat, ESTEC, The Netherlands (July 2008).
[4] ECSS, “Standardization Policy”, ECSS-P-00A, ECSS Secretariat, ESTEC, The Netherlands (April 2000).
[5] Standards for Space Radiation Environments and Effects” E. Daly, P. Nieminen, A. Mohammadzadeh et al. RADECS Proceedings of the 7th European Conference on Radiation and Its Effects on Components and Systems, 2003.
[6] Poivey C. Radiation Hardness Assurance for Space Systems Component Selection, System Hardening and Counter-Measures RADECS-2003 Short Course notes (2003).
[7] Emerging Radiation Hardness Assurance (RHA) issues: A NASA Approach for Space Flight Programs K. A. LaBel, A. H. Johnston, J. L. Barth, R. A. Reed et al. IEEE Trans. Nucl. Sci., vol. 45, n 6, pp. 2727-2736, Dec. 1998.
[8] Radiation assurance for the space environment J.L. Barth, K.A. LaBel, C. Poivey IEEE Cat. No.04EX866, International Conference on Integrated Circuit Design and Technology, May 2004.
[9] Radiation Hardness Assurance for Space Systems C. Poivey IEEE NSREC Short Course, Phoenix, July 2002.
[10] Hardness assurance for space system microelectronics R. L. Pease, D. R. Alexander. Rad. Phys. Chem., vol. 43, n ½, pp. 191 – 204, Jan. 1994.
[11] GOST R 51901.1-2002. Menedzhment riska. Analiz riska tehnologicheskih sistem [Risk management. Risk analysis of technological systems], 2002, 21 p. (in Russian).
[12] GOST R 51901.5-2005 Menedzhment riska. Rukovodstvo po primeneniju metodov analiza nadezhnosti [Risk management. Guide for application of analysis techniques for dependability], 2005, 43 p. (in Russian).
[13] Improving failure analysis efficiency by combining FTA and FMEA in a recursive manner J. F. W. Peeters, R. J. I. Basten, T. Tinga. Reliability Engineering & System Safety, vol. 172, pp. 36-44, December 2017.
[14] Reliability of non-repairable phased-mission systems with propagated failures G. Levitin, L. Xing, S. V. Amari, Y. Dai. Reliability Engineering & System Safety, vol. 119, pp. 218-228, November 2013.
[15] RD 134-0139-2005. Metody ocenki stojkosti apparatury k vozdejstviyu zaryazhennyh chastic po odinochnym sboyam i otkazam [Equipment resistance assessment methods to charged particles of space for single errors and failures], vved. 2005-07-01, 2005, 74 p. (in Russian).
[16] Sivacheva K.G., Skorobogatov P. K., Vetrinskij Y. A. Metodologija ocenki stojkosti radiojelektronnoj apparatury k vozdejstviju otdel'nyh zarjazhennyh chastic kosmicheskogo prostranstva p oodinochnym sbojam i otkazam [Evaluation methodology of the spacecraft electronic equipment radiation hardness to single event effects], Questions of atomic science and technics. Series: Physics of radiation effects on radio-electronic equipment, 2017, no 1, pp 5 – 11. (in Russian).

[17] GOST 25.001 – 78. Raschety i ispytanija na prochnost' v mashinostroenii. [Desing calculations and strength testing in machinebuilding. Standards, technical documentation and manuals. General regulations], vved. 1980-01-01, Moscow: Standartinform, 2005, 4 p. (in Russian).

[18] Pisarev V.N. K voprosu o standartizacii v oblasti nadezhnosti voennoj tehniki [The issue of standardization in the field of military equipment reliability]. Proceedings of the International Symposium «Reliability and Quality», 2016, pp 293-295. (in Russian).

Поступила в редакцию – 01 декабря 2017 г. Окончательный вариант –05 февраля 2018 г.
Received – December 01, 2017. The final version – February 05, 2018.

Михаил Б. Абросимов, Ихаб А. Камил
СГУ имени Н.Г.Чернышевского,
ул. Астраханская, 83, г. Саратов, 410012, Россия
e-mail: mic@rambler.ru, https://orcid.org/0000-0002-4473-8790
e-mail: kamil.iehab@mail.ru, https://orcid.org/0000-0003-1100-5635

РАЗРАБОТКА СИСТЕМЫ ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ С ИСПОЛЬЗОВАНИЕМ ПАРАЛЛЕЛЬНОГО ПРОГРАММИРОВАНИЯ И СИСТЕМЫ ОТКАЗОУСТОЙЧИВОСТИ

DOI: http://dx.doi.org/10.26583/bit.2018.1.06

Аннотация. Одной из первых угроз побудивших создание систем предотвращения вторжений считают «червь Морриса», который поразил компьютеры в конце 1988г. Системы предотвращения вторжений развивались, и со временем стали полноценной системой, включающей в себя специальные проактивные методы предотвращения атак, рассчитанные для защиты от различного рода угроз. Среди проактивных систем предотвращения вторжений можно выделить следующие: поведенческий анализатор процессов для анализа поведения запущенных в системе процессов, системы устранение возможностей попадания инфекции на компьютер, системы блокировка портов, системы блокировки DoS-атак.

В статье описывается разработанная система предотвращения вторжений. Цель работы раскрыть возможности использования параллельных потоков для улучшения работы систем предотвращения вторжений. Эффективность разрабатываемой системы достигается за счет организации предотвращение атак на уровне конкретного узла, путем контроля всех системных вызовов. Система служит посредником между открытой и защищенной средой. Для повышения скорости передачи/приема информации в системе была использована технология отказоустойчивости. Актуальность темы определяется ростом бесчисленного количества разнообразных вредоносных программ, и возрастающей необходимости в защите корпоративной информации.

Ключевые слова: системы предотвращения вторжений, безопасное соединение, отказоустойчивость, параллельное программирование, вирусы, технология виртуализации, вредоносный трафик.

Для цитирования. ***АБРОСИМОВ, Михаил Б.; КАМИЛ, Ихаб А.*** *РАЗРАБОТКА СИСТЕМЫ ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ С ИСПОЛЬЗОВАНИЕМ ПАРАЛЛЕЛЬНОГО ПРОГРАММИРОВАНИЯ И СИСТЕМЫ ОТКАЗОУСТОЙЧИВОСТИ. Безопасность информационных технологий, [S.l.], v. 25, n. 1, p. 65-73, 2018. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1094>. Дата доступа: 15 feb. 2018. doi:http://dx.doi.org/10.26583/bit.2018.1.06.*

Mikhail B. Abrosimov, Iehab A. Kamil
Saratov state University named after N. G. Chernyshevskogo,
St. Astrakhanskaya, 83, Saratov, 410012, Russia
e-mail: mic@rambler.ru, https://orcid.org/0000-0002-4473-8790
e-mail: kamil.iehab@mail.ru, https://orcid.org/0000-0003-1100-5635

Development Intrusion Prevention System by Using Parallel Programming and Fault Tolerance Technology

DOI: http://dx.doi.org/10.26583/bit.2018.1.06

Abstract. One of the first threats that prompted the creation of intrusion prevention systems is considered to be the "Morris worm", which hit computers in late 1988. Intrusion prevention systems evolved, and eventually became a full-fledged system incorporating special proactive methods to prevent attacks, designed to protect against various kinds of threats. Among the proactive intrusion prevention systems are the following: a behavioral process analyzer for

analyzing the behavior of processes running in the system, eliminating the possibility of infection on the computer, locking the ports, blocking the DoS attacks.
In article the developed system of prevention of invasions is described. It is more effective to develop and use the systems of prevention of invasions as separate means of protection which will serve as the intermediary between the protected and opened networks. It is more expedient to organize prevention of the attacks at the level of concrete knot, by control of all system calls. Special attention in article is paid to use of technologies of parallel programming in the developed system. The main advantages of system of fault tolerance and the used algorithms for realization of technology of prevention of invasions are described.
Keywords: the intrusion prevention system, secure communication, fault tolerance, parallel programming, viruses, virtualization, malicious traffic.
For citation. ***ABROSIMOV, Mikhail B.; KAMIL, Iehab A.*** *Development Intrusion Prevention System by Using Parallel Programming and Fault Tolerance Technology. IT Security (Russia), [S.l.], v. 25, n. 1, p. 65-73, 2018. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1094>. Date accessed: 15 feb. 2018. doi:http://dx.doi.org/10.26583/bit.2018.1.06.*

Введение

Системы предотвращения вторжений – это современные технологии защиты, построенные на анализе поведения. Решения, которые раньше помогали, становятся неэффективными против некоторых видов угроз. Многие вирусы умеют адаптироваться, изменять размер, имена файлов, процессов и служб [1]. Процесс обнаружения и предотвращения атак на уязвимости, как таковой, подразумевает анализ и реакции на события: нарушения политик безопасности, политик использования ресурсов, политик стандартизации. Инциденты могут иметь любую природу, например, вредоносный код, неавторизованный доступ или попытки получения дополнительных прав. Системы предотвращения вторжения умеют непосредственно воздействовать на такие компоненты атаки, как тело атаки, например, обрыв соединения; среда безопасности, например, переконфигурирование для запрета сетевого доступа в сегмент; содержимое атаки, или удаление вредного аттачмента. Если нельзя обнаружить потенциальную опасность файла по внешним признакам, можно определить его вредоносную природу по поведению. Именно поведенческим анализом занимается система предотвращения вторжений.

IPS-системы корпорации Cisco

Cisco предоставляет решения по управлению IPS для развертываний любого размера, от небольших организаций до крупных предприятий. Cisco IPS Manager Express представляет собой полнофункциональное приложение для управления системами IPS и формирования отчетов по этим системам, поддерживающее до 10 устройств. Cisco Security Manager представляет собой решение управления безопасностью корпоративного класса с тысячами реальных развертываний. Кроме того, имеется полнофункциональный локальный интерфейс командной строки.

Cisco IPS Manager Express и Cisco Security Manager поддерживают устройства Cisco IPS серии 4500, а также другие сенсоры Cisco IPS. Cisco Security Manager 4.x предоставляет следующие функции:

- Гибкие процессы для поэтапной поставки новых и обновленных сигнатур, а также создания политик для IPS относительно этих сигнатур с последующим распространением политик на другие устройства;
- Поддержка расширенной отчетности и управления событиями для новейших функций IPS Cisco, включая глобальную корреляцию;
- Контроль доступа на основе ролей и рабочие процессы для обеспечения безошибочных, тразвертываний и соответствия установленным требованиям.

Cisco IPS Manager Express предоставляет следующие функции:

- Подготовку, мониторинг и устранение неполадок
- Перетаскиваемые устройства панели мониторинга для простоты настройки

– Персонализированные области просмотра, которые запоминают параметры пользователя, чтобы минимизировать время настройки и управления

– Гибкое средство создания отчетов, которое позволяет создавать настраиваемые отчеты и отчеты по соответствию нормативным требованиям в течение секунд

– Предварительно определенные шаблоны настройки, привязанные к объекту.

Системы защиты от Cisco на сегодняшний день являются лидерами во многих странах мира, в том числе и в России. Несмотря на все преимущества данной системы, существует главный недостаток – это большие финансовые затраты при внедрении.

Интегрированная система предотвращения вторжений

Существует два типа IPS: отдельные (или специальные) и интегрированные. Cisco IPS Manager Express относится к первому типу систем. Отдельные IPS обеспечивают:

– дополнительный уровень сетевой защиты от вторжений;

– возможность установки посредством выделенного специализированного оборудования.

Интегрированные IPS предлагают:

– комплексную систему защиты от вторжений по всей инфраструктуре безопасности;

– возможность интеграции в существующие узлы безопасности, как правило, в межсетевые экраны.

Разрабатываемая система относится к интегрированным системам предотвращения вторжений – что требует минимальных затрат на внедрение защиты. Система базируется на операционной системе Linux, что позволяет использовать встроенные средства штатного пакетного фильтра операционной системы Linux для подключения которого используются библиотеки netlink-queue и libnfnetlink. Они позволяют наблюдать за файлами, процессами и службами при поиске подозрительной активности. В случае подозрительной активности происходит блокировка вредоносных программ по критерию опасного выполнения кода – это позволяет поддерживать оптимальную безопасность системы без необходимости обновления баз [2, с.8]. Система позволяет управлять входящим и исходящим трафиком, основываясь на наборах правил, а также запуском и работой процессов на основании выполняемых изменений в компьютере согласно правилам контроля. Выделим основные сигнатуры угроз, определенные в системе (рис.1).

Для аудита системы ведется системный журнал – в котором регистрируются нетипичные поведения системы, которые распознаются благодаря заранее определенным сценариям вторжений (известные шаблоны атак). Например, при атаке TearDrop по типу «отказ в обслуживании» (Denial of Service, DoS) рассылаемые пакеты фрагментированы таким образом, что это вызывает крах атакуемой системы. На основе журнала формируется черный список IP-адресов, что позволяет предотвратить подключение к ботнетам, источникам спама и другим вредоносным IP-адресам.

Благодаря комбинации правил IPS с учетом уязвимостей, пользовательских правил, интеллектуального механизма анализа IP-адресов и возможностей оценки файлов интегрированная система имеет в своем распоряжении более широкий арсенал средств для защиты своих систем, и низкую – стоимость внедрения [3].

Разработанная система:

– анализирует входной трафик;
– принимает решения о блокировке трафика, для обеспечения надежного удаленного управления системой.
– помещает данные об угрозах в журнал;
– присваивает угрозе индекс вредоносного поведения;
– осуществляет соединение по параллельным каналам.

Средства конфигурирования должны быть удобны конечным пользователям, с этой целью была добавлена возможность определения правил обнаружения угроз

пользователями. Эта функция доступна в режиме online. Она позволяет, пропуская трафик через себя, не изменяя скорость работы системы [4, с.119]. Помимо проверки входных данных система обеспечивает сборку и передаваемых пакетов, анализируя данные пакетов для обнаружения следов опасной активности.

```
// создание нового потока для организации сигнатурного способа защиты
void * pthread_capture_tcp(void *arg);
```

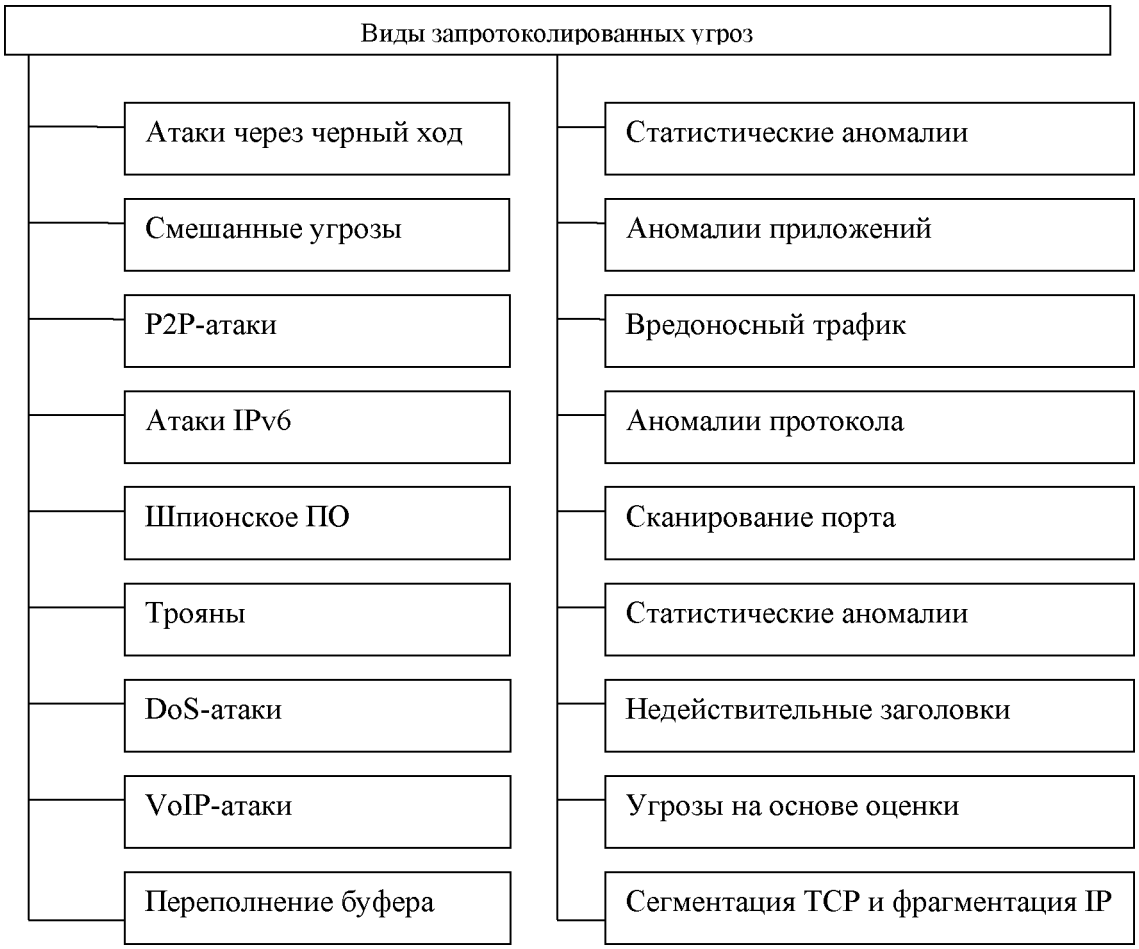

Рис. 1. Виды запротоколированных угроз
(Fig.1. Types of logged threats)

При передачи данных система устанавливает начальное число последовательности пакетов, и ряд других переменных, связанных с этим соединением. Числа последовательностей выбираются случайно на обоих сторонах. Клиентом выбирается случайное число X и отправляет SYN-пакет, который может также содержать дополнительные флаги TCP и значения опций. Сервером определяется случайное число Y, которое прибавляет 1 к значению X и отправляется ответ. В итоге завершение обмена данными происходит после прибавления 1 к значениям X и Y и отправления ACK-пакета [5].

В случае выявления подозрительных действий вредоносной программой или злоумышленником, система заблокирует данную активность (рис. 2).

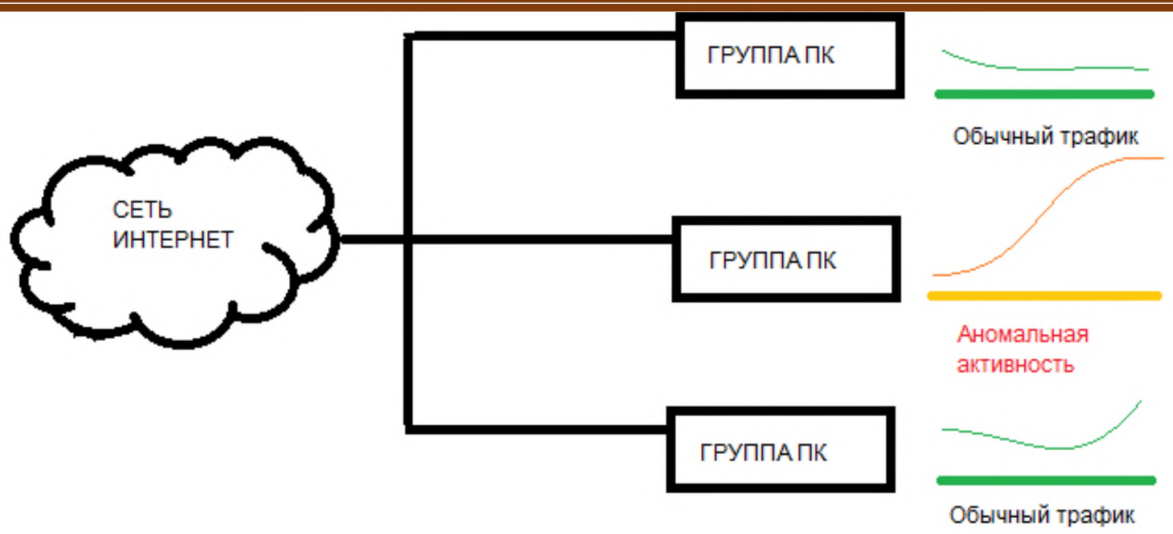

Рис. 2. Технология обнаружение уязвимостей
(Fig.2. Technology detection of vulnerabilities)

После обнаружения опасной уязвимости система реагирует на сетевую активность эксплойтов, которые используют данную уязвимость. Система предотвращения вторжений, заблокирует такой трафик заблаговременно, до достижения, им атакуемого сервера или рабочей станции [6, с.312]. Если запрос в базу не позволяет установить диспозицию файла, то она отправляется в хранилище, где производится подробный анализ: определяется его способность к сохранению после перезагрузки, проверяется трафик, генерируемый приложением, а также создаваемые процессы, записи реестра и техники скрытия процессов. В результате анализа присваивается индекс вредоносного поведения.

Разработанная система позволит отследить следующие действия:

- передачу управления другими установленными программами;
- внесение изменений в записи системного реестра;
- несанкционированное отключение программ;
- организацию межпроцессорного доступа к памяти, который позволяет внедрять вредоносный код в доверительную программу;
- а также изменения, выполняемые другими программами [7, с.63].

При использовании для защиты технологии предотвращения вторжений, контролируя параметры сессии (IP, номер порта, состояние связей), можно изучить пакет, анализируя передаваемые и получаемые данные [8, с.105].

```
if (setsockopt(raw_socket, IPPROTO_IP, IP_HDRINCL, &optval, sizeof(optval)) < 0)
{
  cerr << "Error: setsockopt(...IP_HDRINCL...)." << endl;
  exit(EXIT_FAILURE);
 }
 // Добавление сокета IP_DONTFRAG как отдельный фрагмент флага
 if (setsockopt(raw_socket, IPPROTO_IP, IP_MTU_DISCOVER, &frag, sizeof(frag)) <
0) {
  cerr << "Error: setsockopt(...IP_DONTFRAG...)." << endl;
  exit(EXIT_FAILURE);
 }
```

В разработанной системе осуществляется более глубокая проработка алгоритма функционирования прикладных протоколов (контроль состояния сеансов) (рис.3).

Рис. 3. Основные угрозы и методы их решения
(Fig.3. The main threats and methods for solving them)

Добавление профилирования трафика, и организация централизованного управления системой предотвращения вторжений, позволяют улучшить точность обнаружения вторжений [9, с.240].

Данную технологию можно использовать для организации безопасной системы, что и было использовано в разработанной системе [10, с.107].

Параллельные потоки в интегрированной системе IPS

Развитие технологий параллельного программирования привело к эффективному использованию вычислительных ресурсов многопроцессорных систем и их вычислительных ресурсов [11, с.89]. Использование технологии параллельного программирования в работе приложения, позволило реализовать дополнительные механизмы защиты. С помощью генерации параллельных потоков данных выявляются возможные аномалии, например, при организации механизма отслеживания многократного введения паролей для входа в систему [12, с.49].

```
// создаем новый поток
if (pthread_create(&thread,
NULL, // создание потока со стандартными атрибутами
pthread_capture_tcp,
NULL (!= 0) {
cerr << "Error: pthread_create().\n" << endl;
exit(status);
}
```

Используя данные из потока, системой создаются счетчики, сохраняющиеся для последующего использования.

Параллельно организованные потоки позволяют быстро подключать нужные элементы для захвата, декодирования, анализа и обработки пакетов. Это позволяет не снижать скорость приема/передачи данных, а также увеличивать пропускную способность системы.

Решение проблемы отказоустойчивости в системах предотвращения вторжений является одной из приоритетных, потому что в случае выхода из строя системы, в канале образуется затор, и трафик не доходит до адресата [13, с.50].

В разработанной системе для бесперебойного доступа созданы параллельные процессы. Процесс отправляет устройству heartbeat-пакеты, это позволяет не терять соединения в случае обрыва канала [14]. При возникновении сбоя работы встроенного приложения, система автоматически направит трафик в обход отказавшего устройства. Параллельно с этим происходит восстановление состояния системы до ближайшей

контрольной точки состояния вычислений. Данные для восстановления хранятся в специальных репозиториях.

Адаптивный подход, реализованный в системе позволяет продолжить вычисления на оставшихся работоспособных узлах без аварийного завершения работы системы. Это происходит благодаря трансляции найденных локальных значений соседним узлам. То есть на каждом узле хранится локальный экземпляр списка сохраненных задач, который сохраняет все подзадачи данного узла и пересылает их на другие соседние узлы. После завершения работы системы отчет отправляется на родительский узел, и удаляется из списка сохраненных.

Реализованный подход позволяет определять все сбои и вычислять необходимые подзадачи для отказоустойчивости системы. Совместное использование методов параллельного программирования и основных принципов отказоустойчивости позволяет перейти к реализации концепции локальной синхронизации и корректной завершаемости вычислительных приложений.

Тестирование системы

Для тестирования созданной системы использовался программный пакет BreakingPoint Virtual Edition фирмы IXIA. С его помощью искусственно было увеличено количество SYN-запросов до 12000 в секунду и произведены атаки IP-адреса с постоянной скоростью 6000 SYN в секунду. На следующем этапе было возвращено исходное значение в 12000 (достаточно для имитации DDoS-защиты, для обнаружения SYN-флуд-атаку). Для одиночных серверов был установлен порог срабатывания 3000 чтобы обеспечить то, что одиночные сервера не получат DDoS атаку при превышении лимита для всей платформы в 30000.

По результатам теста были сделаны следующие выводы:

- Система уменьшает скорость срабатывания защиты с 50 минут вначале тестов до 5 минут.
- Нет перебоев в работе, при обнаружении атаки.
- Необходимо около 15 секунд в тесте чтобы определить атаку
- Необходимо заранее подготовить персонал к действиям в случае атаки.
- При повторном тестировании система сократила время реагирования до 15 минут.

Заключение

Таким образом, системы предотвращения вторжений являются важным элементом многоуровневой защиты. Для оптимальной и эффективной работы IPS пользователь должен обладать определенными знаниями и квалификацией. Разработанная система предотвращения вторжений, имея достаточные полномочия, позволяет прекращать активность вредоносной программы. Если для остановки работы опасной программы требуется подтверждение пользователя, эффективность системы мала. Система предотвращения вторжений включает в себя определенный набор правил, который может применить пользователь. Правильное администрирование системы позволяет избежать появления конфликтов программного обеспечения и системы.

Увеличение пропускной способности сети привело к увеличению скорости обмена данными, снижению стоимости Интернет трафика. Разработанная система позволяет, используя систему предотвращения вторжений и технологию параллельного программирования организовать эффективную работу по организации безопасности системы.

СПИСОК ЛИТЕРАТУРЫ:

1 Спатулас Г.П., Катсикас С.К. Методы пост-обработки оповещений при обнаружении вторжений: опрос. Международный журнал информатики безопасности №2, 2013. с. 64-80. URL: http://www.ijiss.org/ijiss/index.php/ijiss/article/view/50/pdf_8. (Дата обращения: 10.12.2017).
2 Annual Security Report URL: http://www.cisco.com/c/m/en_us/offers/sc04/2016-annual-security-report/index.html (дата обращения: 20.11.2017).
3 James P. Computer Security Threat Monitoring and Surveillance. Fort Washington, PA: James P. Anderson Co., 1980.
4 Denning D. An intrusion detection model. Proc. of IEEE Symposium on Security and Privacy, 1987, pp.118–131.
5 Глебов М., Селищев И. Системы предотвращения вторжений «из коробки». Тест-драйв. URL: https://habrahabr.ru/company/it/blog/209714/. (дата обращения: 12.12.2017).
6 Правиков Д. И., Закляков П. В. Использование виртуальных ловушек для обнаружения телекоммуникационных атак. Проблемы управления безопасностью сложных систем: Труды международной конференции. Москва, декабрь 2011 г./ Под ред. Архиповой Н. И. и Кульбы В. В. Часть 1. М.: РГГУ - Издательский дом МПА-Пресс. 342 с., с 310-314.
7 Брюховецкий А.А., Сосоновский Ю.В., Милюков В.В. Фундаментальное исследование в области методов построения систем обнаружения и предотвращения сетевых вторжений. Вестник СЕВНТУ. 2014. № 154.С. 60-63.
8 Баччелли Ф., Рыбко Н.А., Шлосман С.Б. Сети массового обслуживания с подвижными приборами – предел среднего поля. Проблемы передачи информации. 2016, том 52:2, 86–110.
9 Пузырьков Д.В., Подрыга О.П., Поляков С.В. Параллельная обработка и визуализация для результатов моделирования методом молекулярной динамики Труды Института системного программирования РАН. Том 28, №2, 2016 г. С. 221-242.
10 Taheri S. JellyFish attack: Analysis, detection and countermeasure in TCP-based MANET. Journal of Information Security and Applications. 22, June 2015, Pages 99-112 URL: https://doi.org/10.1016/j.jisa.2014.09.003 (дата обращения: 12.12.2017).
11 Taheri S. Hartung S. Anonymous group-based routing in MANETs. Journal of Information Security and Applications. Volume 22, June 2015, Pages 87-98. https://doi.org/10.1016/j.jisa.2014.09.002 (дата обращения: 12.12.2017).
12 Вьюкова Н.И., Галатенко В.А., Сумборский С.В. Поддержка параллельного и конкурентного программировнаия в языке С++. Журнал «Программирование». 2017. № 5 С. 48-59
13 Хорошилов А.В., Щепетков И.В. ADV_SPM — Формальные модели политики безопасности на практике Труды Института системного программирования РАН. Том 29, № 3, 2017 г. С. 43-56.
14 Fua Y., Koné O. Model based security verification of protocol implementation. Journal of Information Security and Applications. 22, June 2015, Pages 17-27 URL: https://doi.org/10.1016/j.jisa.2014.08.002 (дата обращения: 12.12.2017).

REFERENCES:

[1] Spatulas G.P., Katsikas S.K. Methods of post-processing of alerts in intrusion detection: a survey. International journal of safety Informatics №2, 2013. p.64-80. URL: http://www.ijiss.org/ijiss/index.php/ijiss/article/view/50/pdf_8. (Data obrashhenija: 10.12.2017). (in Russian).
[2] Annual Security Report URL: http://www.cisco.som /c/m/en_us/offers/ sc04/2016- annual- security -report/ index .html (data obrashhenija: 20.11.2017).
[3] James P. Computer Security Threat Monitoring and Surveillance. Fort Washington, PA: James P. Anderson Co., 1980.
[4] Denning D. An intrusion detection model. Proc. of IEEE Symposium on Security and Privacy, 1987, pp.118–131.
[5] Glebov M., Selishhev I. Intrusion prevention systems "out of the box". Test-drive. URL: https://habrahabr.ru/ company/it/blog /209714/. (data obrashhenija: 12.12.2017). (in Russian).
[6] Pravikov D. I., Zakljakov P. V. The use of virtual traps for detection of telecommunication attacks. Security management problems of complex systems: Proceedings of the international conference. Moskva, dekabr' 2011 g. Pod red. Arhipovoj N. I. i Kul'by V. V. Chast' 1. M.: RGGU - Izdatel'skij dom MPA-Press. 342 p., p 310-314. (in Russian).
[7] Brjuhoveckij A.A., Sosonovskij Ju.V., Miljukov V.V. Fundamental research in the field of methods of construction of detection systems and network intrusion prevention. Vestnik SEVNTU. 2014. № 154.P. 60-63. (in Russian).
[8] Bachchelli F., Rybko N.A., Shlosman S.B. Queueing networks with mobile devices-the limit of the average field. Problems of information transmission. 2016, tom 52:2, p86–110. (in Russian).

[9] Puzyr'kov D.V., Podryga O.P., Poljakov S.V. Parallel processing and visualization to simulation results by the molecular dynamics method Proceedings of Institute for system programming Russian Academy of Sciences. Tom 28, №2, 2016 g. P. 221-242. (in Russian).

[10] Taheri S. JellyFish attack: Analysis, detection and countermeasure in TCP-based MANET. Journal of Information Security and Applications. 22, June 2015, Pages 99-112 URL:https://doi.org/10.1016/j.jisa.2014.09.003 (data obrashhenija: 12.12.2017).

[11] Taheri S. Hartung S. Anonymous group-based routing in MANETs. Journal of Information Security and Applications. Volume 22, June 2015, Pages 87-98. https://doi.org/10.1016/j.jisa.2014.09.002 (data obrashhenija: 12.12.2017).

[12] V'jukova N.I., Galatenko V.A., Sumborskij S.V. Support for parallel and competitive programming in C++. The Journal "Programming". 2017. № 5 P. 48-59. (in Russian).

[13] Horoshilov A.V., Shhepetkov I.V. ADV_SPM — Formal models of security policy in practice the Proceedings of the Institute for system programming Russian Academy of Sciences. Tom 29, № 3, 2017 g. P. 43-56. (in Russian).

[14] Fua Y., Koné O. Model based security verification of protocol implementation. Journal of Information Security and Applications. 22, June 2015, Pages 17-27 URL: https://doi.org/10.1016/j.jisa.2014.08.002 (data obrashhenija: 12.12.2017).

Поступила в редакцию – 18 декабря 2017 г. Окончательный вариант –08 февраля 2018 г.
Received – December 18, 2017. The final version – February 08, 2018.

Юрий Е. Козлов
Финансовый университет при Правительстве Российской Федерации (Финансовый университет),
Ленинградский проспект, 49, Москва, 125993, Россия
e-mail: kozlovye@yandex.ru, https://orcid.org/0000-0002-4448-0232

ПОДХОДЫ К ОПРЕДЕЛЕНИЮ НАДЕЖНОСТИ МУЛЬТИМОДАЛЬНОЙ ТРЕХМЕРНОЙ ДИНАМИЧЕСКОЙ ПОДПИСИ

DOI: http://dx.doi.org/10.26583/bit.2018.1.07

Аннотация. Рынок современных мобильных приложений предъявляет все более жесткие требования к надежности систем аутентификации. В статье рассматривается аутентификация с использованием мультимодальной трехмерной динамической подписи (МТДП), которая может использоваться в качестве основного или дополнительного средства аутентификации пользователей в мобильных приложениях. В ее основе лежит использование жеста в воздухе, выполняемого двумя независимыми мобильными устройствами в качестве идентификатора. Методика использования МТДП имеет ряд преимуществ по сравнению с используемыми в настоящее время биометрическими методиками, такими как отпечаток пальца, аутентификация по форме лица или речевая аутентификация. Она позволяет быстро сменить жест, который служит идентификатором, а также скрывать саму процедуру аутентификации, используя жесты, не привлекающие внимание. Несмотря на преимущества, использование МТДП имеет ряд ограничений, прежде всего — это необходимость выработки человеком функционально динамического комплекса (ФДК). Он необходим для повторения аутентифицирующего жеста с достаточной точностью. Для корректного формирования МТДП необходима система, реализующая оценку надежности жеста, а также его допустимые вариации. Подходы к решению данной задачи описаны в данной статье с разделением их по способам их реализации. Два подхода могут быть реализованы только с использованием сервера, как центра обработки МТДП, а один может быть реализован с использованием вычислительных ресурсов смартфона. В заключительной части статьи приведены данные опробования одной из методик на макете, реализующем аутентификацию при помощи МТДП.

Ключевые слова: аутентификация, мобильное устройство, акселерометр, персонализированный жест, подпись в воздухе, аутентификация жестом.
Для цитирования. ***КОЗЛОВ, Юрий Е.*** *ПОДХОДЫ К ОПРЕДЕЛЕНИЮ НАДЕЖНОСТИ МУЛЬТИМОДАЛЬНОЙ ТРЕХМЕРНОЙ ДИНАМИЧЕСКОЙ ПОДПИСИ. Безопасность информационных технологий, [S.l.], v. 25, n. 1, p. 74-80, 2018. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1095>. Дата доступа: 15 feb. 2018. doi:http://dx.doi.org/10.26583/bit.2018.1.07.*

Yury E. Kozlov
Financial University under the Government of the Russian Federation (Financial University),
Leningradsky Prospekt, 49, Moscow, 125993 (ГСП-3), Russia
e-mail: kozlovye@yandex.ru, https://orcid.org/0000-0002-4448-0232

Approaches to determining the reliability of a multimodal three-dimensional dynamic signature

DOI: http://dx.doi.org/10.26583/bit.2018.1.07

Abstract. The market of modern mobile applications has increasingly strict requirements for the authentication system reliability. This article examines an authentication method using a multimodal three-dimensional dynamic signature (MTDS), that can be used both as a main and

additional method of user authentication in mobile applications. It is based on the use of gesture in the air performed by two independent mobile devices as an identifier.
The MTDS method has certain advantages over currently used biometric methods, including fingerprint authentication, face recognition and voice recognition. A multimodal three-dimensional dynamic signature allows quickly changing an authentication gesture, as well as concealing the authentication procedure using gestures that do not attract attention. Despite all its advantages, the MTDS method has certain limitations, the main one is building functionally dynamic complex (FDC) skills required for accurate repeating an authentication gesture.
To correctly create MTDS need to have a system for assessing the reliability of gestures. Approaches to the solution of this task are grouped in this article according to methods of their implementation. Two of the approaches can be implemented only with the use of a server as a centralized MTDS processing center and one approach can be implemented using smartphone's own computing resources. The final part of the article provides data of testing one of these methods on a template performing the MTDS authentication.
Keywords: authentication, mobile device, accelerometer, personalized gestured, in-air signature, handwaving authentication.
For citation. ***KOZLOV, Yury E.*** *Approaches to determining the reliability of a multimodal three-dimensional dynamic signature. IT Security (Russia), [S.l.], v. 25, n. 1, p. 74-80, 2018. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1095>. Date accessed: 15 feb. 2018. doi:http://dx.doi.org/10.26583/bit.2018.1.07.*

ВВЕДЕНИЕ

Развитие информационных технологий и тренд мобильности привели к тому, что современное мобильное устройство – смартфон/планшет или иной «гаджет» зачастую используется в качестве мобильного офиса, центра развлечений и инструмента для потребления Интернет-контента. Использование биометрических методик аутентификации в мобильных приложениях повышает информационную безопасность. Это связано с таким свойством биометрии как неотторжимость биометрического признака. Однако возросло количество сообщений о краже и фальсификации биометрических признаков [1, 2]. Это, прежде всего, связано с тем, что в подавляющее большинство этих признаков, таких как отпечаток пальца, радужная оболочка глаза и речь не могут быть скрыты. Кроме того, методики аутентификации при помощи данных признаков тоже не являются секретом.

Противодействие подделкам биометрических признаков идет в двух направлениях – разработка новых методик защиты биометрических параметров [3-5], а также разработка новых методик. Например, делаются попытки сделать систему, делающую традиционные биометрические признаки модифицируемыми и сменяемыми [6]. Среди работ по поиску легко модифицируемых и сменяемых биометрических признаков стоит выделить аутентификацию при помощи жеста [7-9]. Мультимодальная трехмерная динамическая подпись (МТДП) является одной из таких методик и может быть использована как основное, так и резервное средство. МТДП имеет ряд преимуществ перед традиционными биометрическими методиками, используемыми в мобильных приложениях, таких как отпечаток пальца, распознавание по радужной оболочки глаза, распознавание лица, а также распознавание речевых характеристик. Это, прежде всего, возможность скрытой аутентификации и быстрой смены признака. Однако МТДП имеет ряд недостатков, главным из которых является необходимость запоминания жеста, служащего биометрическим признаком, или если говорить научным языком - выработка при этом функционально-динамического комплекса навыков (ФДК). Одним из средств, которые могут помочь в этом пользователю, является создание системы классификации жестов. Такая система позволит выдавать пользователю оценку надежности жеста и рекомендации по его использованию.

Варианты реализации аутентификация при помощи МТДП

Методика МТДП основана на использовании специального жеста для аутентификации, который регистрируется акселерометрами двух устройств – смартфона и умных часов. Данные акселерометра от умных часов по bluetooth попадают в смартфон. Дальнейшие вычисления могут идти в смартфоне или передаваться на сервер.

Фактически МТДП представляет собой «эталоны» и «пороги». Эталоны - это данные акселерометров умных часов и смартфона, полученные во время жеста, который пользователь выбирает как свою мультимодальную трехмерную подпись. «Пороги» - это максимально возможный разброс значений акселерометров, при превышении которых аутентификация будет считаться не пройденной.

Данные акселерометров устройств, участвующих в формировании МТДП и аутентификации, являются временными рядами и для нахождения меры схожести использование хорошо зарекомендовавшего себя алгоритма DTW (алгоритм трансформации временной шкалы) для сравнения жеста с эталоном [10, 11]. Суть алгоритма в вычислении нелинейного отображения одного временного ряда в другой с помощью минимизации расстояний между ними.

Допустим имеется эталон $Q = q_1,q_2,\ldots,q_n$ и воспроизведенный жест $C = c_1,c_2,\ldots,c_m$, тогда с помощью алгоритма DTW по формуле (1) можно определить кратчайший путь W [12]:

$$DTW(Q,C) = min\left\{\frac{\sum_{k=1}^{k} d(w_k)}{K}\right\}, \quad (1)$$

где K - длина пути, $d(w_k) =(q_i-c_j)^2$ - элемент пути.

В ходе исследования жестов в качестве идентификаторов использовались два макета - МТДП1 и МТДП2. Макет МТДП1 предполагал выработку двух порогов для смартфона и часов по формулам (2). Под порогом срабатывания подразумевается значение, при превышении которого, аутентификация считается не пройденной:

$$\begin{aligned} P_s &= DTW(X_s,X_{se}) + DTW(Y_s,Y_{se}) + DTW(Z_s,Z_{se}) \\ P_w &= DTW(X_w,X_{we}) + DTW(Y_w,Y_{we}) + DTW(Z_w,Z_{we}), \end{aligned} \quad (2)$$

где P_s и P_w – соответственно меры схожести жеста с эталоном смартфона и жеста с эталоном умных часов; X_s, Y_s, Z_s – значения ускорений по трем осям, полученные от смартфона; X_w,Y_w, Z_w - значения ускорений по трем осям, полученные от умных часов; X_{se}, Y_{se}, Z_{se}, X_{we},Y_{we}, Z_{we} - значения ускорений, хранящиеся в качестве эталона, для трех осей смартфона и трех осей умных часов.

Для второго макета пороги вырабатываются для каждой координаты отдельно (3):

$$\begin{aligned} P_{sx} = DTW(X_s,X_{se});\ P_{sy} = DTW(Y_s,Y_{se});\ P_{sz} = DTW(Z_s,Z_{se}) \\ P_{wx} = DTW(X_w,X_{we});\ P_{wy} = DTW(Y_w,Y_{we});\ P_{wz} = DTW(Z_w,Z_{we}), \end{aligned} \quad (3)$$

где P_{sx}, P_{sy}, P_{sz} - меры схожести жеста с эталоном смартфона, P_{wx}, P_{wy}, P_{wz} - меры схожести жеста с эталоном умных часов.

Решение об успешной аутентификации A=1 принимается в случае, если меры схожести между воспроизведенным жестом и эталонами смартфона и умных часов не превышают установленных порогов – формулы (4) и (5) для первого и второго макетов, соответственно:

$$A = (P_s \le P_{se}) \cap (P_w \le P_{we}), \quad (4)$$

$$A = (P_{sx} \le P_{sxe}) \cap (P_{sy} \le P_{sye}) \cap (P_{sz} \le P_{sze}) \cap$$

$$\cap (P_{wx} \leq P_{wxe}) \cap (P_{wy} \leq P_{wye}) \cap (P_{wz} \leq P_{wze}), \quad (5)$$

где P_{se}, P_{sxe}, P_{sye}, P_{sze} - пороги для смартфона, P_{we}, P_{wxe}, P_{wye}, P_{wze} - пороги для умных часов.

Пороги для двух вышеуказанных макетов формируются следующим образом:

- пользователь придумывает жест и принимает решение о том, что он будет эталоном;
- выбранный жест пользователь воспроизводит пять раз. Для каждого раза вычисляются меры схожести по формулам (2) или (3);
- наибольшие меры схожести из пяти попыток выбираются в качестве порогов.

При этом могут возникнуть следующие негативные сценарии формирования МТДП:

- если жесты очень похожи и пороги были установлены слишком жестко, то в реальных условиях возможно большое количество ошибок первого рода - недопуск своего;
- если был выбран слишком простой жест или жесты слишком различались, то пороги будут установлены слишком мягко - это повысит вероятность ошибки второго рода - допуск чужого (иной жест будет принят за подлинный) и ошибка третьего рода – подделка (спуфинг) МТДП.

Оба сценария будут ставить под угрозу информационную безопасность мобильного приложения в случае выбора МТДП в качестве средства аутентификации.

Задачи системы оценки МТДП

Первой и очевидной задачей системы оценки МТДП является определение максимального порога, исходя из характеристик жеста – чем проще жест, тем жестче должен быть установлен порог. Это необходимо для того, чтобы ошибки третьего и второго рода для всех видов жестов была в допустимых пределах.

Исходя из назначения мобильного приложения, система оценки МТДП может решать еще одну задачу – выдавать рекомендацию к применению. Так, например, для входа в банковские приложения стоит рекомендовать более сложные жесты, а для разблокировки смартфона можно использовать более простые. Отсюда вытекает еще одна задача – система не должна пропускать слишком простые жесты. Например, когда пользователь вместо жеста будет держать телефон на одном месте.

Важно отметить, что, поскольку МТДП предполагает жесткую связку смартфона и умных часов, то системе оценки достаточно работать только с показаниями смартфона – оценивая только жест, зарегистрированный им. Далее в статье все оценки будут предполагать оценку данных только смартфона.

Прежде чем искать пути реализации системы оценки МТДП стоит определить диапазон работы этой системы. Одной из самых очевидных характеристик, позволяющих провести такой анализ, является сумма значений временных рядов МТДП.

В таблице 1 представлены результаты суммирования всех значений временных рядов (какими являются показания акселерометра по трем осям), выполненные по формуле (6) для различных жестов:

$$M = \sum_1^i |x_i| + |y_i| + |z_i|, \quad (6)$$

где M – сумма всех значений ускорений по трем осям, i – количество значений во временном ряду, x_i, y_i, z_i – показания акселерометра для осей x, y и z. При этом влияние гравитации убрано согласно рекомендациям разработчиков ОС Android.

Таблица 1. Результаты суммирования временных рядов МТДП для разных жестов.

Жест	Сумма значений M
Круг	250 - 350
Квадрат	300 - 450
Крест	1300 - 1700
Тряска смартфона	3000 - 5000

Время воспроизведения всех указанных жестов примерно равно 1 с. Предельная же сумма значений с учетом максимального значения ускорения равного 39 м/с^2 и частоте работы акселерометра 1600 Гц равна 187200 за одну секунду.

Так как система оценки МТДП должна быть доступна широкому кругу пользователей, то представляется целесообразным, свести задачу системы к отнесению выбранного жеста к одному из четырех классов:

- высокая надежность;
- средняя надежность;
- низкая надежность;
- недопустимая МТДП.

При этом внутренний алгоритм может использовать более широкий диапазон классов для реализации более тонкой настройки.

Подходы к реализации системы оценки МТДП

Можно выделить три наиболее подходящих методики решения задачи классификации МТДП:

1) использование метода KNN – k - ближайших соседей;
2) использование нейронной сети;
3) ранжирование надежности в зависимости от M (суммы модулей ускорений).

Методика KNN–k - ближайших соседей широко используется для анализа рукописных подписей [13]. Она предполагает создание базы МТДП ранжированных по классам от высокой надежности до недопустимой МТДП. При создании подписи происходит вычисление меры схожести к каждому объекту в базе. В качестве меры схожести также может быть использован алгоритм DTW (7):

$$Q_j = \sum_{i=1}^{n} \frac{1}{DTW(x,a_i)}, \quad (7)$$

где Q_j – классы МТДП, x – воспроизведенный жест, a_i - объекты класса.

Вторая методика – использование нейронной сети также используется для анализа рукописной подписи [14]. Для использования данной технологии, как и для метода k-ближайших соседей, должен быть использован сервер, как центр обработки МТДП.

Для создания классификатора МТДП могут использоваться нейронные сети хорошо себя зарекомендовавшие в распознавании рукописных подписей:

1)персептроны, ГОСТ Р 52633.5-2011, и их модификации;
2)нечеткий экстрактор;
3)сети квадратичных форм.

Методика KNN – k - ближайших соседей и использование нейронной сети не могут использовать вычислительные ресурсы только смартфона, однако такая реализация МТДП может потребоваться, например, для разблокировки смартфона.

Методика ранжирования надежности в зависимости от суммы модулей всех значений ускорений – M для своей работы может использовать ресурсы только

смартфона. Суть ее в классификации МТДП в зависимости от М. Кроме того следует ввести ограничение на максимально возможный порог P_{max}. Так как от величины М должна зависеть величина порога, можно устанавливать P_{max} в зависимости от М (8):

$$P_{max} = \frac{M}{M+\Delta}, \quad (8)$$

где Δ - значение, которое может быть рассчитано экспериментально и будет ограничивать P_{max}. Пример ограничения по P_{max} показан кривой на рисунке 1.

Жесты, имеющие слишком маленькое значение М, либо слишком большой разброс $P>P_{max}$, стоит признать недопустимыми. Для остальных жестов эмпирически могут быть подобраны значения М, при превышении которых жест будет попадать в классы высокой, средней или низкой надежности.

На рисунке 1 представлены результаты опробования макета МТДП1 на группе из пяти человек.

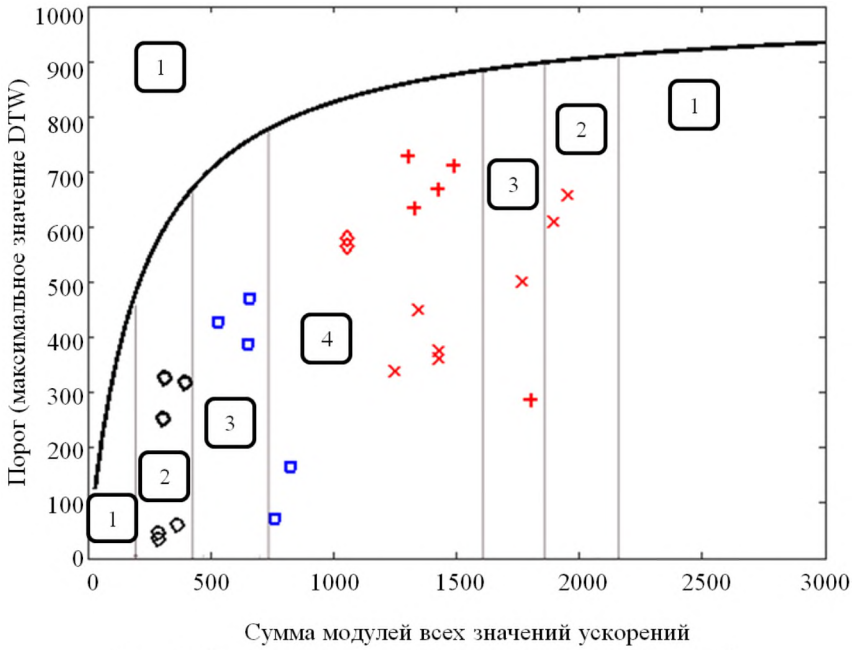

Рис. 1. Результаты опробования макета МТДП1)
(Fig. 1. Results of testing the layout of MTDP1)

На рисунке 1 кроме ограничения, заданного по формуле (8), показаны зоны, ранжированные по величине М:

1 - зона недопустимых жестов;

2 - зона жестов с низкой надежностью;

3 - зона жестов со средней надежностью;

4 - зона жестов с высокой надежностью.

Для каждого представленного на рисунке 1 жеста были проведены проверки воспроизводимости и не менее пяти попыток взлома (спуфинга), когда жест выполнялся другим человеком.

Заключение

Несмотря на участившиеся сообщения о возможностях подделки и кражи биометрических признаков, использование биометрии в системах верификации и аутентификации продолжит расти. Новые технологии будут применяться и в смежных областях деятельности человека, например, бумажном документообороте [15]. Система аутентификации личности на основе МТДП может получить распространение в мобильных приложениях за счет ее преимуществ перед ныне используемыми

биометрическими технологиями, такими как возможность скрытной аутентификации и быстрая смена идентификатора. Реализация системы оценки жеста позволит сделать его удобным для использования и повысить его характеристики с точки зрения надежности.

СПИСОК ЛИТЕРАТУРЫ:

1 Abhishek K., Yogi A. «A minutiae Count Based Method for Fake Fingerprint Detection» Procedia Computer Science. – 2015. – Т. 58. – P. 447-452.
2 Chingovska I. Trustworthy Biometric Verification under Spoofing Attacks. – 2016.
3 Козлачков С.Б., Дворянкин С.В., Бонч-Бруевич А.М. «Проблемы и перспективы защиты акустической речевой информации». Специальная техника. – 2016. – №. 6. – С. 15-21.
4 Galbally J., Gomez-Barrero M. «A review of iris anti-spoofing». Biometrics and Forensics (IWBF), 2016 4th International Workshop on. – IEEE, 2016. – P. 1-6.
5 Sinha V.K., Gupta A. «Enhancing Iris Security by Detection of Fake Iris». National Conference Gyan Jyoti–National Conference MITE. – 2016. – P. 1-22.
6 Patel V. M., Ratha N. K., Chellappa R. Cancelable biometrics: A review IEEE Signal Processing Magazine. – 2015. – Т. 32. – №. 5. – P. 54-65.
7 Wang Z., Shen C., Chen Y. Handwaving Authentication: Unlocking Your Smartwatch Through Handwaving Biometrics. Chinese Conference on Biometric Recognition. – Springer, Cham, 2017. – P. 545-553.
8 Casanova J. G. et al. A real-time in-air signature biometric technique using a mobile device embedding an accelerometer. International Conference on Networked Digital Technologies. – Springer, Berlin, Heidelberg, 2010. – P. 497-503.
9 Козлов Ю.Е., Евсеев В.Л. «Мультимодальная трехмерная динамическая подпись». Безопасность информационных технологий. – 2017 г., № 4, С. 44-51.
10 Козлов Ю.Е., Евсеев В.Л. «Метаматематическая модель мультимодальной жестовой аутентификации при помощи двух независимых мобильных устройств». Безопасность информационных технологий. – 2017 г., № 1, С. 49-55.
11 Bailador G. et al. «Analysis of pattern recognition techniques for in-air signature biometrics». Pattern Recognition. – 2011. – Т. 44. – №. 10. – P. 2468-2478.
12 Salvador S., Chan P. «Toward accurate dynamic time warping in linear time and space». Intelligent Data Analysis. – 2007. – Т. 11. – №. 5. – P. 561-580.
13 Kaur J., Sharma R. «A comparison of artificial neural network and k-nearest neighbor classifiers in the off-line signature verification». International Journal. – 2017. – Т. 8. – №. 7. P. 380-383.
14 Ложников П.С. и др. «Экспериментальная оценка надежности верификации подписи сетями квадратичных форм, нечеткими экстракторами и персептронами». Информационно-управляющие системы. – 2016. – №. 5 (84). С. 73-85.
15 Алюшин А.М., Дворянкин С.В. «Использование речевых технологий для защиты документооборота». Безопасность информационных технологий. – 2017. № 2. С. 6-15.

REFERENCES:

[1] Abhishek K., Yogi A. «A minutiae Count Based Method for Fake Fingerprint Detection». Procedia Computer Science. – 2015. – Т. 58. – P. 447-452.
[2] Chingovska I. Trustworthy Biometric Verification under Spoofing Attacks. – 2016.
[3] Kozlachkov S.B., Dvorjankin S.V., Bonch-Bruevich A.M. «Problems and prospects of protection of acoustic speech information". Special equipment. – 2016. – №. 6. – P. 15-21. (in Russian)
[4] Galbally J., Gomez-Barrero M. «A review of iris anti-spoofing». Biometrics and Forensics (IWBF), 2016 4th International Workshop on. – IEEE, 2016. – P. 1-6.
[5] Sinha V. K., Gupta A. «Enhancing Iris Security by Detection of Fake Iris». National Conference Gyan Jyoti – National Conference MITE. – 2016. – P. 1-22.
[6] Patel V. M., Ratha N. K., Chellappa R. Cancelable biometrics: A review. IEEE Signal Processing Magazine. – 2015. – T. 32. – №. 5. – P. 54-65.
[7] Wang Z., Shen C., Chen Y. Handwaving Authentication: Unlocking Your Smartwatch Through Handwaving Biometrics. Chinese Conference on Biometric Recognition. – Springer, Cham, 2017. – P. 545-553.
[8] Casanova J. G. et al. A real-time in-air signature biometric technique using a mobile device embedding an accelerometer. International Conference on Networked Digital Technologies. – Springer, Berlin, Heidelberg, 2010. – P. 497-503.
[9] Kozlov Ju.E., Evseev V.L. « Multimodal three-dimensional dynamic signature". Security of information technologies. – 2017 г., № 4, P. 44-51. (in Russian)
[10] Kozlov Ju.E., Evseev V.L. «Metamathematics model multimodal gestural authentication with two independent mobile devices." Security of information technologies. – 2017 г., № 1, P. 49-55. (in Russian)
[11] Bailador G. et al. «Analysis of pattern recognition techniques for in-air signature biometrics». Pattern Recognition. – 2011. – T. 44. – №. 10. – P. 2468-2478.
[12] Salvador S., Chan P. «Toward accurate dynamic time warping in linear time and space». Intelligent Data Analysis. – 2007. – T. 11. – №. 5. – P. 561-580.
[13] Kaur J., Sharma R. «A comparison of artificial neural network and k-nearest neighbor classifiers in the off-line signature verification». International Journal. – 2017. – T. 8. – №. 7. P. 380-383.
[14] Lozhnikov P. S. i dr. «Experimental estimation of reliability of signature verification by networks of quadratic forms, fuzzy extractors and perceptrons". Information and control systems. – 2016. – №. 5 (84). P. 73-85. (in Russian)
[15] Aljushin A.M., Dvorjankin S.V. « Use of speech technologies to protect document flow". Security of information technologies. – 2017. № 2. P. 6-15. (in Russian)

Поступила в редакцию – 18 декабря 2017 г. Окончательный вариант – 06 февраля 2018г.
Received – December 18, 2017. The final version – February 06, 2018.

Эдита К. Куулар[1], Андрей И. Труфанов[1], Алексей А. Тихомиров[2]
[1]Иркутский Национальный Исследовательский Технический Университет,
Лермонтова, 83, Иркутск, 6664074, Россия
e-mail: kuular1991@mail.ru, https://orcid.org/0000-0003-4832-3397
e-mail: troufan@gmail.com, https://orcid.org/0000-0002-6967-3495
[2]Университет ИНХА,
Инчеон, Республика Корея
e-mail: alexeitikhomirovprof@gmail.com, https://orcid.org/0000-0002-7317-5851

ДВУХКОМПОНЕНТНАЯ СЕТЕВАЯ МОДЕЛЬ В ТЕХНОЛОГИЯХ ГОЛОСОВОЙ ИДЕНТИФИКАЦИИ ЛИЧНОСТИ

DOI: http://dx.doi.org/10.26583/bit.2018.1.08

Аннотация. Среди важнейших параметров биометрических систем голосовой модальности, определяющих их эффективность, наряду с надежностью и помехоустойчивостью выделяют скорость идентификации и верификации личности. Данный параметр особенно чувствителен при обработке крупномасштабных баз голосовых данных в режиме реального времени. Многие исследовательские работы в данной области направлены на разработку новых и совершенствование имеющихся алгоритмов представления и обработки речевых записей, обеспечивающих высокую производительность голосовых биометрических систем. Здесь перспективным представляется современный подход к решению сложных объемных задач с большим числом элементов и учетом их взаимосвязей, использующий платформу комплексных сетей. Так, известны работы, в которых при решении задачах анализа и распознавания лиц по фотографиям изображения трансформируются в комплексные сети для последующей их обработки стандартными приемами. Одним из первых применений комплексных сетей в задачах анализа звуковых рядов (музыкальных и речевых) являлось описание их частотных характеристик с помощью построения сетевых моделей – конвертации рядов в сети. На платформе сетевой онтологии в данной работе развит предложенный ранее метод представления аудиоинформации с целью ее высокопроизводительного автоматического анализа и снижения погрешности в распознавании личности – диктора. Для этого предполагается конвертирование звуковой информации в форму ассоциативной семантической (когнитивной) сетевой структуры, содержащей две компоненты: амплитудную и частотную. Были записаны два речевых примера с последующей их трансформацией в соответствующие сети и сравнением топологических метрик. Набор топологических метрик каждой из сетевых моделей (амплитудной и частотной) представляет собой вектор, а вместе - матрицу, как цифровой "сетевой" отпечаток голоса. Предлагаемый сетевой подход с его чувствительностью к состоянию индивида – физиологическому, психологическому, эмоциональному, может оказаться полезным не только для задач идентификации личности, но и для определения ее состояния.

Ключевые слова: биометрические модальности, звуковая информация, идентификация диктора, комплексные сети, амплитуда, частота.

Для цитирования. ***КУУЛАР, Эдита К.; ТРУФАНОВ, Андрей И.; ТИХОМИРОВ, Алексей А.*** *ДВУХКОМПОНЕНТНАЯ СЕТЕВАЯ МОДЕЛЬ В ТЕХНОЛОГИЯХ ГОЛОСОВОЙ ИДЕНТИФИКАЦИИ ЛИЧНОСТИ. Безопасность информационных технологий, [S.l.], v. 25, n. 1, p. 81-89, 2018. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1096>. Дата доступа: 15 feb. 2018. doi:http://dx.doi.org/10.26583/bit.2018.1.08.*

Edita K. Kuular[1], Andrey I. Trufanov[1], Alexei A. Tikhomirov[2]
[1]*Irkutsk National Research Technical University,*
Lermontov street,83, Irkutsk,664074,Russia
e-mail: kuular1991@mail.ru, https://orcid.org/0000-0003-4832-3397
e-mail: troufan@gmail.com, https://orcid.org/0000-0002-6967-3495
[2]*INHA University,*
Incheon, Republic of Korea
e-mail: alexeitikhomirovprof@gmail.com, https://orcid.org/0000-0002-7317-5851

Two-component network model in voice identification technologies

DOI: http://dx.doi.org/10.26583/bit.2018.1.08

Abstract. Among the most important parameters of biometric systems with voice modalities that determine their effectiveness, along with reliability and noise immunity, a speed of identification and verification of a person has been accentuated. This parameter is especially sensitive while processing large-scale voice databases in real time regime. Many research studies in this area are aimed at developing new and improving existing algorithms for presentation and processing voice records to ensure high performance of voice biometric systems. Here, it seems promising to apply a modern approach, which is based on complex network platform for solving complex massive problems with a large number of elements and taking into account their interrelationships. Thus, there are known some works which while solving problems of analysis and recognition of faces from photographs, transform images into complex networks for their subsequent processing by standard techniques. One of the first applications of complex networks to sound series (musical and speech) analysis are description of frequency characteristics by constructing network models - converting the series into networks. On the network ontology platform a previously proposed technique of audio information representation aimed on its automatic analysis and speaker recognition has been developed. This implies converting information into the form of associative semantic (cognitive) network structure with amplitude and frequency components both. Two speaker exemplars have been recorded and transformed into pertinent networks with consequent comparison of their topological metrics. The set of topological metrics for each of network models (amplitude and frequency one) is a vector, and together those combine a matrix, as a digital "network" voiceprint. The proposed network approach, with its sensitivity to personal conditions-physiological, psychological, emotional, might be useful not only for person identification, but also for determining his /her condition.

Keywords: biometric modalities, sound information, speaker identification, complex net-works, amplitude, frequency.

For citation. ***KUULAR, Edita K.; TRUFANOV, Andrey I.; TIKHOMIROV, Alexei A.*** *Two-component network model in voice identification technologies. IT Security (Russia), [S.l.], v. 25, n. 1, p. 81-89, 2018. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1096>. Date accessed: 15 feb. 2018. doi:http://dx.doi.org/10.26583/bit.2018.1.08.*

Введение.

В последнее время биометрия – наука о распознавании личности по ее физическим и поведенческим признакам – стремительно развивалась, а ее достижения нашли применение в ряде областей, таких как правоохранительные, медицинские и финансовые службы [1]. Основная задача биометрической системы заключается в сравнении двух биометрических экземпляров и установлении принадлежности их к одной или разным личностям. Как в целом в проблеме управления доступом выделяют два класса задач – идентификации и аутентификации субъектов. Можно отметить, что субъект является носителем модуля биометрик – идентификаторов и одновременно признаков, позволяющих провести проверку – верификацию- и тем самым подтвердить или опровергнуть искомую аутентичность. Характерно, что для биометрии трудности задач идентификации в большей мере носят технологический характер, когда одна

регистрируемая биометрика пользователя сравнивается со всеми N, хранящимися в базе данных, (1:N). Так, Integrated Automated Fingerprint System (IAFIS), репозитарий в США, управляемый ФБР в 2016 году содержал сведения о более чем 100 млн. лиц, давая возможность доступа к базе данных правоохранительным органам в режиме 24x7x365 [2].

Биометрическая аутентификация не предполагает сравнения регистрируемой биометрики со всеми записями в репозитарии, а только с единственной, (1:1), но для поддержки формального подтверждения подлинности необходимы сложные организационно-правовые решения, включая стандартизацию процессов, принятие протоколов.

Таким образом технологические требования к решениям (производительности и надежности) проявляются в большей степени в биометрических задачах идентификации.

Анализ голоса представляет собой одну из форм биометрической аутентификации, позволяющая установить личность индивида по набору его уникальных акустических характеристик.

Голосовая модальность, среди прочих [3], демонстрирует свою эффективность в задачах идентификации личности, что особенно важно в телекоммуникационных приложениях. [4] подчеркивалось, что это единственная биометрическая модальность, которая позволяет идентифицировать человека по телефону. Оценка точности идентификации, как правило основывается на характеристике, введенной Национальным институтом стандартов и технологий США (National Institute of Standards and Technology, NIST)- Equal Error Rate, EER, равной ошибке первого и второго рода: FRR=FAR. (Традиционно, под ошибкой первого рода подразумевается отказ в правах легальному пользователю, FRR; ошибка второго рода, – предоставление прав самозванцу, FAR, при этом с противоположным смыслом в NIST [5]). Среди систем распознавания личности по голосу, использующих базы данных, с голосовыми фразами сотен акторов -дикторов, наилучшие показатели EER составляют 3–5% [6,7]

В настоящее время для голосовой идентификации применяется широкий спектр моделей, методик, программных и технических средств. [8-15]

Главные усилия исследователей и разработчиков в данной предметной области направлены на снижение как погрешности в распознавании личности - диктора, так и сопутствующих технологических затрат в процессе распознавания. В работе [16] было предложено использовать сетевой подход, как позволяющий обойтись низко затратными вычислениями.

Сетевое описание являет собой современную платформу исследований самых разных данных, в т.ч. временных рядов [17] что может представлять интерес для биометрического анализа. Здесь важным представляется разработка схем и алгоритмов трансформации изображений и звуковых записей [18-20] в комплексные сети для последующего их сопровождения надежными эффективными методами теории графов, теории вероятностей и линейной алгебры.

Модель.

Звуковой сигнал можно представить, как совокупность различных синусоидальных составляющих. *Высота звука* - определяется частотой звуковой волны (или, периодом волны). Чем выше частота, тем выше звучание. *Громкость звука* определяется амплитудой сигнала. Чем выше амплитуда звуковой волны, тем громче сигнал.

Известно, что процедура распознавания личности по голосовому биометрическому показателю заключается в сравнении записей голоса, сделанных с помощью различных аудио устройств. Но сравнивать предъявляемый голос с огромным объемом аудио данных с целью выявления совпадения голоса диктора довольно сложно и технологически затратно. В отличие от традиционных методов в [16] предложен метод сравнения аудиоданных путем построения сетевой модели и получения матрицы сетевых метрик. Обеспечивая высокое быстродействие, данный метод, однако, характеризуется

недостаточной надежностью и годится лишь для предварительной (грубой) оценки звуковых записей из-за близости сетевых метрик различных голосовых рядов и, тем самым значительной вероятности ошибок второго рода.

С использованием общего подхода [16] в данной работе ставилась задача сетевого представления аудиоинформации как с целью ее высокопроизводительного автоматического анализа, так и снижения погрешности в распознавании личности – диктора. Решение предполагает конвертирование звуковой информации в форму ассоциативной семантической (когнитивной) сетевой структуры с двумя компонентами: амплитудной и частотной.

Для сравнительного анализа были записаны 2 речевых файла двух разных дикторов в формате WAV. Записи сделаны микрофоном мобильного телефона. Условно речевые акторы- дикторы обозначены как С1 и Э1. С1- мужского рода, 27 лет. Э1- женского рода, 26 лет. В качестве речевой информации, воспроизводимой дикторами выбрано одно предложение с одинаковым количеством слов. Аудио файлы предварительно обрабатывались, переводились из MP3 формата в формат данных WAV.

С помощью специализированной программы Spectral Plus (программа для работы с аудио –файлами [21]) определены временные точки с пиковыми амплитудными и частотными данными. Данные представлены на рис.1-2.

Рис. 1. Диаграмма временных точек с пиковыми амплитудными и частотными показаниями (речевая запись С1)

(Fig. 1. Chart of time points with peak amplitude and frequency indicators (speech record C1))

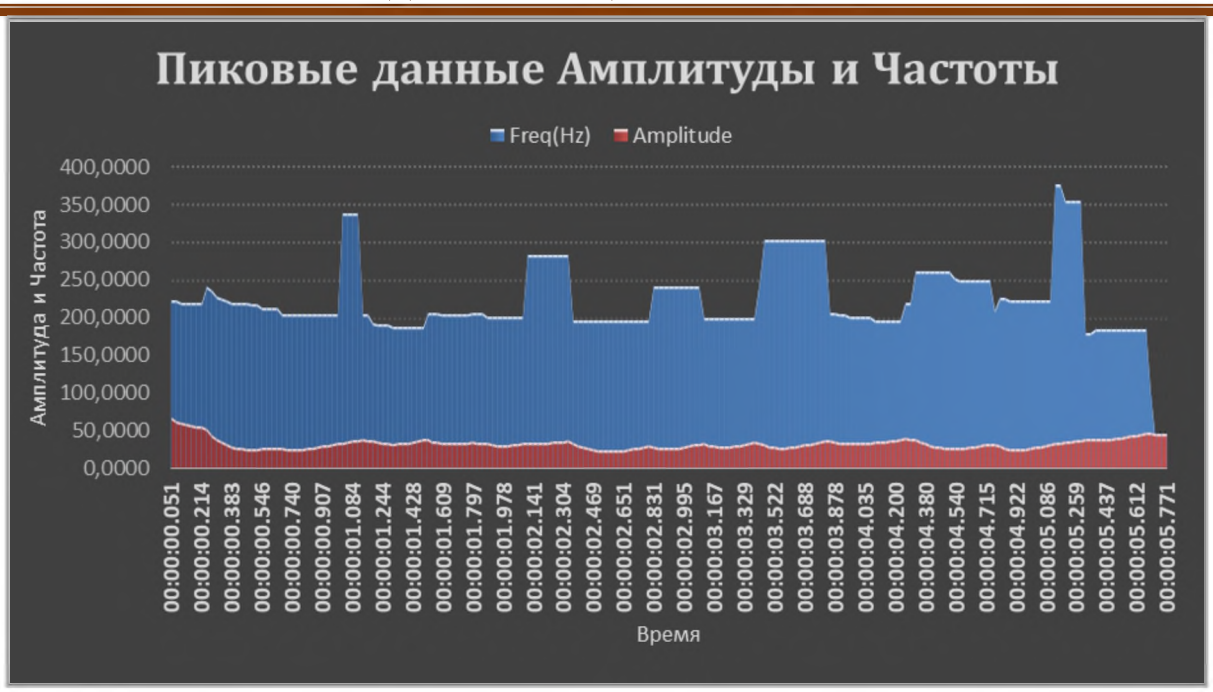

Рис. 2. Диаграмма временных точек с пиковыми амплитудными и частотными показаниями (речевая запись Э1)
(Fig. 2. Chart of time points with peak amplitude and frequency indicators (speech record E1))

Поскольку наблюдения проводятся в некотором временном интервале, то для каждой временной точки следует определить значение амплитуды (рис. 3.) и частоты (рис. 4.) сигнала.

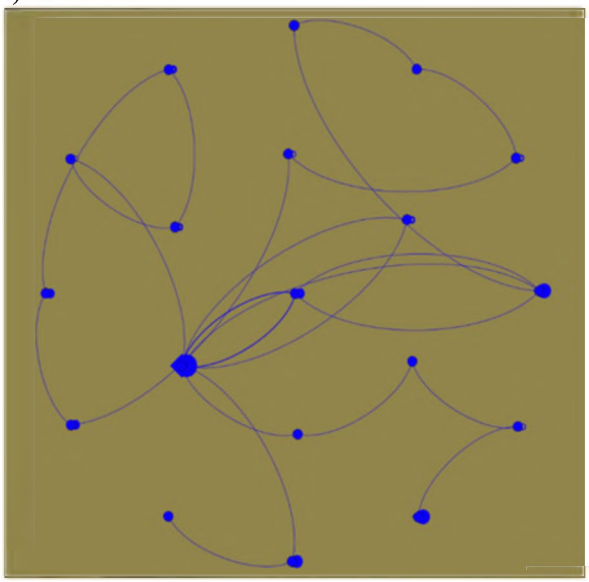

Рис. 3. Граф по частотным показаниям (речевая запись С1)
(Fig. 3. Graph built on frequency indicators (speech record C1))

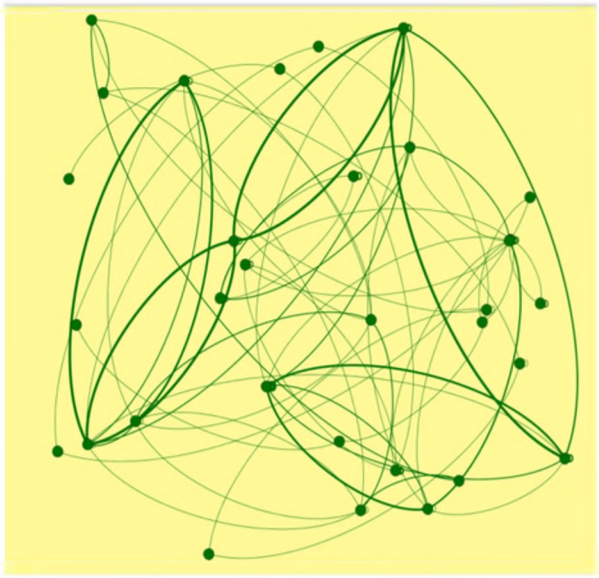

Рис. 4. Граф по амплитудным показаниям (речевая запись С1)
(Fig. 4. Graph built on the amplitude indicators (speech record C1))

В нашем случае при конвертировании данных в комплексную сеть узлом для построения сетевой модели является либо амплитуда (рис. 5.), либо частота (рис. 6.) в определённой временной точке. Подобно [16] за счет применения схемы «модели соседства» [18] устанавливается последовательная связь между узлами – частотами - соседняя

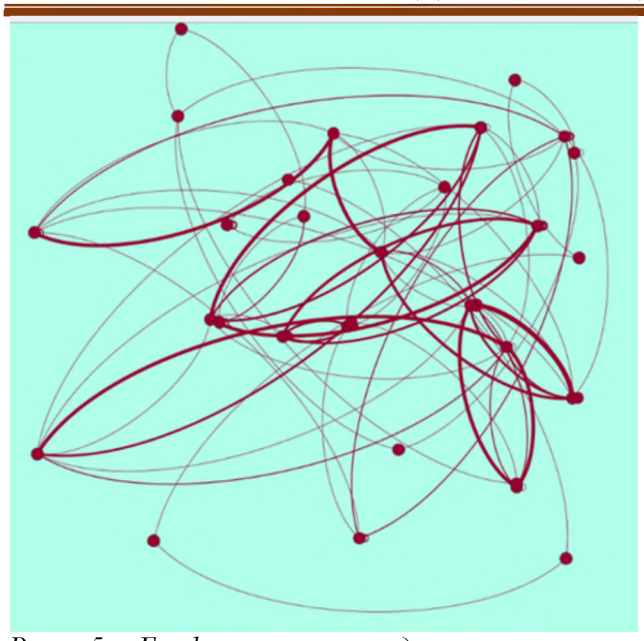

Рис. 5. Граф по амплитудным показаниям (речевая запись Э1)
(Fig. 5. Graph built on the amplitude indicators (speech record E1))

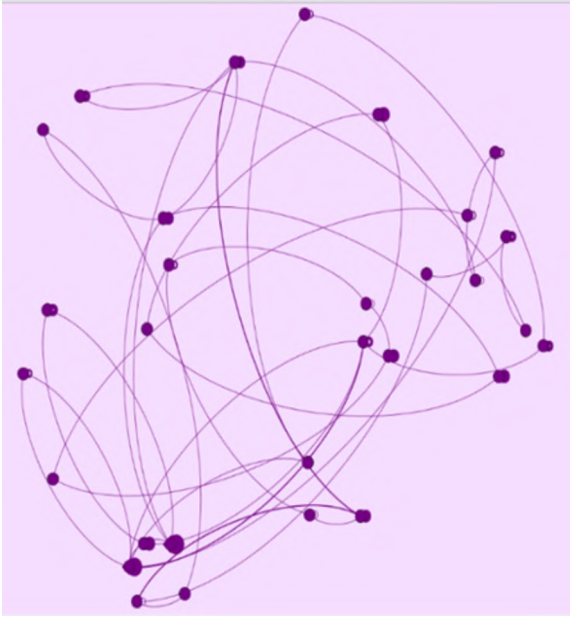

Рис. 6 - Граф по частотным показаниям (речевая запись Э1)
(Fig. 6. Graph built on frequency indicators (speech record E1))

присоединяется к соседней (по значению, не по времени) и, аналогично, между амплитудами. Повторение узлов определено увеличением их весовых значений. Для получения матрицы метрик строятся по отдельности 2 графа по частотным и амплитудным индикаторам. Естественно, что объединить два графа ни в мультиплекс [22], ни в общую стволовую структуру [23] не представляется возможным, хотя изначально данные соответствуют одной временной точке. Отметим, что при установлении связи амплитуда и частота будут определены их первыми значениями. Повторяющееся амплитуды и частоты просто приведут к увеличению весовых значений узлов.

Результаты исследований.

Выбор ключевых сетевых метрик, характеризующих процессы в исследуемой системе является вторым важнейшим этапом после строительства самой сетевой модели.

Таблица 1 Матрица метрик (Речевая запись С1)

метрика	Статистика амплитуды	Статистика частоты
узлы	32	19
ребра	82	37
Средняя степень	2,562	1,947
Средняя взвешенная степень	4,844	3,158
Средний коэффициент кластеризации	0,368	0,32
Средняя длина пути	6,215	5,522

Таблица 2 Матрица метрик (Речевая запись Э1)

метрика	Статистика амплитуды	Статистика частоты
узлы	30	30
ребра	80	62

Средняя степень	2,667	2,067
Средняя взвешенная степень	6,6	6,6
Средний коэффициент кластеризации	0,359	0,272
Средняя длина пути	5,562	5,969

Ряд топологических метрик (2-й и 3-й столбцы в таблицах 1-2) соответственно амплитудной и частотной сетевых моделей речевого текста представляет собой вектор, а вместе - матрицу, как цифровой "сетевой" отпечаток голоса. Этот цифровой отпечаток, в нашем случае – матрица сетевых метрик, должен наилучшим образом отражать индивидуальные голосовые особенности актора- диктора, и при этом в соответствии с требованиями к биометрическим системам безопасности [24] оставаться стабильным во времени, легко измеряемым и не поддаваться имитации. Анализ матриц (Табл.1-2), характеризующих метрики, указывает на их различие, которое обеспечивает возможность надежной идентификации диктора. Для подтверждения чувствительности матрицы метрик к голосу актора-диктора, дальнейшие исследования будет включать сравнение записей одного диктора с аутентичными и неаутентичными записями.

Область применения системы идентификации по голосовым биометрическим данным достаточно обширна: верификация клиентов при доступе к данным, тем более что остальные биометрические данные человека не так-то просто получить через системы удаленного доступа. Обработка речевых баз данных, сравнительный анализ на соответствие данных. Довольно часто применяется в криминалистике.

Данный метод можно применять при верификации, пользователь предъявляет в том или ином виде свой идентификатор, и система распознавания должна сравнить полученную матрицу метрик с имеющейся матрицей метрик соответствующего идентификатору личности предъявителя, и система распознавания должна подтвердить или отвергнуть этот идентификатор. Поскольку пользователь заинтересован в подтверждении его идентификатора, то старается не вносить в речевой пароль вариаций, которые отсутствовали в период записи его голосовых биометрических данных.

Выводы.

Подготовлена двухкомпонентная сетевая модель голосовой биометрической модальности, включающей амплитудную и частотную составляющие, к которым можно применить известные алгоритмы топологического сопоставления. Сделан вывод о том, что матрица ключевых топологических параметров сетевых компонентов модели может служить сетевым цифровым отпечатком, позволяющим эффективно сравнивать голоса предъявителя и имеющиеся в базе данных, в предположении большей чувствительности метода и значительно меньших технологических затрат, чем того требуют традиционные системы.

Планируется исследовать особенности использования сетевых моделей в текст зависимых и текст независимых системах голосовой идентификации.

Важным и необходимым представляется дальнейшее изучение влияния на результаты голосового распознавания личности с помощью сетевых метрик таких факторов, как помехи и шумы, ошибочность произношения, состояние диктора, различие устройств голосовой записи. С другой стороны, если предлагаемый сетевой подход продемонстрирует чувствительность к состоянию индивида – физиологическому, психологическому, эмоциональному, он может оказаться полезным не только для задач идентификации личности, но и для определения ее состояния. Концепцию комплексных сетей, как исследовательскую платформу разумно оценить для применения также к иным биометрическим модальностям.

СПИСОК ЛИТЕРАТУРЫ:

1 Talreja V., Ferrett M. T., Valenti C., Ross A. Biometrics-as-a-Service: A Framework to Promote Innovative Biometric Recognition in the Cloud. arXiv:1710.09183v1. 2017. -6 p. URL: https://arxiv.org/pdf/1710.09183.pdf (дата обращения: 25.11.17)
2 Goode A. Biometric Identification or Biometric Authentication? URL: https://www.veridiumid.com/blog/biometric-identification-and-biometric-authentication/ (дата обращения: 18.02.16)
3 Ibrahim D.R., Tamimi A.A., Abdalla A.M. Performance Analysis of Biometric Recognition Modalities 8th International Conference on Information Technology (ICIT). Amman, Jordan. 2017. pp. 980-984
4 Матвеев Ю.Н. Технологии биометрической идентификации личности по голосу и другим модальностям. Вестник МГТУ им. Н.Э. Баумана. Сер. “Приборостроение”. 2012, С. 46-61
5 Wu J. C., Martin A. F., Greenberg C. S., Kacker R. N. The Impact of Data Dependence on Speaker Recognition Evaluation IEEE/ACM Trans Audio Speech Lang Process. 2017. vol. 25, no.1, pp. 5–18
6 Сорокин В.Н. Распознавание личности по голосу: аналитический обзор. В.Н. Сорокин, В.В. Вьюгин, А.А. Тананыкин. Информационные процессы. 2012. Т. 12, вып. 1. С. 1–30
7 Poddar A., Sahidullah M., Saha G. Performance comparison of speaker recognition systems in presence of duration variability. India Conference (INDICON), 2015 Annual IEEE, 2015 -6 p.
8 Sahidullah M., Saha G. A novel windowing technique for efficient computation of MFCC for speaker recognition. IEEE signal processing letters. 2013. vol. 20. no. 2. pp. 149–152.
9 Bahmaninezhad F., Hansen J.H.L. I-vector/PLDA speaker recognition using support vectors with discriminant analysis. IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). 2017. pp. 5410-5414
10 Yao T., Meng C., Liang H., Jia L. Speaker recognition system based on deep neural networks and bottleneck features. Journal of Tsinghua University (Science and Technology). 2016. vol. 56, no. 11, pp. 1143–1148
11 Shulipa A., Novoselov S., Melnikov A. Approaches for Out-of-Domain Adaptation to Improve Speaker Recognition Performance. A. Ronzhin et al. (Eds.): SPECOM 2016, LNAI 9811.2016. pp. 124–130
12 Reynolds D.A. Gaussian mixture models. Encyclopedia of biometric recognition. Heidelberg: Springer 2015– pp. 827–832
13 Козлов А.В., Кудашев О.Ю., Матвеев Ю.Н., Пеховский Т.С., Симончик К.К., Шулипа А.К. Система идентификации дикторов по голосу для конкурса NIST SRE 2012. Труды СПИИРАН. 2013. Вып. 25. С. 350-370
14 Рахманенко И.А. Программный комплекс для идентификации диктора по голосу с применением параллельных вычислений на центральном и графическом процессорах. Доклады ТУСУРа, Т. 20, № 1, 2017. С. 70-74
15 Идентификация человека по голосу URL: http://infoprotect.net/varia/identifikaciya_po_golosu (дата обращения: 06.11.17)
16 Куулар Э.К., Тихомиров А.А., Труфанов А.И. Идентификация источников звуковой информации методом сетевого анализа. Безопасность информационных технологий 2016. №2 С. 43-48 URL: https://bit.mephi.ru/index.php/bit/article/view/78/85
17 Yang D., Li X. Bridge time series and complex networks with a frequency-degree mapping algorithm. Proc. IEEE International Symposium on Circuits and Systems (ISCAS). 2012. pp.910-913
18 Bezsudnov I.V., Snarskii A.A. From the time series to the complex networks: the parametric (dynamical) natural visibility graph. Physica. 2014 no. 414 pp. 53-60 arXiv:1208.6365 URL: https://arxiv.org/ftp/arxiv/papers/1208/1208.6365.pdf
19 Zinoviev D. Networks of Music Groups as Success Predictors. arXiv:1709.08995v1. 2017 -6 p. URL: https://arxiv.org/abs/1709.08995 (дата обращения: 04.08.17)
20 Ferretti S. On the Complex Network Structure of Musical Pieces: Analysis of Some Use Cases from Different Music Genres. arXiv:1709.09708v1. 2017 -32 p. URL: https://arxiv.org/abs/1709.09708 (дата обращения: 13.09.17)
21 SpectraPLUS ®. Pioneer Hill Software. [Электронный ресурс] URL: http://www.spectraplus.com/
22 Boccaletti S., Bianconi G., Criado R., Del Genio C.I., Gómez-Gardeñes J., Romance M., Sendiña-Nadal I., Wang Z., Zanin M. The structure and dynamics of multilayer networks. Physics Reports, 2014, no. 544 (1) pp. 1-122
23 Тихомиров А. А., Труфанов А. И., Россодивита А. Модель взаимодействующих стволовых сетей в решении задач топологической устойчивости сложных систем. Безопасность информационных технологий. 2013, №1, с.125-126
24 Ворона В. А., Костенко В. О. Биометрические технологии идентификации в системах контроля и управления доступом. Computational nanotechnology. 2016 вып. 3, с. 224–241

REFERENCES:

[1] Talreja V., Ferrett M. T., Valenti C., Ross A. Biometrics-as-a-Service: A Framework to Promote Innovative Biometric Recognition in the Cloud. arXiv:1710.09183v1. 2017. -6 p. URL: https://arxiv.org/pdf/1710.09183.pdf (дата обращения: 25.11.17)
[2] Goode A. Biometric Identification or Biometric Authentication? URL: https://www.veridiumid.com/blog/biometric-identification-and-biometric-authentication/ (дата обращения: 18.02.16)
[3] Ibrahim D.R., Tamimi A.A., Abdalla A.M. Performance Analysis of Biometric Recognition Modalities 8th International Conference on Information Technology (ICIT). Amman, Jordan. 2017. pp. 980-984
[4] Matveev Yu.N. Technologies of biometric identification of a person by voice and other modalities. Vestnik of MSTU. N.E. Bauman. Ser. Instrument making. 2012 P. 46-61. (in Russian).
[5] Wu J. C., Martin A. F., Greenberg C. S., Kacker R. N. The Impact of Data Dependence on Speaker Recognition Evaluation IEEE/ACM Trans Audio Speech Lang Process. 2017. vol. 25, no.1, pp. 5–18
[6] Sorokin V.N. Personality recognition by voice: analytical review. V.N. Sorokin, V.V. Vjugin, A.A. Tananykin. Information Processes. 2012. T. 12, vip. 1. - P. 1-30. (in Russian).
[7] Poddar A., Sahidullah M., Saha G. Performance comparison of speaker recognition systems in presence of duration variability. India Conference (INDICON), 2015 Annual IEEE, 2015 -6 p.
[8] Sahidullah M., Saha G. A novel windowing technique for efficient computation of MFCC for speaker recognition. IEEE signal processing letters. 2013. vol. 20. no. 2. pp. 149–152.
[9] Bahmaninezhad F., Hansen J.H.L. I-vector/PLDA speaker recognition using support vectors with discriminant analysis. IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). 2017. pp. 5410-5414
[10] Yao T., Meng C., Liang H., Jia L. Speaker recognition system based on deep neural networks and bottleneck features. Journal of Tsinghua University (Science and Technology). 2016. vol. 56, no. 11, pp. 1143–1148
[11] Shulipa A., Novoselov S., Melnikov A. Approaches for Out-of-Domain Adaptation to Improve Speaker Recognition Performance. A. Ronzhin et al. (Eds.): SPECOM 2016, LNAI 9811.2016. pp. 124–130
[12] Reynolds D.A. Gaussian mixture models. Encyclopedia of biometric recognition. Heidelberg: Springer 2015– pp. 827–832
[13] Kozlov A.V., Kudashev O.Yu., Matveev Yu.N., Pehovskiy TS, Simonchik K.K., Shulipa A.K. The system of voice announcers identification for the NIST SRE 2012 competition. Proceedings of SPIIRAS. 2013. vol. 25. P. 350-370. (in Russian).
[14] Rakhmanenko I.A. A software package for voice speaker identification using parallel computations on the central and graphics processors. Reports of TUSUR, vol. 20, no. 1, 2017. pp. 70-74. (in Russian).
[15] Identification of a person by voice URL: http://infoprotect.net/varia/identifikaciya_po_golosu (reference date: 06.11.17). (in Russian).
[16] Kuular E.K., Tikhomirov A.A., Trufanov A.I. Identification of sources of sound information using the method of network analysis. Information Technology Security. 2016 No. 2 URL: https://bit.mephi.ru/index.php/bit/article/view/78/85.(in Russian).
[17] Yang D., Li X. Bridge time series and complex networks with a frequency-degree mapping algorithm. Proc. IEEE International Symposium on Circuits and Systems (ISCAS). 2012. pp.910-913
[18] Bezsudnov I.V., Snarskii A.A. From the time series to the complex networks: the parametric (dynamical) natural visibility graph. Physica. 2014 no. 414 pp. 53-60 arXiv:1208.6365 URL: https://arxiv.org/ftp/arxiv/papers/1208/1208.6365.pdf
[19] Zinoviev D. Networks of Music Groups as Success Predictors. arXiv:1709.08995v1. 2017 -6 p. URL: https://arxiv.org/abs/1709.08995 (дата обращения: 04.08.17)
[20] Ferretti S. On the Complex Network Structure of Musical Pieces: Analysis of Some Use Cases from Different Music Genres. arXiv:1709.09708v1. 2017 -32 p. URL: https://arxiv.org/abs/1709.09708 (дата обращения: 13.09.17)
[21] SpectraPLUS ®. Pioneer Hill Software. [Электронный ресурс] URL: http://www.spectraplus.com/
[22] Boccaletti S., Bianconi G., Criado R., Del Genio C.I., Gómez-Gardeñes J., Romance M., Sendiña-Nadal I., Wang Z., Zanin M. The structure and dynamics of multilayer networks. Physics Reports, 2014, no. 544 (1) pp. 1-122
[23] Tikhomirov AA, Trufanov AI, Rossodivita A. A model of interacting stem networks in solving problems of topological stability of complex systems. Security of information technology. 2013, №1, p.125-126. (in Russian).
[24] Vorona VA, Kostenko V. O. Biometric identification technologies in access control systems. Computational nanotechnology. 2016 vol. 3, p. 224-241. (in Russian).

Поступила в редакцию – 28 декабря 2017 г. Окончательный вариант –06 февраля 2018 г.
Received – December 28, 2017. The final version – February 06, 2018.

Игнатий А. Грачков
Федеральная служба по техническому и экспортному контролю,
105175, г. Москва, Старая Басманная, 17
e-mail: ignat958@gmail.com, https://orcid.org/0000-0001-6327-3530

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АСУ ТП: ВОЗМОЖНЫЕ ВЕКТОРА АТАКИ И МЕТОДЫ ЗАЩИТЫ

DOI: http://dx.doi.org/10.26583/bit.2018.1.09

Аннотация. Автоматизированные системы управления технологическими процессами (АСУ ТП) являются важнейшей частью промышленной инфраструктуры и используются на таких объектах, как нефте- и газопроводы, водораспределительные системы, электрические сети, атомные электростанции и производство. На сегодняшний день проблема обеспечения информационной безопасности АСУ ТП стоит довольно остро. Специалистами из разных стран проведено большое количество исследований в данной области. Способность злоумышленников обнаружить промышленные устройства, доступные через Интернет, и получать к ним несанкционированный доступ вызывает тревогу в кругах специалистов по информационной безопасности. Поисковик Shodan предоставляет атакующим мощный инструмент для идентификации автоматизированных системы управления и их компонентов и последующих злонамеренных воздействий на них. В данной статье дано описание типовой АСУ ТП; представлен общий анализ защищенности современных АСУ ТП; описаны возможные вектора атак на АСУ ТП; описан пример получения несанкционированного доступа к АСУ ТП с использованием поисковика Shodan; даны рекомендации по обеспечению информационной безопасности АСУ ТП.
Ключевые слова: автоматизированные системы управления, технологические процессы, АСУ ТП, информационная безопасность, защита информации, вектор атаки, Shodan.
Для цитирования. ***ГРАЧКОВ, Игнатий А.*** *ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АСУ ТП: ВОЗМОЖНЫЕ ВЕКТОРА АТАКИ И МЕТОДЫ ЗАЩИТЫ. Безопасность информационных технологий, [S.l.], v. 25, n. 1, p. 90-98, 2018. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1096>. Дата доступа: 19 feb. 2018. doi:http://dx.doi.org/10.26583/bit.2018.1.09.*

Ignatiy A. Grachkov
FSTEC of Russia,
105175, Moscow, Staraya Basmannaya, 17
e-mail: ignat958@gmail.com, https://orcid.org/0000-0001-6327-3530

Information security of industrial control systems: possible attack vectors and protection methods

DOI: http://dx.doi.org/10.26583/bit.2018.1.09

Abstract. Industrial control systems are employed in numerous critical infrastructure assets including oil and gas pipelines, water distribution systems, electrical power grids, nuclear plants and manufacturing facilities. Today the problem of ensuring information security of the industrial control system is quite acute. Specialists from different countries conducted a large number of studies in this field. The ability of intruders to discover industrial devices accessible via the Internet and to obtain unauthorized access to them is of concern to information security professionals. The Shodan search engine provides the attacker with a powerful tool to identify industrial control systems and their components and subsequent malicious effects on them.
In this article the author describes the typical industrial control system, presents general analy-sis of the security of modern ICS and describes possible attack vectors on the ICS. An example of obtaining unauthorized access to industrial control systems using the Shodan search engine is described and recommendations how to ensure information security of the industrial control system are given.

Keywords: industrial control systems, technological processes, ICS, Information Security, data protection, attack vector, Shodan.

For citation. ***GRACHKOV, Ignatiy A.*** *Information security of industrial control systems: possible attack vectors and protection methods. IT Security (Russia), [S.l.], v. 25, n. 1, p. 90-98, 2018. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1096>. Date accessed: 19 feb. 2018. doi:http://dx.doi.org/10.26583/bit.2018.1.09.*

Введение

Широкий интерес к защищенности промышленных систем возник не так давно, после серии инцидентов со специализированными компьютерными вирусами. Тогда выяснилось, что спецслужбы иностранных государств, конкурирующие корпорации или кибертеррористы могут использовать в своих целях недостаточное внимание к информационной безопасности автоматизированных систем управления технологическими процессами и их компонентов.

На сегодняшний день существует большое количество научных работ в области обеспечения информационной безопасности АСУ ТП [1-3]. Большой интерес у исследователей вызывают уязвимости различных компонентов АСУ ТП и возможность проведения атак на них [4-6]. Многие из уязвимых компонентов автоматизированных систем можно обнаружить напрямую из сети Интернет с помощью поисковика Shodan [7]. Одним из направлений научных изысканий в данной области также является анализ рисков информационной безопасности АСУ ТП [8]. Кроме того, много внимания уделяется сетевой безопасности автоматизированных систем управления [9-12]. По результатам исследования компании Positive Technologies, 54 % всех АСУ ТП уязвимы к различным атакам [13]. И причин столь плачевного положения дел - несколько. Во-первых, это консерватизм руководителей предприятий, которые нацелены на приоритетное обеспечение стабильности производственных процессов, а потому не желают рисковать, внося изменения (пусть даже связанные с безопасностью) в производственные системы. Во-вторых, это морально устаревшие решения, используемые в современных производственных комплексах. В-третьих, отсутствие высококвалифицированных специалистов в области обеспечения ИБ на производстве и КВО.

В отличие от уже привычных вирусов для персональных компьютеров и мобильных телефонов, деструктивное информационно-техническое воздействие на автоматизированные системы управления технологическими процессами несет огромную социальную опасность. Такое «информационное оружие» может привести к серьезным человеческим жертвам [14].

Возможные вектора атаки и их реализация в типовой АСУ ТП

Автоматизированная система управления технологическим процессом (АСУ ТП) - это совокупность технических и программных средств, предназначенных для автоматизации управления технологическим и промышленным оборудованием.

Структура типовой АСУ ТП представляет собой трехуровневую модель (разделение на уровни в соответствии с приказом ФСТЭК России №31) (рис. 1):

- На нижнем уровне располагаются исполнительные механизмы, датчики, приводы, регистраторы и индикаторы, связанные локальной сетью нижнего уровня.
- На среднем уровне находятся программируемые логические контроллеры (ПЛК), которые с помощью аналоговых подключений, полевых шин и проприетарных проколов связаны с устройствами нижнего уровня.
- На верхнем уровне могут располагаться автоматизированные рабочие места сотрудников, сервера, SCADA-системы и человеко-машинный интерфейс.

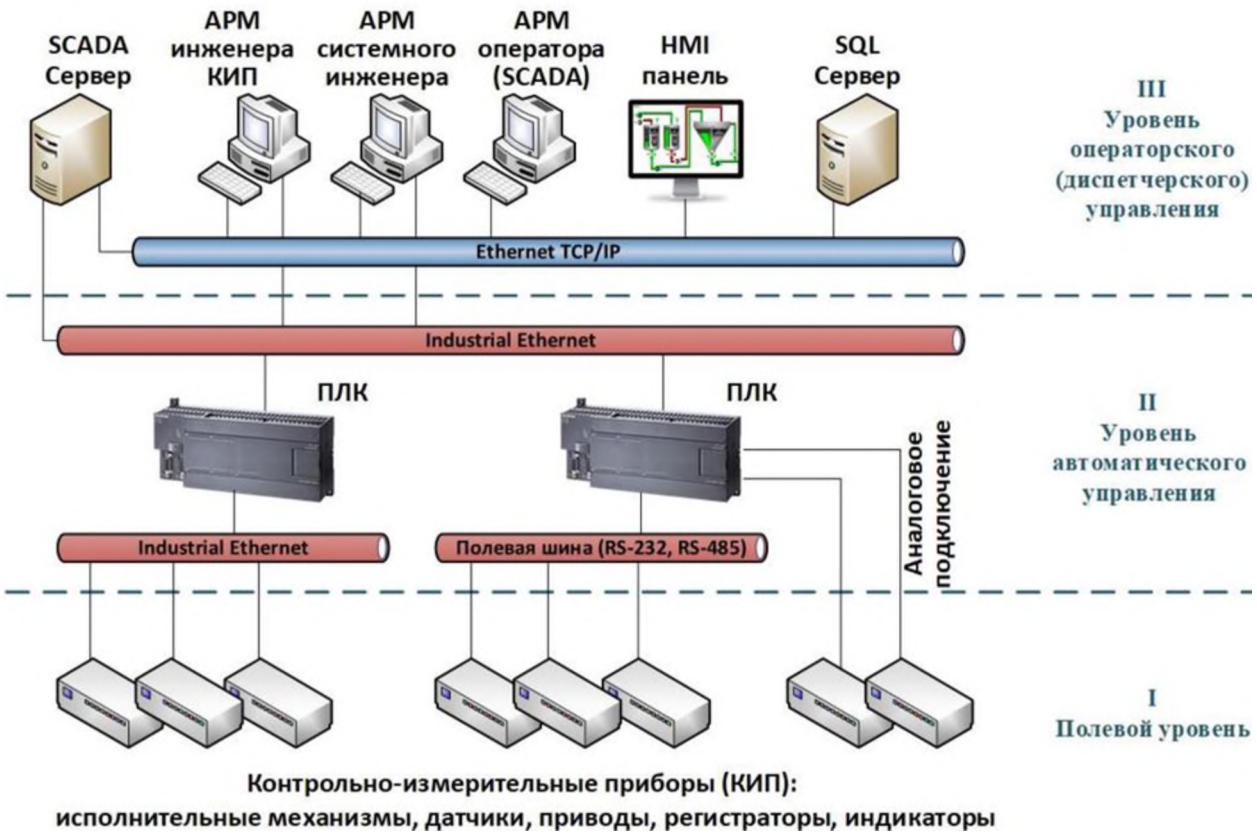

Рис. 1. Типовая архитектура АСУ ТП
(Fig.1. Structure of usual ICS)

Программные составляющие АСУ ТП:

- операционные системы реального времени;
- системы сбора данных и диспетчерского управления (SCADA).

Аппаратные составляющие АСУ ТП:

- программируемые логические контроллеры;
- датчики, регистраторы, привода и исполнительные механизмы;
- модули цифрового и/или человеко-машинного интерфейса;
- АРМ оператора и серверы системы;
- коммуникационные сети.

Перечень основных угроз АСУ ТП, отмеченных в реальных инцидентах:

- атаки на системы сбора данных и диспетчерского управления (SCADA);
- атаки на ПЛК с использованием их уязвимостей (неавторизованный доступ к фирменному программному обеспечению, пароль по умолчанию, удалённое изменение пароля и т. д.);
- атаки на инфраструктуру и операционные системы (троянские программы, вирусы, черви, ARP-спуфинг, DoS- и DDos-атаки);
- атаки на протоколы с использованием их уязвимостей;
- атаки на базы данных (SQL инъекция);
- другие атаки (переполнение буфера, отказ в доступе, отказ в управлении, отказ в представлении, подмена представления) [15].

Наибольшее количество уязвимостей среди компонентов АСУ ТП имеют SCADA-системы - 87% (процент уязвимых систем от их общего количества), далее следуют системы человеко-машинного интерфейса - 49%, реже обнаруживаются уязвимости в

программируемых логических контроллерах - 20%, и совсем редко в проприетарных протоколах - 1% [13].

На сегодняшний день огромное количество различных компонентов автоматизированных систем управления технологическими процессами доступны из сети Интернет, о чем свидетельствуют результаты поиска с использованием поисковика Shodan (рисунок 2). Shodan (https://www.shodan.io) посылает запрос на публично доступные IP-адреса и протоколирует информацию, полученную в ответ (название устройств, их тип, наличие веб-интерфейса и т.д.). В результате создается карта сети Интернет, с помощью которой можно искать устройства с сетевым интерфейсом или, установив нужные фильтры, смотреть за актуальным состоянием глобальной сети и изучать характер распространения уязвимостей [7].

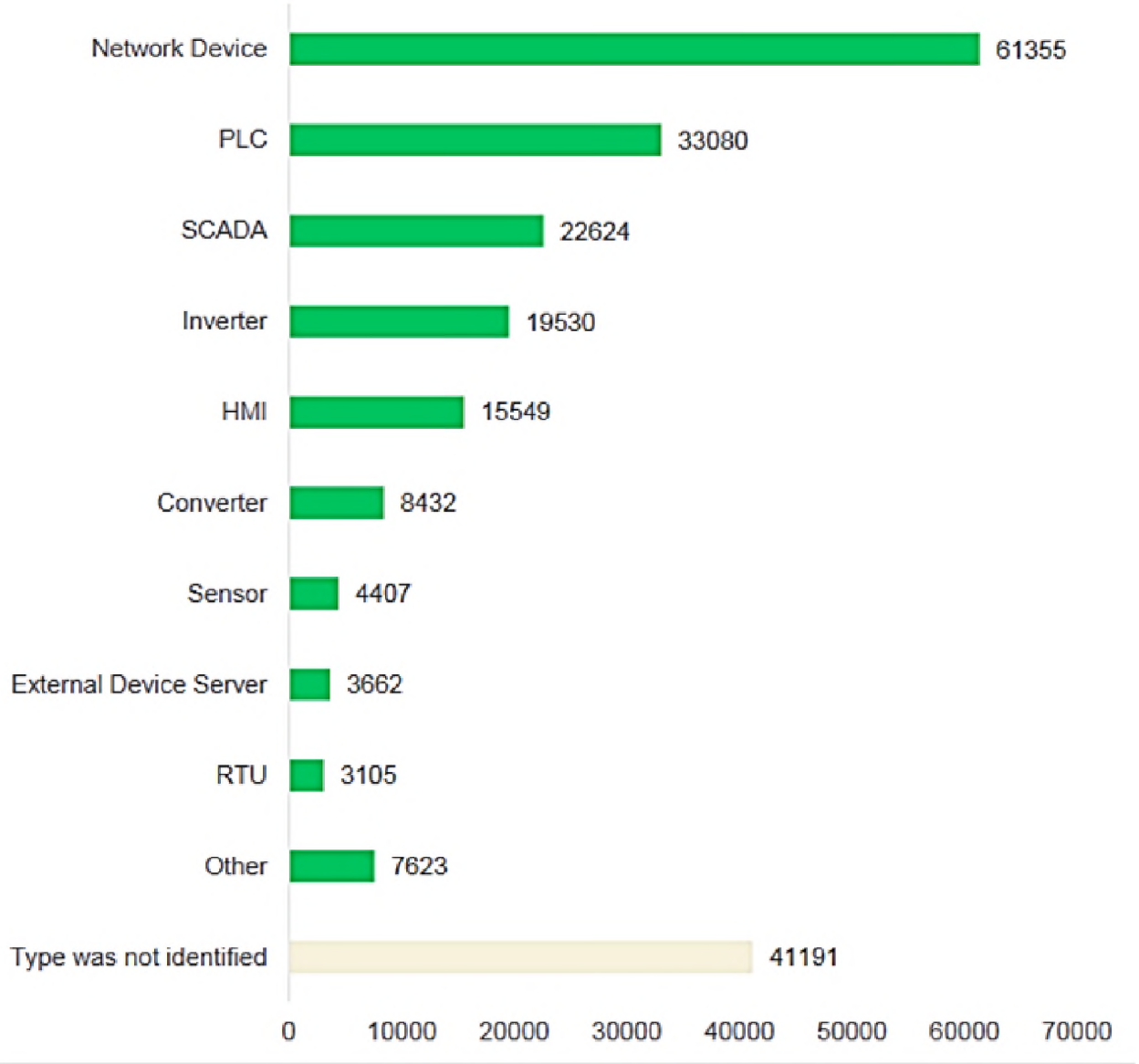

Рис.2. Количество доступных компонентов АСУ ТП из сети Интернет [16]
(Fig.2. Amount of available from the Internet components of ICS)

В качестве примера для практической реализации можно рассмотреть потенциальный вектор атаки на типовую АСУ ТП - доступ к проприетарному программному обеспечению с использованием аутентификационных данных «по умолчанию».

С помощью поисковика Shodan были найдены доступные из сети устройства i.LON SmartServer с открытым веб-интерфейсом (фильтр «200» в Shodan) - их обнаружилось 36

шт. (рисунок 3). Интернет-сервер i.LON SmartServer компании Echelon предназначен для управления сетями LonWorks и используется для автоматизации зданий, управления системами освещения, отопления, вентиляции и кондиционирования, позволяет подключать напрямую счетчики воды, электроэнергии и газа, а также применяется для централизованного энергетического менеджмента на территориально распределенных предприятиях.

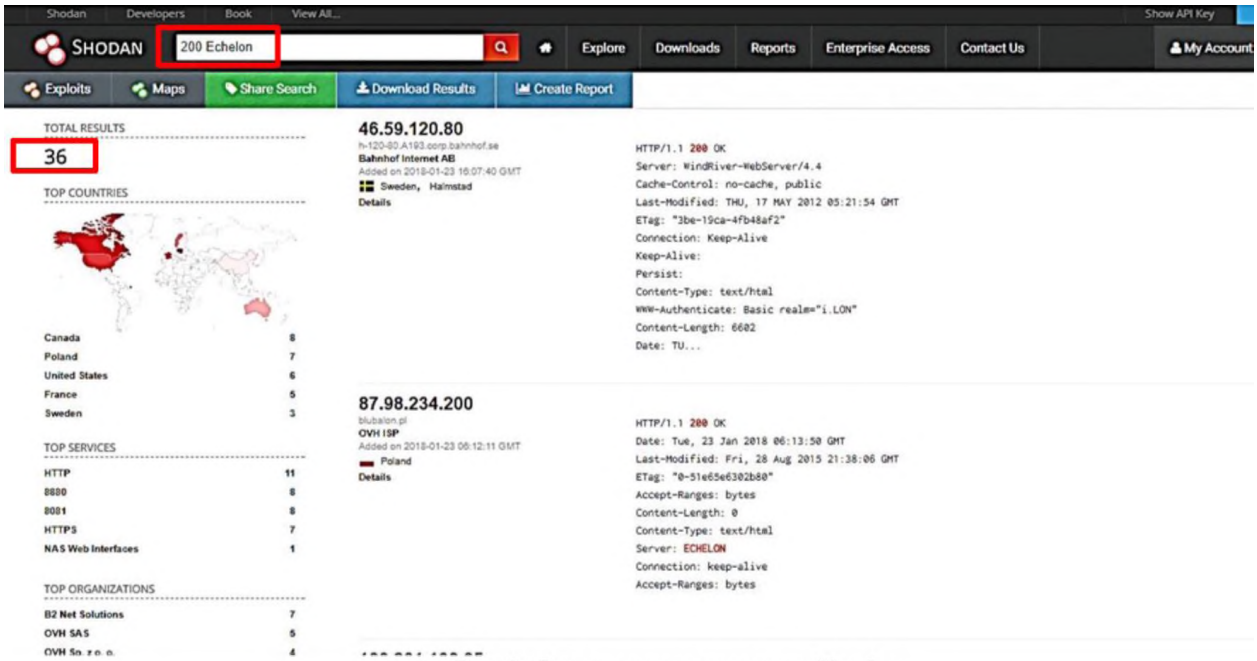

Рис.3. Результаты поиска в Shodan
(Fig.3. Results of Shodan search)

Далее был выбран интернет-серверы i.LON SmartServer, расположенной в Корее, с ip-адресом 1.212.147.219 (рисунок 4).

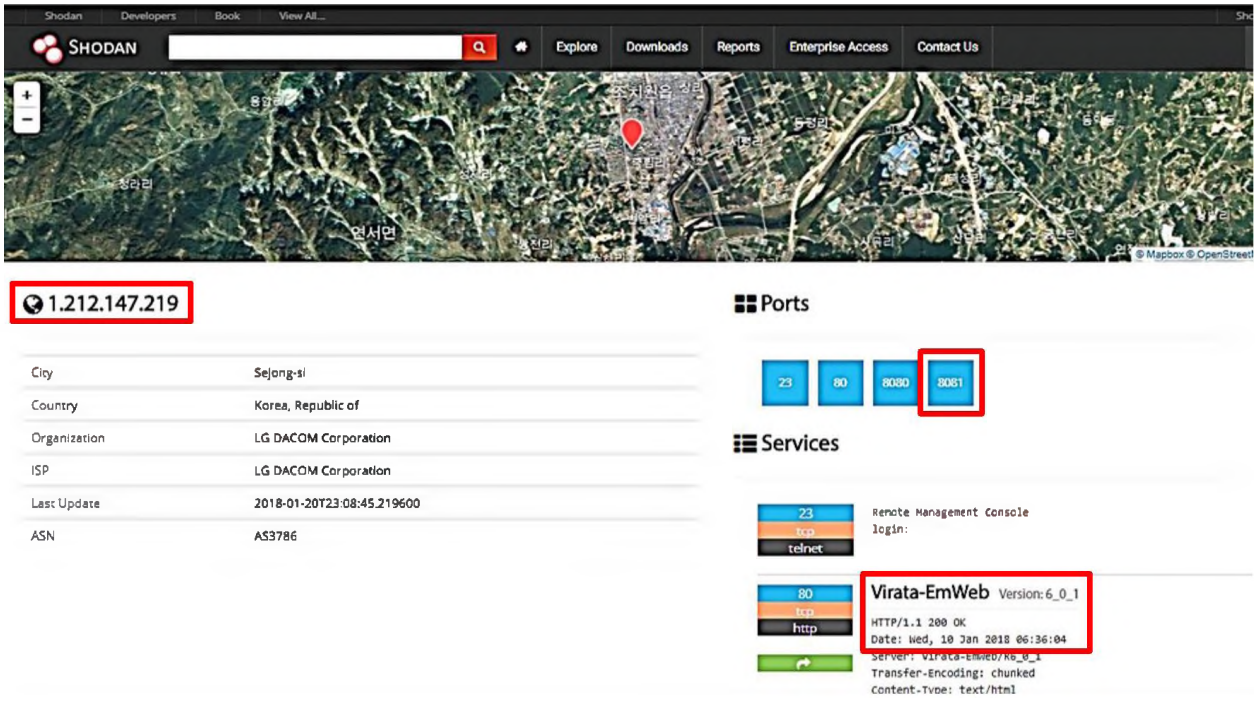

Рис.4. Устройство, доступное по адресу 1.212.147.219
(Fig.4. Device with 1.212.147.219 address)

Был выполнен переход по указанному адресу и обнаружено, что панель управления интернет-сервером защищена при помощи авторизации (рисунок 5).

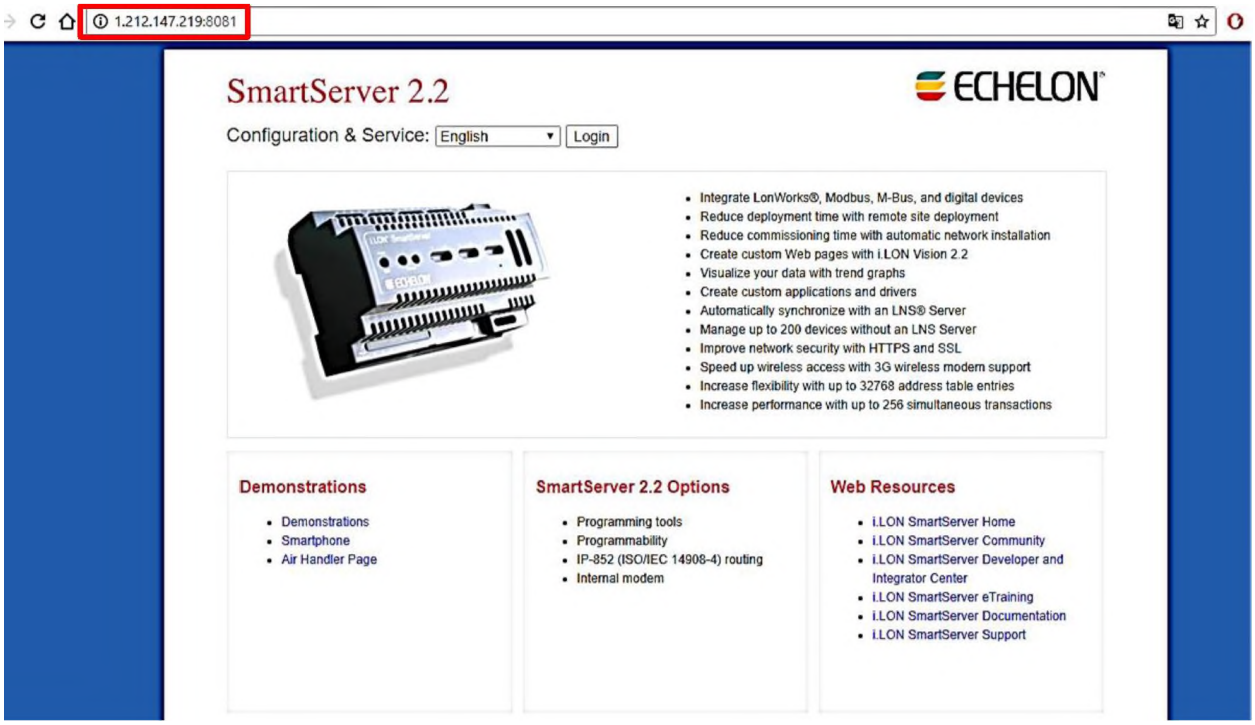

Рис.5. Окно авторизации на интернет-сервере
(Fig.5. Authorization window of the internet-server)

Для успешной авторизации на интернет-сервере с помощью базы логинов и паролей «по умолчанию» для различных компонентов SCADA-систем была подобрана пара логин/пароль для данного устройства (рисунок 6).

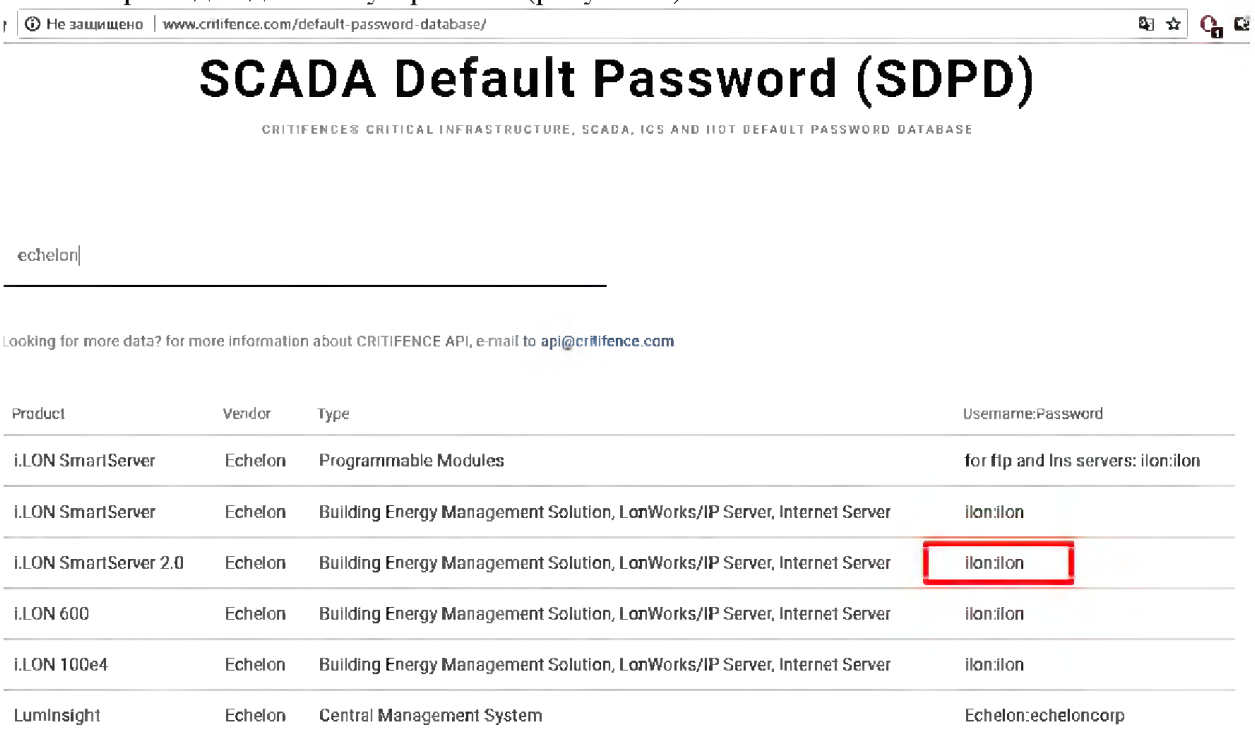

Рис.6. База логинов и паролей «по умолчанию» для различных компонентов SCADA-систем
(Fig.6. SCADA Default Password Database)

Далее был осуществлен успешный вход в консоль администратора интернет-сервера (рисунок 7). Используя консоль администратора, потенциальный злоумышленник может получить различные данные об устройстве, например, версию прошивки, и использовать соответствующие уязвимости, информация о которых находится в открытом доступе в сети Интернет.

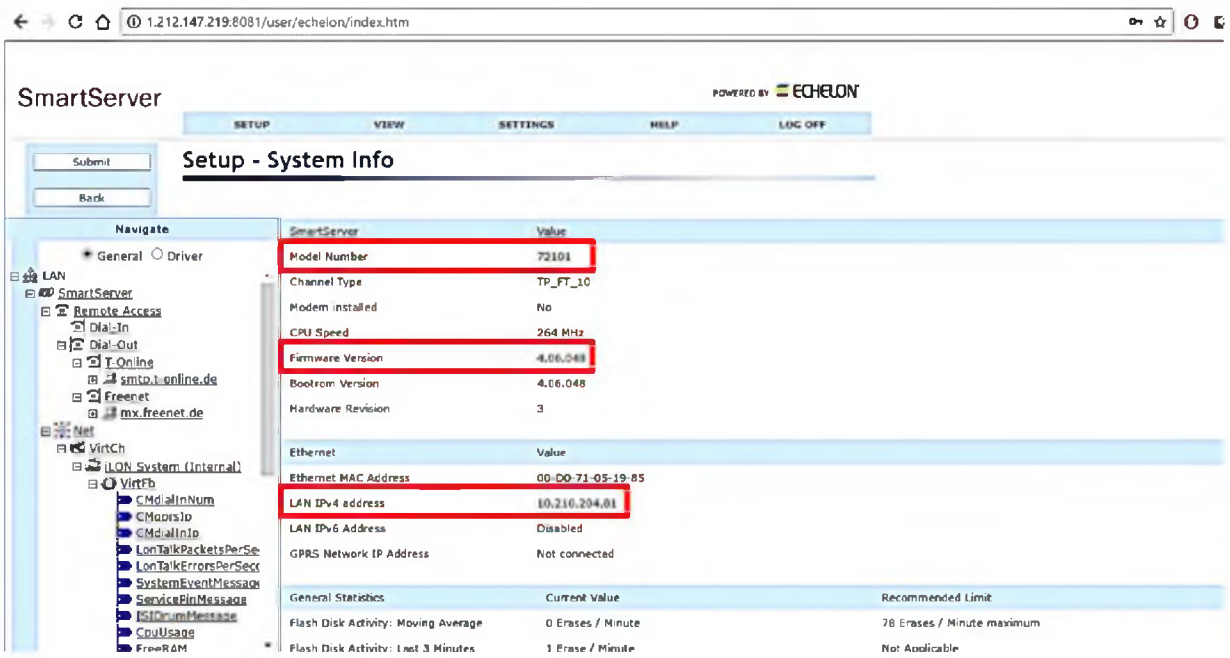

Рис.7. Информация об устройстве
(Fig.7. Information about device)

Также потенциальный злоумышленник может нарушить работу устройства, сменить пароль консоли управления и, тем самым, запретить доступ к нему системному администратору (рисунок 8).

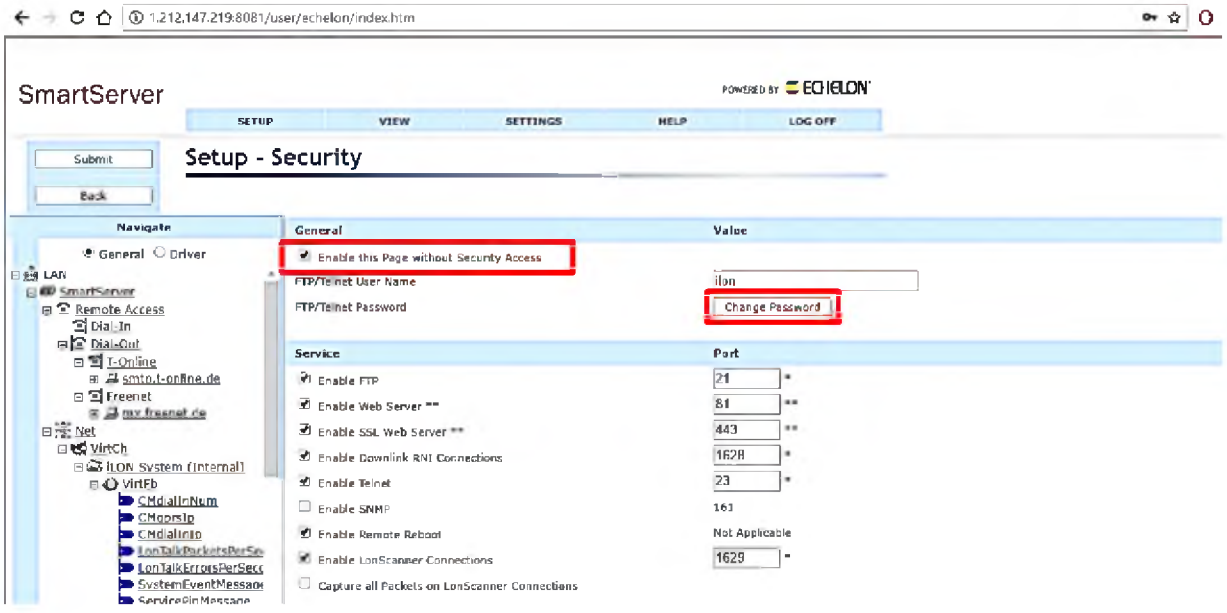

Рис.8. Страница управления паролем консоли
(Fig.8. Password management page)

В результате данного исследования ни одно устройство не пострадало. Данный эксперимент преследовал исключительно научные цели - показать реальность атак и простоту их реализации.

Заключение

Вышеописанный пример показал, что атаки такого типа реальны, легко реализуемы и могут касаться как обычных систем автоматизации зданий, которые используют интернет-сервер i.LON SmartServer для удаленного доступа, управления и конфигурирования устройств, так и предприятий, которые организуют свой производственный процесс с использованием данного оборудования (например – насосных станций). Последствия нарушения производственного процесса такого предприятия могут быть весьма масштабными.

Возможные способы защиты от атак данного типа:

- обязательная смена паролей «по умолчанию» и увеличение их сложности;
- своевременное обновление прошивок оборудования до последней версии;
- периодический мониторинг уязвимостей и обновлений программного обеспечения, устраняющих их.

На сегодняшний день подход производителей промышленного программного обеспечения и оборудования к исправлению уязвимостей, а также ситуация с устранением известных уязвимостей в автоматизированных системах, развернутых на предприятиях, остаются плачевными. Как результат, подавляющее большинство автоматизированных систем управления технологическими процессами в данный момент остаются уязвимы к атакам.

Данное исследование преследует цель показать, насколько легко можно получить доступ к компонентам реальной автоматизированной системы управления, а также пролить свет на то, какие негативные последствия могут быть этим вызваны.

СПИСОК ЛИТЕРАТУРЫ:

1 Sajid Nazir, Shushma Patel, Dilip Patel, Assessing and augmenting SCADA cyber security: A survey of techniques, Computers & Security, Volume 70, September 2017, Pages 436-454. DOI: 10.1016/j.cose.2017.06.010.
2 A. Nicholson, S. Webber, S. Dyer, T. Patel, H. Janicke, SCADA security in the light of Cyber-Warfare, Computers & Security, Volume 31, Issue 4, June 2012, Pages 418-436. DOI: 10.1016/j.cose.2012.02.009.
3 Lachlan Urquhart, Derek McAuley, Avoiding the internet of insecure industrial things, Computer Law & Security Review, Available online, January 2018. DOI: 10.1016/j.clsr.2017.12.004.
4 Danny Bradbury, SCADA: a critical vulnerability, Computer Fraud & Security, Volume 2012, Issue 4, April 2012, Pages 11-14. DOI: 10.1016/S1361-3723(12)70030-1.
5 Christopher M. Talbot, Michael A. Temple, Timothy J. Carbino, J. Addison Betances, Detecting rogue attacks on commercial wireless Insteon home automation systems, Computers & Security, In press, cor-rected proof, Available online 13 October 2017. DOI: 10.1016/j.cose.2017.10.001.
6 Igor Nai Fovino, Andrea Carcano, Marcelo Masera, Alberto Trombetta, An experimental investigation of malware attacks on SCADA systems, International Journal of Critical Infrastructure Protection, Volume 2, Issue 4, December 2009, Pages 139-145. DOI: 10.1016/j.ijcip.2009.10.001.
7 Roland Bodenheim, Jonathan Butts, Stephen Dunlap, Barry Mullins, Evaluation of the ability of the Shodan search engine to identify Internet-facing industrial control devices, International Journal of Criti-cal Infrastructure Protection, Volume 7, Issue 2, June 2014, Pages 114-123. DOI: 10.1016/j.ijcip.2014.03.001.
8 H. Abdo, M. Kaouk, J.-M. Flaus, F. Masse, A safety/security risk analysis approach of Industrial Control Systems: A cyber bowtie – combining new version of attack tree with bowtie analysis, Computers & Security, Volume 72, January 2018, Pages 175-195. DOI: 10.1016/j.cose.2017.09.004.
9 Luis Martín-Liras, Miguel A. Prada, Juan J. Fuertes, Antonio Morán, Manuel Domínguez, Comparative analysis of the security of configuration protocols for industrial control devices, International Journal of Critical Infrastructure Protection, Volume 19, December 2017, Pages 4-15. DOI: 10.1016/j.ijcip.2017.10.001.
10 Cristina Alcaraz, Javier Lopez, Kim-Kwang Raymond Choo, Resilient interconnection in cyber-physical control systems, Computers & Security, Volume 71, November 2017, Pages 2-14. DOI: 10.1016/j.cose.2017.03.004.
11 Niv Goldenberg, Avishai Wool, Accurate modeling of Modbus/TCP for intrusion detection in SCADA systems, International Journal of Critical Infrastructure Protection, Volume 6, Issue 2, June 2013, Pages 63-75. DOI:

10.1016/j.ijcip.2013.05.001.
12 Rafael Ramos Regis Barbosa, Ramin Sadre, Aiko Pras, Flow whitelisting in SCADA networks, Interna-tional Journal of Critical Infrastructure Protection, Volume 6, Issues 3–4, December 2013, Pages 150-158. DOI: 10.1016/j.ijcip.2013.08.003.
13 Грицай, Г., Тиморин, А., Гольцев, Ю. Positive Technologies. Безопасность промышленных систем в цифрах [Электронный ресурс] Режим доступа: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/SCADA-analytics-rus.pdf (дата обращения 23.01.2018).
14 Михайлов, Д.М., Жуков, И.Ю., Шеремет, И.А. Защита автоматизированных систем от информационно-технологических воздействий. – М.: НИЯУ МИФИ, 2014. – 184 с.
15 Пищик, Б.Н. Безопасность АСУ ТП // ЖВТ. 2013. №. С.170-175
16 Andreeva, O., Gordeychik, S., Gritsai, G., Kochetova, O., Potseluevskaya, E., Sidorov, S., Timorin, A., Industrial control systems and their online availability. Access mode: https://kasperskycontenthub.com/securelist/files/2016/07/KL_REPORT_ICS_Availability_Statistics.pdf.

REFERENCES:

[1] Sajid Nazir, Shushma Patel, Dilip Patel, Assessing and augmenting SCADA cyber security: A survey of techniques, Computers & Security, Volume 70, September 2017, Pages 436-454. DOI: 10.1016/j.cose.2017.06.010.
[2] A. Nicholson, S. Webber, S. Dyer, T. Patel, H. Janicke, SCADA security in the light of Cyber-Warfare, Computers & Security, Volume 31, Issue 4, June 2012, Pages 418-436. DOI: 10.1016/j.cose.2012.02.009.
[3] Lachlan Urquhart, Derek McAuley, Avoiding the internet of insecure industrial things, Computer Law & Security Review, Available online, January 2018. DOI: 10.1016/j.clsr.2017.12.004.
[4] Danny Bradbury, SCADA: a critical vulnerability, Computer Fraud & Security, Volume 2012, Issue 4, April 2012, Pages 11-14. DOI: 10.1016/S1361-3723(12)70030-1.
[5] Christopher M. Talbot, Michael A. Temple, Timothy J. Carbino, J. Addison Betances, Detecting rogue attacks on commercial wireless Insteon home automation systems, Computers & Security, In press, cor-rected proof, Available online 13 October 2017. DOI: 10.1016/j.cose.2017.10.001.
[6] Igor Nai Fovino, Andrea Carcano, Marcelo Masera, Alberto Trombetta, An experimental investigation of malware attacks on SCADA systems, International Journal of Critical Infrastructure Protection, Volume 2, Issue 4, December 2009, Pages 139-145. DOI: 10.1016/j.ijcip.2009.10.001.
[7] Roland Bodenheim, Jonathan Butts, Stephen Dunlap, Barry Mullins, Evaluation of the ability of the Shodan search engine to identify Internet-facing industrial control devices, International Journal of Critical Infrastructure Protection, Volume 7, Issue 2, June 2014, Pages 114-123. DOI: 10.1016/j.ijcip.2014.03.001.
[8] H. Abdo, M. Kaouk, J.-M. Flaus, F. Masse, A safety/security risk analysis approach of Industrial Control Systems: A cyber bowtie – combining new version of attack tree with bowtie analysis, Computers & Security, Volume 72, January 2018, Pages 175-195. DOI: 10.1016/j.cose.2017.09.004.
[9] Luis Martín-Liras, Miguel A. Prada, Juan J. Fuertes, Antonio Morán, Manuel Domínguez, Comparative analysis of the security of configuration protocols for industrial control devices, International Journal of Critical Infrastructure Protection, Volume 19, December 2017, Pages 4-15. DOI: 10.1016/j.ijcip.2017.10.001.
[10] Cristina Alcaraz, Javier Lopez, Kim-Kwang Raymond Choo, Resilient interconnection in cyber-physical control systems, Computers & Security, Volume 71, November 2017, Pages 2-14. DOI: 10.1016/j.cose.2017.03.004.
[11] Niv Goldenberg, Avishai Wool, Accurate modeling of Modbus/TCP for intrusion detection in SCADA systems, International Journal of Critical Infrastructure Protection, Volume 6, Issue 2, June 2013, Pages 63-75. DOI: 10.1016/j.ijcip.2013.05.001.
[12] Rafael Ramos Regis Barbosa, Ramin Sadre, Aiko Pras, Flow whitelisting in SCADA networks, Interna-tional Journal of Critical Infrastructure Protection, Volume 6, Issues 3–4, December 2013, Pages 150-158. DOI: 10.1016/j.ijcip.2013.08.003.
[13] Gritsay, G., Timorin, Yu, Goltsev, A., Positive Technologies. Safety of industrial systems in figures. Access mode: https://www.ptsecurity.com/upload/corporate/ru-en/analytics/SCADA- analytics-eng.pdf. (in Russian).
[14] Mikhailov, D.M., Zhukov, I.Yu., Sheremet, I.A. Zashhita avtomatizirovannyx sistem ot informacionno-texnologicheskix vozdejstvij, NRNU MEPhI, 2014, P.184 (in Russian).
[15] Pischik, B.N. Bezopasnost ASU TP. ZhVT. 2013. No. P.170-175. (in Russian).
[16] Andreeva, O., Gordeychik, S., Gritsai, G., Kochetova, O., Potseluevskaya, E., Sidorov, S., Timorin, A., Industrial control systems and their online availability. Access mode: https://kasperskycontenthub.com/securelist/files/2016/07/KL_REPORT_ICS_Availability_Statistics.pdf.

Поступила в редакцию – 12 декабря 2017 г. Окончательный вариант –19 февраля 2018 г.
Received – December 12, 2017. The final version – February 19, 2018.

Юлия Г. Красножон
Филиал Федерального казенного учреждения «Налог-Сервис» Федеральной налоговой службы России по центрам обработки данных в г. Москве,
125373, г. Москва, Проходной пер., д. 3, к.3,
e-mail: turchina.yuliya.07@gmail.com, https://orcid.org/0000-0001-8048-3521

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ КАК СРЕДСТВО ОПТИМИЗАЦИИ СИСТЕМЫ АВТОМАТИЗАЦИИ ПРОЦЕССА УПРАВЛЕНИЯ ИНЦИДЕНТАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

DOI: http://dx.doi.org/10.26583/bit.2018.1.10

Аннотация. Современные информационные технологии оказывают все большее влияние на динамику развития и структуру управления организацией. Эффективность управленческой деятельности при внедрении современных информационных технологий, напрямую зависит от качества управления инцидентами информационной безопасности. Вместе с тем, как в российских, так и в зарубежных трудах не в достаточной степени освещены вопросы оценки влияния управления инцидентами информационной безопасности на качество и эффективность системы управления предприятием. Для решения этих проблем ключевым направлением является оптимизация системы автоматизации процесса управления инцидентами информационной безопасности. Сегодня особое внимание уделяется процессам управления инцидентами информационной безопасности на таких критически важных объектах Российской Федерации, как Федеральная налоговая служба России (ФНС). Для построения математической модели оптимизации данной системы предлагается использовать математический аппарат теории массового обслуживания. Разработанная модель позволит оценить качество управленческой деятельности с учетом правил и ограничений, накладываемых на систему влияниями реальных факторов инцидентов информационной безопасности. В статье рассматривается пример, демонстрирующий работу системы, приведены полученные статистические данные. Построение такой системы позволит повысить качество предоставляемых ФНС России сервисов и скорость реагирования на инциденты информационной безопасности.

Ключевые слова: угроза информационной безопасности, автоматизированная информационная система, инциденты информационной безопасности, Центры обработки данных Федеральной налоговой службы России, управление инцидентами информационной безопасности.

Для цитирования. ***КРАСНОЖОН, Юлия Г.*** *МАТЕМАТИЧЕСКАЯ МОДЕЛЬ КАК СРЕДСТВО ОПТИМИЗАЦИИ СИСТЕМЫ АВТОМАТИЗАЦИИ ПРОЦЕССА УПРАВЛЕНИЯ ИНЦИДЕНТАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. Безопасность информационных технологий, [S.l.], v. 25, n. 1, p. 99-107, 2018. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1096>. Дата доступа: 19 feb. 2018. doi:http://dx.doi.org/10.26583/bit.2018.1.10.*

Yulia G. Krasnozhon
The Federal State-funded Institution branch «Nalog-Servis» of the Federal Tax Service of Russia on data processing centre in Moscow city,
125373, Moscow city, Prokhodnoy offstreet, h. 3, bld. 3,
e-mail: turchina.yuliya.07@gmail.com, https://orcid.org/0000-0001-8048-3521

Mathematical model as means of optimization of the automation system of the process of incidents of information security management

DOI: http://dx.doi.org/10.26583/bit.2018.1.10

Abstract. Modern information technologies have an increasing importance for development dynamics and management structure of an enterprise. The management efficiency of

implementation of modern information technologies directly related to the quality of information security incident management. However, issues of assessment of the impact of information security incidents management on quality and efficiency of the enterprise management system are not sufficiently highlighted neither in Russian nor in foreign literature. The main direction to approach these problems is the optimization of the process automation system of the information security incident management. Today a special attention is paid to IT-technologies while dealing with information security incidents at mission-critical facilities in Russian Federation such as the Federal Tax Service of Russia (FTS). It is proposed to use the mathematical apparatus of queueing theory in order to build a mathematical model of the system optimization. The developed model allows to estimate quality of the management taking into account the rules and restrictions imposed on the system by the effects of information security incidents. Here an example is given in order to demonstrate the system in work. The obtained statistical data are shown. An implementation of the system discussed here will improve the quality of the Russian FTS services and make responses to information security incidents faster.

Keywords: information security threat, automated information data system, information security incidents, Data-processing centers of Federal Tax Service of the Russian Federation, management of incidents of information security.

For citation. ***KRASNOZHON, Yulia G.*** *Mathematical model as means of optimization of the automation system of the process of incidents of information security management. IT Security (Russia), [S.l.], v. 25, n. 1, p. 99-107, 2018. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1096>. Date accessed: 19 feb. 2018. doi:http://dx.doi.org/10.26583/bit.2018.1.10.*

Введение

В наши дни эффективное управление является очень ценным ресурсом для каждой компании, оно стоит на ряду с финансовыми, материальными, человеческими и иными ресурсами организации. Именно поэтому эффективность управленческой деятельности и, в частности, её повышение за счёт изучения и анализа отдельных аспектов внедрения современных информационных технологий управления, можно считать ключевым направлением модернизации деятельности всей компании. В настоящее время особое внимание уделяется ИТ-технологиям в процессе управления инцидентами информационной безопасности [1-3] на критически важных объектах Российской Федерации. Таким объектом является Федеральная налоговая служба России (ФНС).

На сегодняшний день для российской и зарубежной науки интерес представляет вопрос влияния современных информационных технологий на динамику развития и структуру управления организацией. Среди российских учёных, которые уделяли большое внимание аспектам внедрения ИТ в различные сферы деятельности предприятий, следует отметить таких исследователей, как Г. В. Алехину, Т. П. Барановскую, К. Ю. Воробьёва, Н. А. Коробова, В. И. Лойко, Д. Р. Махмутову. Изысканиям в области проблем применения информационных технологий в управлении организациями посвящены работы зарубежных ученых – Б. Гейтса, Р. Каплан, Г. Минска, Д. Нортона, Д. Шнайдера.

Целью статьи является описание математической модели оптимизации системы автоматизации процесса управления инцидентами информационной безопасности.

Обоснование математической модели

Исходя из того, что математическая модель – это математическое представление реальности, то есть модель как система, то для оптимизации системы автоматизации процесса управления инцидентами информационной безопасности мы будем использовать математическое моделирование (совокупность математических выражений) [4], как помощь в решении поставленной задачи. Для построения предпочтительной модели оптимизации данной системы в филиале Ф К У «Налог-Сервис» ФНС России по ЦОД в г. Москве (далее – филиал), необходимо использовать методики теории массового обслуживания.

Так как система массового обслуживания (СМО) – это система, когда в каналы обслуживания в случайные моменты времени поступает поток заявок (требований), происходит их выполнение потоком обслуживания этих заявок [5,6], то следует понимать, что в данном случае клиентами СМО являются сотрудники филиала, заявки от клиентов являются обращениями к СМО, а показатели эффективности работы сотрудников – показателями СМО.

Важным показателем СМО является эффективность работы сотрудников. Создаваемая модель, позволит оценить качество работы сотрудников и всего отдела информатизации в целом. Ключевой задачей при адаптации математического аппарата в решении задачи станет подсчет оценки качества работы и проверка правил и ограничений, накладываемых на систему влияниями реальных факторов [7].

Стоит учитывать, что работа по математическому аппарату невозможна без использования статистических данных. В рассматриваемом примере эти данные будут выведены для демонстрации работы системы [8]. При реальном внедрении, все табличные данные могут быть скорректированы после тестового запуска на основании алгоритмов, которые будут описаны ниже.

Для начала нужно определить задачи, которые поступают специалисту технической поддержки. Для каждой задачи определяем среднее время ее выполнения, приоритетность и к какому специалисту нужно перенаправить данный запрос. В основном, в организации будут использоваться непараллельные процессы, когда типы задач заранее распределены между исполнителями и не могут передаваться от одного к другому в случае, если данный специалист занят [9].

Так как специалисты второго уровня не могут решать сторонние задачи, то для каждого специалиста не составит труда определить список собственных задач и определить время их решения, а также приоритетность этих задач. Также оценку приоритетности должен дать сотрудник третьего уровня. Получив список задач от специалистов второго уровня, система сможет определять задачи для каждого специалиста, прогнозировать его занятость и время ожидания для пользователя [10]. Учитывая, что в системе недопустима потеря заявок, то будет использоваться одноканальная СМО с ожиданиями и неограниченной очередью, но нужно учитывать то, чтобы очередь не стремилась к бесконечности.

Рассмотрим описанную систему на примере работы системного администратора отдела информатизации. В качестве исходных данных возьмем таблицы:

- оценки поступающих запросов (таблица 1),
- среднего количества заявок по дням (таблица 2),
- допустимые показатели качества работы системного администратора (таблица 3),
- допустимые показатели качества работы отдела информатизации (таблица 4),

а также количество заявок n = 10, критичное количество заявок первого уровня P_f = 10, критичное количество заявок второго уровня P_m = 25.

Таблица 1. Оценка поступающих запросов

Специалист	*Порядковый номер задачи*	*Имя задачи*	*Среднее время исполнения t_n*	*Приоритет L*
Системный администратор	A1	Не работает интернет	0,25 ч	5
	A2	Отсутствует подключение в локальном чате	0,1 ч	1
	A3	Требуется подключить нового пользователя	0,5 ч	4
	A4	Утерян пароль	0,33 ч	2
Администратор БД	B1	Зависла БД	2 ч	3
	B2	Обнаружены совпадающие данные у	0,41ч	3

		разных позиций		
	B3	Ошибка выгрузки БД	0,75 ч	2
	B4	Ошибка добавления в БД	0,33 ч	2
Техник-инженер	C1	Не работает принтер	0,25 ч	2
	C2	Не включается компьютер	0,08 ч	1
	C3	Вирус на компьютере	0,5 ч	2
	C4	Нет необходимого ПО	1 ч	4

Таблица 2. Среднее количество заявок в час по дням

	Количество заявок в день	*Количество рабочих часов*	*Количество заявок в час*
$\lambda_{пн}$ за прошлую	24	8	3
$\lambda_{вт}$ за прошлую	20	8	2,5
$\lambda_{ср}$ за прошлую	16	8	2
$\lambda_{чт}$ за прошлую	14,4	8	1,8
$\lambda_{пт}$ за прошлую	14,7	7	2,1

Таблица 3. Допустимые показатели качества работы системного администратора

Сотрудник	*Показатель качества К*
Сотрудники отдела информатизации	0,7

Таблица 4. Допустимые показатели качества работы отдела информатизации

Показатель	*Критерии*
среднее число заявок, находящееся в системе у определенного сотрудника (Ls)	- от 95% до 100% норматива; - менее 95%; - 110% и более
средняя продолжительность пребывания заявки в системе (Ws)	
среднее число заявок в очереди (Lq)	
средняя продолжительность пребывания заявки в очереди (Wq)	

Итак, допустим, утром в пятницу, 26 мая 2017 года, специалист службы поддержки получил 10 заявок: заявки A2, A4, A3, A1, две заявки B1, заявки C1, C2, C3, C4. Программа начинает оценку среднего времени исполнения для каждого сотрудника и расставляет задачи по приоритетам.

Общее время выполнения задач (на основании таблицы 1) составляет 1,18 ч. Перейдем к прогнозированию нахождения у специалиста второго уровня определенного количества задач. Для начала вычислим $t_{ср}$ выполнения задач [11].

$$t_0 = \frac{t_1+t_2+t_3+t_4}{4} = \frac{0,25 + 0,1 + 0,5 + 0,33}{4} = 0,295. \quad (1)$$

Вычислим плотность распределения заявок:

$$\mu_n = \frac{1}{t_n} = \frac{1}{0,295} = 3,389. \quad (2)$$

Возьмем табличное значение λ для пятницы, λ=2,1. Для подсчета вероятности нахождения у специалиста n заявок вычислим коэффициент r:

$$r = \frac{\lambda}{\mu} = \frac{2,1}{3,389} = 0,619. \quad (3)$$

Теперь определим предельные вероятности системы по формулам:

$$P_0 = (1 - r) = 1 - 0,619 = 0,380, \quad (4)$$

$$P_1 = (1 - r) * r = r * P_0 = 0,619 * 0,380 = 0,235, \quad (5)$$

$$P_2 = r^2 * P_0 = 0,145, \quad (6)$$

$$P_3 = r^3 * P_0 = 0,090, \quad (7)$$

$$P_4 = r^4 * P_0 = 0,055. \quad (8)$$

Так как с утра коэффициент $r < 1$, проблема бесконечно растущей очереди отсутствует.

Изменение порядка очереди по приоритету привело к тому, что задачи в очереди идут следующим образом: А1, А3, А4, А2.

Оценка продуктивности специалиста происходит после получения реального времени выполнения задач.

Изменения статистических данных происходит в конце рабочего дня.

На основании подсчитанных выше вероятностей, можно вычислить следующие коэффициенты для новых утренних задач и задач, оставшихся с прошлого рабочего дня:

- среднее число заявок, находящееся в системе у системного администратора

$$L_s = \frac{r}{1-r} = \frac{0,619}{0,381} = 1,625, \quad (9)$$

- средняя продолжительность пребывания заявки в системе

$$W_s = \frac{L_s}{\lambda} = \frac{1,625}{2,1} = 0,773\text{ч}, \quad (10)$$

- среднее число заявок в очереди

$$L_{\bar{q}} = L_s - \frac{\lambda}{\mu} = 1,625 - 0,619 = 1,006, \quad (11)$$

- средняя продолжительность пребывания заявки в очереди

$$W_q = \frac{r}{\mu*(1-r)} = \frac{0,619}{3,389*0,380} = 0,480. \quad (12)$$

Предположим, что через 10 минут в систему поступили заявки А2(2) и А3(2). Следовательно, нужно пересмотреть очередь и все остальные показатели. Общее время выполнения задач теперь составляет 1,78 ч. Заявки в очереди встанут в порядке А3, А3(2), А4, А2, А2(2), так как заявка А1 уже обработана, а заявки с одинаковым приоритетом встают в очередь по тому порядку, в котором они пришли. Перейдем к прогнозированию нахождения у специалиста второго уровня определенного количества задач, где $t_{ср}$ выполнения задач:

$$t_0 = \frac{t_1+t_2+t_3+t_4+t_5}{5} = \frac{0,5 + 0,5 + 0,33 + 0,1+ 0,1}{5} = 0,306. \quad (13)$$

Вычислим плотность распределения заявок:

$$\mu_{ср} = \frac{1}{t_0} = \frac{1}{0,306} = 3,267. \quad (14)$$

Возьмем табличное значение λ для пятницы, λ=2,1. Для подсчета вероятности нахождения у специалиста n заявок вычислим коэффициент r:

$$r = \frac{\lambda}{\mu} = \frac{2,1}{3,267} = 0,642. \quad (15)$$

Теперь определим предельные вероятности системы по формулам:

$$P_0 = (1 - r) = 1 - 0{,}642 = 0{,}357, \quad (16)$$

$$P_1 = (1 - r) * r = r * P_0 = 0{,}642 * 0{,}357 = 0{,}229, \quad (17)$$

$$P_2 = r^2 * P_0 = 0{,}147, \quad (18)$$

$$P_3 = r^3 * P_0 = 0{,}094, \quad (19)$$

$$P_4 = r^4 * P_0 = 0{,}060 \quad , \quad (20)$$

$$P_5 = r^5 * P_0 \quad = 0{,}038 \quad . \quad (21)$$

Так как коэффициент $r<1$, проблема бесконечно растущей очереди отсутствует [12].

На основании подсчитанных выше вероятностей, можно вычислить следующие коэффициенты для задач, которые находятся в обработке в данный момент:

- среднее число заявок, находящееся в системе у системного администратора

$$L_s = \frac{r}{1-r} = \frac{0{,}642}{0{,}358} = 1{,}793, \quad (22)$$

- средняя продолжительность пребывания заявки в системе

$$W_s = \frac{L_s}{\lambda} = \frac{1{,}793}{2{,}1} = 0{,}853\text{ч}, \quad (23)$$

- среднее число заявок в очереди

$$L_q = L_s - \frac{\lambda}{\mu} = 1{,}793 - 0{,}642 = 1{,}151, \quad (24)$$

- средняя продолжительность пребывания заявки в очереди

$$W_q = \frac{r}{\mu*(1-r)} = \frac{0{,}642}{3{,}267*0{,}358} = 0{,}549. \quad (25)$$

После этого заявок для системного администратора в систему не поступало. Но за 50 минут до окончания рабочего дня в систему поступило 3 заявки – А1(2), А4(2), А3(3). Время на выполнение задач составит 1,08. Следовательно, СМО сформировала запрос, а именно: исключила неприоритетные задачи и включила приоритетные [13].

$$(T - T_{раб}) \leq \sum t_n; \quad (26)$$

(7–0,83)≤1,08 – условие не выполняется, система становится СМО с ограниченной очередью и исключает заявку А4(2) из системы и переносит ее на следующий рабочий день, а у системного администратора образуется очередь из двух задач в порядке А1(2), А3(3).

Произведем расчеты для этих двух задач.

$$t_0 = \frac{t_1+t_2}{2} = \frac{0{,}25 + 0{,}5}{2} = 0{,}375, \quad (27)$$

$$\mu_{\text{ср}} = \frac{1}{t_0} = \frac{1}{0{,}375} = 2{,}667, \quad (28)$$

$$r = \frac{\lambda}{\mu} = \frac{2{,}1}{2{,}667} = 0{,}787, \quad (29)$$

$$P_0 = (1 - r) = 1 - 0{,}787 = 0{,}213, \quad (30)$$

$$P_1 = (1 - r) * r = r * P_0 \quad = 0{,}787 * 0{,}213 = 0{,}167, \quad (31)$$

$$P_2 = r^2 * P_0 = 0{,}132, \quad (32)$$

$$L_s = \frac{r}{1-r} = \frac{0{,}787}{0{,}213} = 3{,}697, \quad (33)$$

$$W_s = \frac{L_s}{\lambda} = \frac{3{,}697}{2{,}1} = 1{,}759 \text{ ч}, \quad (34)$$

$$L_q = L_s - \frac{\lambda}{\mu} = 3{,}697 - 0{,}787 = 2{,}91, \quad (35)$$

$$\mathrm{W_q} = \frac{\mathrm{r}}{\mu*(1-\mathrm{r})} = \frac{0{,}787}{2{,}267*0{,}213} = 1{,}385. \quad (36)$$

По окончании рабочего дня необходимо произвести оценку работы сотрудника на основании реального времени выполнения задач. Это время представлено в таблице 5.

Таблица 5. Реальное время выполнения задач системным администратором

Задача	*Предполагаемое время выполнения*	*Реальное время выполнения*
A1	0,25 ч	0,2 ч
A3	0,5 ч	0,4 ч
A3(2)	0,5 ч	0,45 ч
A4	0,33 ч	0,33 ч
A2	0,1 ч	0,2 ч
A2(2)	0,1 ч	0,25 ч
A1(2)	0,25 ч	0, 25 ч
A3(3)	0,5 ч	0, 5 ч

На основании описанного метода оценки качества работы сотрудника, с учетом времени задержки выполнения заявки, вычислим коэффициент K по формуле [14]:

$$K = \sum_n^0 \frac{w_i * R_i}{\sum w_i} = \frac{1+1+1+1+0{,}2+0{,}25+1+1}{1+1+1+1+0{,}1+0{,}1+1+1} = 1{,}04. \quad (37)$$

Определим полученный коэффициент работы в соответствии с таблицей 4. Таким образом, работа системного администратора из-за двух просроченных задач не соответствует принятым критериям качества работы в отделе.

Для оценки качества работы всей системы, подсчитаем средние значения следующих коэффициентов:

- среднее число заявок, находящееся в системе у системного администратора

$$L_{s\text{ср}} = \frac{1{,}625+1{,}793+3{,}697}{3} = 2{,}372, \quad (38)$$

- средняя продолжительность пребывания заявки в системе

$$W_{s\text{ср}} = \frac{0{,}773+0{,}853+1{,}759}{3} = 1{,}128, \quad (39)$$

- среднее число заявок в очереди

$$L_{q\text{ср}} = \frac{1{,}006+1{,}151+2{,}91}{3} = 1{,}689, \quad (40)$$

- средняя продолжительность пребывания заявки в очереди

$$W_{q\text{ср}} = \frac{0{,}480+0{,}549+1{,}385}{3} = 0{,}805. \quad (41)$$

Данные показатели могут использоваться для оценки работы отдела информатизации по четным периодам. На основании полученных данных, возможно построения графиков, отражающих динамику изменения показателей. Но так как нам важно уменьшение показателей W_s, L_q и W_q, то можно отметить, что качественные показатели работы отдела в данный день ниже заданных в системе [12]. Это является

нормальным, потому что пример показывает работу системы в первые недели после подключения. Реальные значения показателей могут быть внесены в систему только после окончания тестового периода использования.

Автоматическая корректировка данных происходит следующим образом: после окончания рабочего дня показатель λ этого дня заменяет в таблице значение для этого же дня. Также автоматически могут изменяться некоторые значения, такие как t_n. Автоматически t_n может быть скорректировано в следующем случае: если в течение отчетного периода (одна рабочая неделя) было выполнено более трех однотипных задач и реальное время выполнения этих задач было либо меньше, либо больше табличного значения, и их среднее арифметическое отличается от табличного значения не более чем на 25%, то новое значение вносится в таблицу вместо соответствующего t_n. Если среднее арифметическое отличается от табличного значения более чем на 25%, то формируется запрос для начальника отдела о возможном внесении изменений в табличные данные. Если в течение отчетного периода однотипных задач выполнено меньше трех, то корректировка не производится автоматически, но, если у данных задач срок исполнения превышал 25%, это учитывается в отчете оценки качества работы сотрудника. Изменяемыми только начальником отела остаются показатели приоритетности задачи [15]. Эти данные могут быть изменены только на основе статистического анализа работы всей системы на длительном промежутке времени.

Заключение

Таким образом, разработанная математическая модель на основе одноканальной СМО с неограниченной очередью позволяет рассчитать такие показатели, как среднее число заявок, находящееся в системе, средняя продолжительность пребывания заявки в системе, среднее число заявок в очереди, средняя продолжительность пребывания заявки в очереди. Внедрение данной модели поможет улучшить показатели качества работы специалистов отдела информатизации филиала ФКУ «Налог-Сервис» ФНС России по ЦОД в г. Москве, ответственных за данный тип заявки, а также оптимизировать систему автоматизации процесса управления инцидентами информационной безопасности, а именно: сортировку поступающих в систему заявок по приоритетам и время обработки этих заявок.

СПИСОК ЛИТЕРАТУРЫ:

1 Vacca J. R. Computer and Information Security Handbook. J. R. Vacca. – San Francisco: Morgan Kaufmann Publishers, 2017. – 1280 p.
2 Stiennon R. There Will Be Cyberwar: How The Move To Network-Centric Warfighting Has Set The Stage For Cyberwar. R. Stiennon. – Birmingham: IT-Harvest Press, 2015. – 174 p.
3 Friedman A. Cybersecurity and Cyberwar: What Everyone Needs to Know. A. Friedman. – Oxford: Oxford University Press, 2014. – 320 p.
4 Meerschaert M. M. Mathematical Modeling. M. M. Meerschaert. – San Diego: Academic Press, 2013. – 384 p.
5 Никитин А. В. Управление предприятием (фирмой) с использованием информационных систем: учеб. А. В. Никитин, И. А. Рачковская, И. В. Савченко. – М.: ИНФРА-М, 2015. – 188 с.
6 Simon C. P. Mathematics for Economists. C. P. Simon, L. E. Blume. – New York City: W. W. Norton & Company, 1994. – 960 p.
7 Лабунец А. М. Разработка модели автоматизированной системы контроля, как системы массового обслуживания. А. М. Лабунец, Н. А. Орешин, А. Н. Орешин. Телекоммуникации. – М.: Наука и Технологии, 2006. – № 4. – С. 8 – 13.
8 Hyde A. Basic Internet Security. A. Hyde. – Boston: GNU General Public, 2011. – 244 p.
9 Стрельникова К. О. О повышении эффективности налогового администрирования в Российской Федерации. К. О. Стрельникова. – Саратов: Поволжский институт управления имени. П. А. Столыпина – филиал ФГБОУ ВПО «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации», М., 2014. – С. 98 –100.
10 Harkins M. Managing Risk and Information Security: Protect to Enable. M. Harkins. – Berlin: APress, 2016. – 145 p.

11 Кострова А. В. Методы и модели информационного менеджмента. А. В. Кострова. – М.: Инфра-М, 2014. – 247 с.
12 Harchol-Balter M. Performance Modeling and Design of Computer Systems: Queueing Theory in Action. M. Harchol-Balter. – Cambridge: Cambridge University Press, 2013. – 576 p.
13 Статкевич С. Э. Исследование сети массового обслуживания с ненадежными системами в переходном режиме. С. Э. Статкевич, М. А. Маталыцкий. Вестник Томского государственного университета. Управление, вычислительная техника и информатика. – Томск: Национальный исследовательский Томский государственный университет, 2012. – № 1. – С. 112 – 125.
14 Тананко И. Е. Управление входящим потоком требований в открытых сетях массового обслуживания с параллельными системами обслуживания и ненадежными приборами. И. Е. Тананко, Н. П. Фокина. Компьютерные науки и информационные технологии: материалы науч. конфер. – Саратов: Изд-во Сарат. ун-та, 2010. – С. 116 – 119.
15 Balzarotti D. The SysSec Red Book: A Roadmap for Systems Security Research. D. Balzarotti. – EU: SysSec, 2013. – 194 p.

REFERENCES:

[1] Vacca J. R. Computer and Information Security Handbook. J. R. Vacca. – San Francisco: Morgan Kaufmann Publishers, 2017. – 1280 p.
[2] Stiennon R. There Will Be Cyberwar: How The Move To Network-Centric Warfighting Has Set The Stage For Cyberwar. R. Stiennon. – Birmingham: IT-Harvest Press, 2015. – 174 p.
[3] Friedman A. Cybersecurity and Cyberwar: What Everyone Needs to Know. A. Friedman. – Oxford: Oxford University Press, 2014. – 320 p.
[4] Meerschaert M. M. Mathematical Modeling. M. M. Meerschaert. – San Diego: Academic Press, 2013. – 384p.
[5] Nikitin A. V. Enterprise management with using of the informational systems: textbook. A. V. Nikitin, I. A. Rachkovskaya, I. V. Savchenko – M.: INFRA-M, 2015 – 188 p. (in Russian).
[6] Simon C. P. Mathematics for Economists. C. P. Simon, L. E. Blume. – New York City: W. W. Norton & Company, 1994. – 960 p.
[7] Labunets A. M. Development of automated control system as service system. A. M. Labunets, N. A.Oreshin A. N. Oreshin. Telekommunikatsia. – M.: Nauka I Tekhnologii, 2006. – № 4. – pp. 8 – 13. (in Russian).
[8] Hyde A. Basic Internet Security. A. Hyde. – Boston: GNU General Public, 2011. – 244 p.
[9] Strelnikova K. O. About efficiency upgrading of tex administration in Russian Federation. K. O. Strelnikova. – Saratov: Povolzhskiy Institut Upravlenia imeni P. A. Stolypina – filial FGBOU VPO «Rossiyskaya academia narodnogo khozyaistva I gosudarstvennoy sluzhbi pri Prezedente Rossiyskoy Federatsii», M., 2014. – pp. 98 – 100. (in Russian).
[10] Harkins M. Managing Risk and Information Security: Protect to Enable. M. Harkins. – Berlin: APress, 2016. – 145 p.
[11] Kostrova A. V. Methods and models of informational management. A. V. Kostrova. – M.: Infra-M, 2014. – 247 p. (in Russian).
[12] Harchol-Balter M. Performance Modeling and Design of Computer Systems: Queueing Theory in Action. M. Harchol-Balter. – Cambridge: Cambridge University Press, 2013. – 576 p.
[13] Stiennon R. There Will Be Cyberwar: How The Move To Network-Centric Warfighting Has Set The Stage For Cyberwar. R. Stiennon. – Birmingham: IT-Harvest Press, 2015. – 174 p.
[14] Tananko I. E. Management by the arriving units in open network of the mass service with concurrent systems operations and untrusted functional devices. I. E.Tananko, N. P. Fokina. Kompiyuternie nauki i informatsionnie tekhnologii: materiali nauchnoy konferentsii. – Saratov: izd-vo Sarat. un-ta, 2010. – pp. 116 – 119. (in Russian).
[15] Balzarotti D. The SysSec Red Book: A Roadmap for Systems Security Research. D. Balzarotti. – EU: SysSec, 2013. – 194 p.

Поступила в редакцию – 28 декабря 2017 г. Окончательный вариант –20 февраля 2018 г.
Received – December 28, 2017. The final version – February 20, 2018.

АННОТАЦИИ

Анатолий А. Малюк, Ольга Ю. Полянская

Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, г. Москва, 115409, Россия
e-mail: AAMalyuk@mephi.ru, https://orcid.org/0000-0002-5746-1508,
e-mail: OYPolyanskaya@mephi.ru, https://orcid.org/0000-0001-9867-3278

ОПЫТ РЕАЛИЗАЦИИ ПИЛОТНОГО ПРОЕКТА ЕВРОПЕЙСКОЙ СИСТЕМЫ ОПОВЕЩЕНИЯ И ОБМЕНА ИНФОРМАЦИЕЙ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. Формирование глобального информационного общества с особой остротой ставит проблему развития культуры информационной безопасности. В Доктрине информационной безопасности Российской Федерации, принятой в декабре 2016 года, как одна из основных угроз определяется низкая осведомленность граждан в вопросах обеспечения личной информационной безопасности.

Одним из наиболее важных механизмов повышения компетентности и формирования культуры информационной безопасности, помимо массового обучения людей, являются методы пропаганды и создания «горячих линий». Они позволяют широкой общественности брать на себя инициативу в наблюдении и уведомлении о компьютерных инцидентах. Развитие подобных подходов целесообразно осуществлять с учетом накопленного сегодня международного опыта.

С этой целью в статье рассматривается европейский опыт создания системы информационно-консультативной помощи в области предупреждения угроз безопасности использования общедоступных и корпоративных информационных систем, а также ликвидации последствий проявления угроз в информационной сфере. Анализ опыта реализации пилотного проекта европейской системы оповещения и обмена информацией выявил целесообразность проектирования подобных систем на основе модели управления с четырьмя игроками, объединяющей операторов сети, производителей информации (которые являются поставщиками ИТ-продуктов или специалистами в области ИТ-безопасности), локальных информационных посредников и потребителей информации. В качестве модели информационного потока может быть выбран узел, который запускает локальный веб-портал, предоставляющий информацию для конечных пользователей, формирует новую информацию, адаптирует информацию к ограничениям различных каналов распространения и к характеристикам целевых групп конечных пользователей. Методология пилотного проекта может быть использована при проектировании и развертывании системы оповещения и обмена информацией, ориентированной на конечных пользователей нескольких регионов или стран, сотрудничающих в области информационной безопасности.

Ключевые слова: информационная безопасность, осведомленность по вопросам информационной безопасности, система оповещения и обмена информацией, культура информационной безопасности.

Jean Y. Astier[1], Igor Y. Zhukov[2], Oleg N. Murashov[3], Alexey P. Bardin[3]

[1]HyperPanel Lab,
Saclay 4 Rue Rene Razel Building'azur 91400 Saclay, France
e-mail: jean-yves.astier@hyperpanel.fr, https://orcid.org/0000-0002-7002-1195
[2]CEO of Ltd. «The National Mobile Portal»,
Volgogradskiy pr.,2 off.36, Moscow, 109316, Russia
e-mail: i.zhukov@inbox.ru, https://orcid.org/0000-0002-4429-8799
[3]Joint-stock company «Ramec-VS»,
Volgogradskiy pr., 2, Moscow, 109316, Russia
e-mail: olegxozbox@yandex.ru, https://orcid.org/0000-0002-4467-2170
e-mail: lovvi@mail.ru, https://orcid.org/0000-0001-8029-6902

A NEW OS ARCHITECTURE FOR IOT

Abstract. Current computer operating systems architectures are not well suited for the coming world of connected objects, known as the Internet of Things (IoT) for multiple reasons: poor communication performances in both point-to-point and broadcast cases, poor operational reliability and network security, excessive requirements both in terms of processor power and memory size leading to excessive electrical power consumption. We introduce a new computer operating system architecture well adapted to IoT, from the most modest to the most complex, and more generally able to significantly raise the input/output capacities of any communicating computer. This architecture rests on the principles of the Von Neumann hardware model, and is composed of two types of asymmetric distributed containers, which communicate by message passing. We describe the sub-systems of both of these types of containers, where each sub-system has its own scheduler, and a dedicated execution level.
Keywords: Internet of Things (IoT), architectures, operating systems.

Вячеслав М. Барбашов, Николай С. Трушкин

[1]Национальный исследовательский ядерный университет «МИФИ»,
115409, Москва, Каширское шоссе, 31, Россия
e-mail: VMBarbashov@mephi.ru, https://orcid.org/0000-0001-7136-415X
e-mail: NSTrushkin@mephi.ru, https://orcid.org/0000-0003-2407-084X

ОСОБЕННОСТИ МОДЕЛИРОВАНИЯ ИНФОРМАЦИОННЫХ ОТКАЗОВ ЦИФРОВЫХ КМОП СБИС ПРИ ВОЗДЕЙСТВИИ РАДИАЦИИ

Аннотация. Рассмотрены методы обеспечения информационной безопасности, которые основаны на применении функционально-логического моделирования больших цифровых интегральных схем (СБИС) при воздействии ионизирующего излучения. Показано, что кратность узла и мощность спектра более точно описывается при использовании понятия нечеткой кратности. Предложены методы прогнозирования информационной безопасности БИС при воздействии ионизирующего излучения, которые основаны на модели нечеткого цифрового и вероятностного надежностного автоматов. Причем характер их изменения при облучении зависит от многих факторов, включая тип излучения, его интенсивность и спектр, вид критериального параметра характеризующего

радиационную стойкость ИС, режим работы микросхем. Поэтому в разных диапазонах уровней или интенсивностей воздействия модель ИС может носить как нечеткий, так и вероятностный характер. Проведения такого сопоставления является необходимым этапом общей процедуры анализа радиационной стойкости ИС.

Ключевые слова: топологические вероятностные модели, нечеткие вероятности, зоны неопределенности.

Алексей А. Гавришев, Александр П. Жук

Северо-Кавказский федеральный университет,
ул. Пушкина, 1, г. Ставрополь, 355009, Россия
e-mail: alexxx.2008@inbox.ru, https://orcid.org/0000-0002-4242-6152
e-mail: alekszhuk@mail.ru, https://orcid.org/0000-0002-0168-8391

РАЗРАБОТКА БЕСПРОВОДНОЙ ИМИТОЗАЩИЩЕННОЙ СИСТЕМЫ ИДЕНТИФИКАЦИЯ И КОНТРОЛЯ ДОСТУПА ТРАНСПОРТНЫХ СРЕДСТВ

Аннотация. В данной статье рассматриваются беспроводные системы идентификации и контроля доступа транспортных средств на охраняемые объекты. Рассмотрены известные системы. В результате установлено, что одним из перспективных подходов к идентификации и контролю доступа транспортных средств на охраняемые объекты является использование систем на основе принципа «свой-чужой». Среди данных систем выделяются «однонаправленные» и «двунаправленные» системы идентификации и контроля доступа. «Двунаправленные» системы являются более предпочтительными для вопросов идентификации и контроля доступа. Однако, в настоящее время, данные системы должны иметь уменьшенную вероятность распознавания структуры запросных и ответных сигналов в силу того, что потенциальный злоумышленник может достаточно легко выполнить несанкционированный доступ к радиоканалу системы. На основании этого разработана беспроводная система идентификации и контроля доступа транспортных средств на охраняемые объекты на основе принципа «свой-чужой», отличающаяся повышенной защищенностью от несанкционированного доступа и подавления помехами за счет использования перезаписываемых накопителей хаотических последовательностей. Дополнительно к этому предлагается использовать для идентификации транспортного средства RFID-метку, содержащую дополнительную информацию о нем. Приведены некоторые технические характеристики разработанной системы (возможный частотный диапазон запросно-ответных сигналов, дальность связи, скорость передачи данных, объем передаваемых данных, рекомендации по выбору RFID-меток). Так же, с помощью аппарата нечеткой логики, была произведена оценка защищенности от несанкционированного доступа запросно-ответных сигналов на основе системы «свой-чужой», передаваемых по радиоканалу, разработанной системы и аналогов. Оценка защищенности разработанной системы показывает достаточный уровень ее защищенности от комплексных угроз (просмотр, подмена, перехват и радиоэлектронное подавление трафика) по сравнению с известными системами данного класса. Среди основных преимуществ разработанной системы следует упомянуть повышенную защищенность от несанкционированного доступа и подавления помехами за счет использования перезаписываемых накопителей хаотических последовательностей, в

которых потенциально можно использовать широкий класс хаотических сигналов. Так же следует отметить повышенную вероятность идентификации проверяемых транспортных средств за счет использования принципа «свой-чужой» и RFID-меток. Среди основных недостатков предложенной системы следует отметить необходимость наличия точной синхронизации между передающей и приемной сторонами.

Ключевые слова: идентификация, контроль доступа, транспортные средства, радиоканал, имитозащищенность, хаотические сигналы.

Ксения Г. Сизова[1], Петр К. Скоробогатов[2], Максим О. Прыгунов[3]

[1]Общество с ограниченной ответственностью «НПЦ «Топаз»,
Учительская улица, 23, литера А, оф. 533, г. Санкт-Петербург, 195269, Россия
e-mail: ksizova@microtopaz.ru, https://orcid.org/0000-0003-0922-3430
[2]Национальный исследовательский ядерный университет «МИФИ»,
Каширское шоссе, 31, г. Москва, 115409, Россия
e-mail: pkskor@spels.ru, https://orcid.org/0000-0002-3146-0304
[3]Общество с ограниченной ответственностью «О2 Световые Системы»,
Новорощинская улица, 4, литера А, г. Санкт-Петербург, 196084, Россия
e-mail: maxim.prygunov@o2svet.ru, https://orcid.org/0000-0002-7895-3536

ПРИМЕНЕНИЕ МЕТОДОВ АНАЛИЗА НАДЕЖНОСТИ И РИСКА ПРИ ОБЕСПЕЧЕНИИ, ПРОГНОЗИРОВАНИИ И ОЦЕНКЕ РАДИАЦИОННОЙ СТОЙКОСТИ РЭА

Аннотация. Установлено соотношение понятий «качества», «надежности», «стойкости» продукции и «риска». Рассмотрен отечественный и зарубежный опыт, а также международные, национальные и отраслевые стандарты в области обеспечения качества технологических систем различного назначения. Выявлено, что зарубежные отраслевые стандарты в области обеспечения качества космических систем оперируют термином «dependability» (в отечественной терминологии сходен с понятием «надежности»), включая в него понятие радиационной стойкости. Определена взаимосвязь между зарубежными отраслевыми, международными и национальными стандартами. Приведены общие сведения по основным методам анализа и оценки надежности и риска, представленным в отечественных и зарубежных нормативных документах. Предлагается применить имеющуюся развитую методологию анализа и оценки надежности и риска для задач обеспечения, прогнозирования и оценки радиационной стойкости РЭА космической техники на всех этапах жизненного цикла.

Ключевые слова: качество, надежность, радиационная стойкость, радиоэлектронная аппаратура, риск.

Михаил Б. Абросимов, Ихаб А. Камил

СГУ имени Н.Г.Чернышевского,
ул. Астраханская, 83, г. Саратов, 410012, Россия
e-mail: mic@rambler.ru, https://orcid.org/0000-0002-4473-8790
e-mail: kamil.iehab@mail.ru, https://orcid.org/0000-0003-1100-5635

РАЗРАБОТКА СИСТЕМЫ ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ С ИСПОЛЬЗОВАНИЕМ ПАРАЛЛЕЛЬНОГО ПРОГРАММИРОВАНИЯ И СИСТЕМЫ ОТКАЗОУСТОЙЧИВОСТИ

Аннотация. Одной из первых угроз побудивших создание систем предотвращения вторжений считают «червь Морриса», который поразил компьютеры в конце 1988г. Системы предотвращения вторжений развивались, и со временем стали полноценной системой, включающей в себя специальные проактивные методы предотвращения атак, рассчитанные для защиты от различного рода угроз. Среди проактивных систем предотвращения вторжений можно выделить следующие: поведенческий анализатор процессов для анализа поведения запущенных в системе процессов, системы устранение возможностей попадания инфекции на компьютер, системы блокировка портов, системы блокировки DoS-атак.

В статье описывается разработанная система предотвращения вторжений. Цель работы раскрыть возможности использования параллельных потоков для улучшения работы систем предотвращения вторжений. Эффективность разрабатываемой системы достигается за счет организации предотвращение атак на уровне конкретного узла, путем контроля всех системных вызовов. Система служит посредником между открытой и защищенной средой. Для повышения скорости передачи/приема информации в системе была использована технология отказоустойчивости. Актуальность темы определяется ростом бесчисленного количества разнообразных вредоносных программ, и возрастающей необходимости в защите корпоративной информации.

Ключевые слова: системы предотвращения вторжений, безопасное соединение, отказоустойчивость, параллельное программирование, вирусы, технология виртуализации, вредоносный трафик.

Юрий Е. Козлов

Финансовый университет при Правительстве Российской Федерации
(Финансовый университет),
Ленинградский проспект, 49, Москва, 125993, Россия
e-mail: kozlovye@yandex.ru, https://orcid.org/0000-0002-4448-0232

ПОДХОДЫ К ОПРЕДЕЛЕНИЮ НАДЕЖНОСТИ МУЛЬТИМОДАЛЬНОЙ ТРЕХМЕРНОЙ ДИНАМИЧЕСКОЙ ПОДПИСИ

Аннотация. Рынок современных мобильных приложений предъявляет все более жесткие требования к надежности систем аутентификации. В статье рассматривается аутентификация с использованием мультимодальной трехмерной динамической подписи (МТДП), которая может использоваться в качестве основного или дополнительного средства аутентификации пользователей в мобильных приложениях. В ее основе лежит

использование жеста в воздухе, выполняемого двумя независимыми мобильными устройствами в качестве идентификатора. Методика использования МТДП имеет ряд преимуществ по сравнению с используемыми в настоящее время биометрическими методиками, такими как отпечаток пальца, аутентификация по форме лица или речевая аутентификация. Она позволяет быстро сменить жест, который служит идентификатором, а также скрывать саму процедуру аутентификации, используя жесты, не привлекающие внимание. Несмотря на преимущества, использование МТДП имеет ряд ограничений, прежде всего — это необходимость выработки человеком функционально динамического комплекса (ФДК). Он необходим для повторения аутентифицирующего жеста с достаточной точностью. Для корректного формирования МТДП необходима система, реализующая оценку надежности жеста, а также его допустимые вариации. Подходы к решению данной задачи описаны в данной статье с разделением их по способам их реализации. Два подхода могут быть реализованы только с использованием сервера, как центра обработки МТДП, а один может быть реализован с использованием вычислительных ресурсов смартфона. В заключительной части статьи приведены данные опробования одной из методик на макете, реализующем аутентификацию при помощи МТДП.

Ключевые слова: аутентификация, мобильное устройство, акселерометр, персонализированный жест, подпись в воздухе, аутентификация жестом.

Эдита К. Куулар[1], Андрей И. Труфанов[1], Алексей А. Тихомиров[2]

[1]Иркутский Национальный Исследовательский Технический Университет,
Лермонтова, 83, Иркутск, 6664074, Россия
e-mail: kuular1991@mail.ru, https://orcid.org/0000-0003-4832-3397
e-mail: troufan@gmail.com, https://orcid.org/0000-0002-6967-3495
[2]Университет ИНХА,
Инчеон, Республика Корея
e-mail: alexeitikhomirovprof@gmail.com, https://orcid.org/0000-0002-7317-5851

ДВУХКОМПОНЕНТНАЯ СЕТЕВАЯ МОДЕЛЬ В ТЕХНОЛОГИЯХ ГОЛОСОВОЙ ИДЕНТИФИКАЦИИ ЛИЧНОСТИ

Аннотация. Среди важнейших параметров биометрических систем голосовой модальности, определяющих их эффективность, наряду с надежностью и помехоустойчивостью выделяют скорость идентификации и верификации личности. Данный параметр особенно чувствителен при обработке крупномасштабных баз голосовых данных в режиме реального времени. Многие исследовательские работы в данной области направлены на разработку новых и совершенствование имеющихся алгоритмов представления и обработки речевых записей, обеспечивающих высокую производительность голосовых биометрических систем. Здесь перспективным представляется современный подход к решению сложных объемных задач с большим числом элементов и учетом их взаимосвязей, использующий платформу комплексных сетей. Так, известны работы, в которых при решении задачах анализа и распознавания лиц по фотографиям изображения трансформируются в комплексные сети для последующей их обработки стандартными приемами. Одним из первых применений комплексных сетей

в задачах анализа звуковых рядов (музыкальных и речевых) являлось описание их частотных характеристик с помощью построения сетевых моделей – конвертации рядов в сети. На платформе сетевой онтологии в данной работе развит предложенный ранее метод представления аудиоинформации с целью ее высокопроизводительного автоматического анализа и снижения погрешности в распознавании личности – диктора. Для этого предполагается конвертирование звуковой информации в форму ассоциативной семантической (когнитивной) сетевой структуры, содержащей две компоненты: амплитудную и частотную. Были записаны два речевых примера с последующей их трансформацией в соответствующие сети и сравнением топологических метрик. Набор топологических метрик каждой из сетевых моделей (амплитудной и частотной) представляет собой вектор, а вместе - матрицу, как цифровой "сетевой" отпечаток голоса. Предлагаемый сетевой подход с его чувствительностью к состоянию индивида – физиологическому, психологическому, эмоциональному, может оказаться полезным не только для задач идентификации личности, но и для определения ее состояния.

Ключевые слова: биометрические модальности, звуковая информация, идентификация диктора, комплексные сети, амплитуда, частота.

Игнатий А. Грачков

Федеральная служба по техническому и экспортному контролю,
105175, г. Москва, Старая Басманная, 17
e-mail: ignat958@gmail.com, https://orcid.org/0000-0001-6327-3530

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АСУ ТП: ВОЗМОЖНЫЕ ВЕКТОРА АТАКИ И МЕТОДЫ ЗАЩИТЫ

Аннотация. Автоматизированные системы управления технологическими процессами (АСУ ТП) являются важнейшей частью промышленной инфраструктуры и используются на таких объектах, как нефте- и газопроводы, водораспределительные системы, электрические сети, атомные электростанции и производство. На сегодняшний день проблема обеспечения информационной безопасности АСУ ТП стоит довольно остро. Специалистами из разных стран проведено большое количество исследований в данной области. Способность злоумышленников обнаружить промышленные устройства, доступные через Интернет, и получать к ним несанкционированный доступ вызывает тревогу в кругах специалистов по информационной безопасности. Поисковик Shodan предоставляет атакующим мощный инструмент для идентификации автоматизированных системы управления и их компонентов и последующих злонамеренных воздействий на них.

В данной статье дано описание типовой АСУ ТП; представлен общий анализ защищенности современных АСУ ТП; описаны возможные вектора атак на АСУ ТП; описан пример получения несанкционированного доступа к АСУ ТП с использованием поисковика Shodan; даны рекомендации по обеспечению информационной безопасности АСУ ТП.

Ключевые слова: автоматизированные системы управления, технологические процессы, АСУ ТП, информационная безопасность, защита информации, вектор атаки, Shodan.

Юлия Г. Красножон

Филиал Федерального казенного учреждения «Налог-Сервис» Федеральной налоговой службы России по центрам обработки данных в г. Москве,
125373, г. Москва, Проходной пер., д. 3, к.3,
e-mail: turchina.yuliya.07@gmail.com, https://orcid.org/0000-0002-8311-7735

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ КАК СРЕДСТВО ОПТИМИЗАЦИИ СИСТЕМЫ АВТОМАТИЗАЦИИ ПРОЦЕССА УПРАВЛЕНИЯ ИНЦИДЕНТАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. Современные информационные технологии оказывают все большее влияние на динамику развития и структуру управления организацией. Эффективность управленческой деятельности при внедрении современных информационных технологий, напрямую зависит от качества управления инцидентами информационной безопасности. Вместе с тем, как в российских, так и в зарубежных трудах не в достаточной степени освещены вопросы оценки влияния управления инцидентами информационной безопасности на качество и эффективность системы управления предприятием. Для решения этих проблем ключевым направлением является оптимизация системы автоматизации процесса управления инцидентами информационной безопасности. Сегодня особое внимание уделяется процессам управления инцидентами информационной безопасности на таких критически важных объектах Российской Федерации, как Федеральная налоговая служба России (ФНС). Для построения математической модели оптимизации данной системы предлагается использовать математический аппарат теории массового обслуживания. Разработанная модель позволит оценить качество управленческой деятельности с учетом правил и ограничений, накладываемых на систему влияниями реальных факторов инцидентов информационной безопасности. В статье рассматривается пример, демонстрирующий работу системы, приведены полученные статистические данные. Построение такой системы позволит повысить качество предоставляемых ФНС России сервисов и скорость реагирования на инциденты информационной безопасности.

Ключевые слова: угроза информационной безопасности, автоматизированная информационная система, инциденты информационной безопасности, Центры обработки данных Федеральной налоговой службы России, управление инцидентами информационной безопасности.

ABSTRACT

Anatoly A. Malyuk, Olga Y. Polyanskaya

National Nuclear Research University MEPHI (Moscow Engineering Physics Institute),
Kashirskoe shosse, 31, Moscow, 115409, Russia,
e-mail: AAMalyuk@mephi.ru, https://orcid.org/0000-0002-5746-1508,
e-mail: OYPolyanskaya@mephi.ru, https://orcid.org/0000-0001-9867-3278

Experience of the pilot implementation of the european information sharing and alerting system in the field of information security

Abstract. The formation of a global information society poses a particular challenge to the development of an information security culture. In the Doctrine of Information Security of the Russian Federation, adopted in December 2016, one of the main threats is the low awareness of citizens in matters of ensuring personal information security.

One of the most important mechanisms for increasing competence and forming an in-formation security culture, in addition to mass training of people, are methods of propaganda and creation of "hot lines". They allow the general public to take the initiative in monitoring and reporting computer incidents. The development of such approaches should be carried out taking into account the international experience accumulated today.

To this end, the article examines the European experience of creating a system of information and advisory assistance in the field of preventing threats to the security of public and corporate information systems, primarily information and telecommunications networks, as well as eliminating the consequences of threats in the information sphere. The analysis of the experience of implementing the pilot project of the European Information Sharing and Alert System has revealed the advisability of designing such systems on the basis of a management model with four players that unites network operators, information producers (who are IT product suppliers or IT security specialists); local information intermediaries and consumers of information. As a model of the information flow, a node can be selected that runs a local web portal that provides information to end users, generates new information, adapts information to the constraints of various distribution channels, and to the characteristics of end-user target groups. The methodology of the pilot project can be used in the design and deployment of a notification and information exchange system aimed at end-users of several regions or countries cooperating in the field of information security.

Keywords: information security, information security awareness, information sharing and alerting system, culture of information security.

Jean Y. Astier[1], Igor Y. Zhukov[2], Oleg N. Murashov[3], Alexey P. Bardin[3]

[1]*HyperPanel Lab,*
Saclay 4 Rue Rene Razel Building'azur 91400 Saclay, France
e-mail: jean-yves.astier@hyperpanel.fr, https://orcid.org/0000-0002-7002-1195
[2]*CEO of Ltd. «The National Mobile Portal»,*
Volgogradskiy pr.,2 off.36, Moscow, 109316, Russia

e-mail: i.zhukov@inbox.ru, https://orcid.org/0000-0002-4429-8799
[3]Joint-stock company «Ramec-VS»,
Volgogradskiy pr., 2, Moscow, 109316, Russia
e-mail: olegxozbox@yandex.ru, https://orcid.org/0000-0002-4467-2170
e-mail: lovvi@mail.ru, https://orcid.org/0000-0001-8029-6902

A New OS Architecture for IoT

Abstract. Current computer operating systems architectures are not well suited for the coming world of connected objects, known as the Internet of Things (IoT) for multiple reasons: poor communication performances in both point-to-point and broadcast cases, poor operational reliability and network security, excessive requirements both in terms of processor power and memory size leading to excessive electrical power consumption. We introduce a new computer operating system architecture well adapted to IoT, from the most modest to the most complex, and more generally able to significantly raise the input/output capacities of any communicating computer. This architecture rests on the principles of the Von Neumann hardware model, and is composed of two types of asymmetric distributed containers, which communicate by message passing. We describe the sub-systems of both of these types of containers, where each sub-system has its own scheduler, and a dedicated execution level.
Keywords: Internet of Things (IoT), architectures, operating systems.

Vyacheslav M. Barbashov, *Nikolai* S. Trushkin

National Research Nuclear University MEPHI,
Kashirskoe shosse, 31, Moscow, 115409, Russia
e-mail: VMBarbashov@mephi.ru, https://orcid.org/0000-0001-7136-415X
e-mail: NSTrushkin@mephi.ru, https://orcid.org/0000-0003-2407-084X

Features of the model of main information failures in digital CMOS VLSI at impact of the radiation

Abstract. The methods of information security, which are based on the use of functional-logical modeling of very large digital integrated circuits (VLSI) under the influence of ionizing radiation are considered. It is shown that the multiplicity of the node and the power of the spectrum are more accurately described when using the concept of fuzzy multiplicity. Methods are proposed for predicting LSI failures when exposed to ionizing radiation, which are based on the model of fuzzy digital and probabilistic reliability automata. Moreover, the nature of their changes during irradiation depends on many factors, including the type of radiation, its intensity and range, type a criteria parameter characterizing the radiation resistance of ICs and work mode. Therefore, in different ranges of levels or intensities of the impact of the IC model can be either of fuzzy or probabilistic nature. Carrying out such a comparison is an essential step in the overall analysis of the IC radiation resistance.
Keywords: topological probabilistic models, fuzzy probability, areas of uncertainty.

Aleksei A. Gavrishev, Aleksandr P. Zhuk

North Caucasus Federal University,
Pushkin St., 1, Stavropol, 355009, Russia
e-mail: alexxx.2008@inbox.ru, https://orcid.org/0000-0002-4242-6152
e-mail: alekszhuk@mail.ru, https://orcid.org/0000-0002-0168-8391

Development of a wireless protection against imitation system for identification and control of vehicle access

Abstract. This article deals with wireless systems for identification and control of vehicle access to protected objects. Known systems are considered. As a result, it has been established that one of the most promising approaches to identifying and controlling vehicle access to protected objects is the use of systems based on the "friend or foe" principle. Among these systems, there are "one-directional" and "bedirectional" identification and access control systems. "Bidirectional" systems are more preferable for questions of identification and access control. However, at present, these systems should have a reduced probability of recognizing the structure of the request and response signals because the potential attacker can easily perform unauthorized access to the radio channel of the system. On this basis, developed a wireless system identification and control vehicle access to protected objects based on the principle of "friend or foe", featuring increased protection from unauthorized access and jamming through the use of rewritable drives chaotic sequences. In addition, it's proposed to use to identify the vehicle's RFID tag containing additional information about it. Are some specifications of the developed system (the possible frequency range of the request-response signals, the communication range, data rate, the size of the transmitted data, guidelines for choosing RFID). Also, with the help of fuzzy logic, was made the security assessment from unauthorized access request-response signals based on the system of "friend or foe", which are transferred via radio channel, developed systems and analogues. The security assessment of the developed system shows an adequate degree of protection against complex threats (view, spoofing, interception and jamming of traffic) in comparison with known systems of this class. Among the main advantages of the developed system it's necessary to mention increased security from unauthorized access and jamming through the use of rewritable drives chaotic sequences, in which you can potentially use a wide class of chaotic signals. It should also be noted the increased likelihood of identification check the vehicle through the use of the principle of "friend or foe" and RFID. Among the main disadvantages of the proposed system it should be noted the need for precise synchronization between transmitting and receiving sides.
Keywords: identification, access control, vehicles, radio channel, protection against imitation, chaotic signals.

Ksenia G. Sizova[1], Petr K. Skorobogatov[2], Maksim O. Prygunov[3]

[1]Limited liability company "NPC "Topaz",
23 Uchitelskaya str., letter A, Saint-Petersburg, 195269, Russian Federation
e-mail: ksizova@microtopaz.ru, https://orcid.org/0000-0003-0922-3430
[2]National Research Nuclear University MEPHI (Moscow Engineering Physics Institute),
31, Kashirskoe sh., Moscow, 114509, Russian Federation

e-mail: pkskor@spels.ru, https://orcid.org/0000-0002-3146-0304
[3]Limited liability company "O2 Light Systems",
[4]Novoroshhinskaja str., letter A, Saint-Petersburg, 196084, Russian Federation
e-mail: maxim.prygunov@o2svet.ru, https://orcid.org/0000-0002-7895-3536

Application of dependability and risk analysis methods in the process of implementation, prediction and evaluation of electronic equipment radiation hardness

Abstract. The relationship between the concepts of "quality", "dependability", "hardness" of products and "risk" is established. The domestic and foreign experience, as well as international, national and industry standards in the field of quality assurance of electrotechnical systems for various purposes are considered. It was revealed that the foreign industry standards in the field of quality assurance of space systems use the term "dependability" (in the domestic terminology it is similar to the notion of "reliability"), including the concept of radiation resistance. The correlation among foreign industry, international and national standards is defined. General information on the main methods of analysis and assessment of dependability and risk, presented in domestic and foreign documents, are considered. The authors of the paper propose to apply the existing developed methodology of analysis and evaluation of dependability and risk for the tasks of ensuring, predicting and assessing the radiation hardness of space systems at all stages of the life cycle.
Keywords: quality, dependability, radiation hardness, electronic equipment, risk.

Mikhail B. Abrosimov, Iehab A. Kamil

Saratov state University named after N. G. Chernyshevskogo,
St. Astrakhanskaya, 83, Saratov, 410012, Russia
e-mail: mic@rambler.ru, https://orcid.org/0000-0002-4473-8790
e-mail: kamil.iehab@mail.ru, https://orcid.org/0000-0003-1100-5635

Development Intrusion Prevention System by Using Parallel Programming and Fault Tolerance Technology

Abstract. One of the first threats that prompted the creation of intrusion prevention systems is considered to be the "Morris worm", which hit computers in late 1988. Intrusion prevention systems evolved, and eventually became a full-fledged system incorporating special proactive methods to prevent attacks, designed to protect against various kinds of threats. Among the proactive intrusion prevention systems are the following: a behavioral process analyzer for analyzing the behavior of processes running in the system, eliminating the possibility of infection on the computer, locking the ports, blocking the DoS attacks.
In article the developed system of prevention of invasions is described. It is more effective to develop and use the systems of prevention of invasions as separate means of protection which will serve as the intermediary between the protected and opened networks. It is more expedient to organize prevention of the attacks at the level of concrete knot, by control of all system calls. Special attention in article is paid to use of technologies of parallel programming in the developed system. The main advantages of system of fault tolerance and the used algorithms for realization of technology of prevention of invasions are described.

Keywords: the intrusion prevention system, secure communication, fault tolerance, parallel programming, viruses, virtualization, malicious traffic.

Yury E. Kozlov

Financial University under the Government of the Russian Federation
(Financial University),
Leningradsky Prospekt, 49, Moscow, 125993 (ГСП-3), Russia
e-mail: kozlovye@yandex.ru, https://orcid.org/0000-0002-4448-0232

Approaches to determining the reliability of a multimodal three-dimensional dynamic signature

Abstract. The market of modern mobile applications has increasingly strict requirements for the authentication system reliability. This article examines an authentication method using a multimodal three-dimensional dynamic signature (MTDS), that can be used both as a main and additional method of user authentication in mobile applications. It is based on the use of gesture in the air performed by two independent mobile devices as an identifier.

The MTDS method has certain advantages over currently used biometric methods, including fingerprint authentication, face recognition and voice recognition. A multimodal three-dimensional dynamic signature allows quickly changing an authentication gesture, as well as concealing the authentication procedure using gestures that do not attract attention. Despite all its advantages, the MTDS method has certain limitations, the main one is building functionally dynamic complex (FDC) skills required for accurate repeating an authentication gesture.

To correctly create MTDS need to have a system for assessing the reliability of gestures. Approaches to the solution of this task are grouped in this article according to methods of their implementation. Two of the approaches can be implemented only with the use of a server as a centralized MTDS processing center and one approach can be implemented using smartphone's own computing resources. The final part of the article provides data of testing one of these methods on a template performing the MTDS authentication.

Keywords: authentication, mobile device, accelerometer, personalized gestured, in-air signature, handwaving authentication.

Edita K. Kuular[1], Andrey I. Trufanov[1], Alexei A. Tikhomirov[2]

[1]Irkutsk National Research Technical University,
Lermontov street,83, Irkutsk,664074,Russia
e-mail: kuular1991@mail.ru, https://orcid.org/0000-0003-4832-3397
e-mail: troufan@gmail.com, https://orcid.org/0000-0002-6967-3495
[2]INHA University,
Incheon, Republic of Korea
e-mail: alexeitikhomirovprof@gmail.com, https://orcid.org/0000-0002-7317-5851

Two-component network model in voice identification technologies

Abstract. Among the most important parameters of biometric systems with voice modalities that determine their effectiveness, along with reliability and noise immunity, a speed of identification

and verification of a person has been accentuated. This parameter is especially sensitive while processing large-scale voice databases in real time regime. Many research studies in this area are aimed at developing new and improving existing algorithms for presentation and processing voice records to ensure high performance of voice biometric systems. Here, it seems promising to apply a modern approach, which is based on complex network platform for solving complex massive problems with a large number of elements and taking into account their interrelationships. Thus, there are known some works which while solving problems of analysis and recognition of faces from photographs, transform images into complex networks for their subsequent processing by standard techniques. One of the first applications of complex networks to sound series (musical and speech) analysis are description of frequency characteristics by constructing network models - converting the series into networks. On the network ontology platform a previously proposed technique of audio information representation aimed on its automatic analysis and speaker recognition has been developed. This implies converting information into the form of associative semantic (cognitive) network structure with amplitude and frequency components both. Two speaker exemplars have been recorded and transformed into pertinent networks with consequent comparison of their topological metrics. The set of topological metrics for each of network models (amplitude and frequency one) is a vector, and together those combine a matrix, as a digital "network" voiceprint. The proposed network approach, with its sensitivity to personal conditions-physiological, psychological, emotional, might be useful not only for person identification, but also for determining his /her condition.

Keywords: biometric modalities, sound information, speaker identification, complex net-works, amplitude, frequency.

Ignatiy A. Grachkov

FSTEC of Russia,
105175, Moscow, Staraya Basmannaya, 17
e-mail: ignat958@gmail.com, https://orcid.org/0000-0001-6327-3530

Information security of industrial control systems: possible attack vectors and protection methods

Abstract. Industrial control systems are employed in numerous critical infrastructure assets including oil and gas pipelines, water distribution systems, electrical power grids, nuclear plants and manufacturing facilities. Today the problem of ensuring information security of the industrial control system is quite acute. Specialists from different countries conducted a large number of studies in this field. The ability of intruders to discover industrial devices accessible via the Internet and to obtain unauthorized access to them is of concern to information security professionals. The Shodan search engine provides the attacker with a powerful tool to identify industrial control systems and their components and subsequent malicious effects on them.
In this article the author describes the typical industrial control system, presents general analy-sis of the security of modern ICS and describes possible attack vectors on the ICS. An example of obtaining unauthorized access to industrial control systems using the Shodan search engine is described and recommendations how to ensure information security of the industrial control system are given.

Keywords: industrial control systems, technological processes, ICS, Information Security, data protection, attack vector, Shodan.

Yulia G. Krasnozhon

The Federal State-funded Institution branch «Nalog-Servis» of the Federal Tax Service of Russia on data processing centre in Moscow city,
125373, Moscow city, Prokhodnoy offstreet, h. 3, bld. 3,
e-mail: turchina.yuliya.07@gmail.com, https://orcid.org/0000-0002-8311-7735

Mathematical model as means of optimization of the automation system of the process of incidents of information security management

Abstract. Modern information technologies have an increasing importance for development dynamics and management structure of an enterprise. The management efficiency of implementation of modern information technologies directly related to the quality of information security incident management. However, issues of assessment of the impact of information security incidents management on quality and efficiency of the enterprise management system are not sufficiently highlighted neither in Russian nor in foreign literature. The main direction to approach these problems is the optimization of the process automation system of the information security incident management. Today a special attention is paid to IT-technologies while dealing with information security incidents at mission-critical facilities in Russian Federation such as the Federal Tax Service of Russia (FTS). It is proposed to use the mathematical apparatus of queueing theory in order to build a mathematical model of the system optimization. The developed model allows to estimate quality of the management taking into account the rules and restrictions imposed on the system by the effects of information security incidents. Here an example is given in order to demonstrate the system in work. The obtained statistical data are shown. An implementation of the system discussed here will improve the quality of the Russian FTS services and make responses to information security incidents faster.
Keywords: information security threat, automated information data system, information security incidents, Data-processing centers of Federal Tax Service of the Russian Federation, management of incidents of information security.

ПРАВИЛА ДЛЯ АВТОРОВ

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, полоса А4, кегль 12, шрифт TimesNewRoman, интервал полуторный;
– в начале статьи идут сведения о статье **на английском языке**: И.О. Фамилия авторов (по центру, строчными буквами); далее сведения об авторах – должность, ученая степень, ученое звание, место работы, контактный телефон, адрес электронной почты и личный идентификатор ORCID (по центру, строчными буквами, курсив); затем название статьи (по центру, строчными буквами, полужирно с подчеркиванием); ключевые слова (не более шести, по ширине, курсив); аннотация (8–12 строк, по ширине, строчными буквами);
– далее идут сведения о статье **на русском языке**: И.О. Фамилия авторов (по ценитру, строчными буквами); далее сведения об авторах – должность, ученая степень, ученое звание, место работы, контактный телефон, адрес электронной почты и личный идентификатор ORCID (по центру, строчными буквами, курсив); затем название статьи (по центру, строчными буквами, полужирно с подчеркиванием); ключевые слова (не более шести, по ширине, курсив); аннотация (8–12 строк, по ширине, строчными буквами);
– затем идет текст статьи на русском или английском языке, кегль 12, интервал полуторный, рекомендуемый общий объем статьи не должен превышать 10 страниц, включая таблицы, иллюстрации;
– 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);
– после списка литературы идет REFERENCES, в котором эти библиографические источники должны быть написаны латиницей (т.е. латинскими буквами).

Условия опубликования статьи:

– статья может быть выслана по электронной почте или представлена в редакцию на бумажном (одном экземпляре) и электронном носителях (кроме дискет);
– 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 изработ других лиц, необходимы ссылки на соответствующие публикации или письменное разрешение автора;
– решение о публикации рукописи принимается редакционной коллегией на основании результата рецензирования и экспертной оценки квалифицированными специалистами в области ИБ;
– 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 публикации;

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

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. Картинки, графики, фотографии и другие виды иллюстраций, по возможности, следует предоставлять не только включенными в текст, но и отдельными файлами в исходном формате (не интегрированными в документ Word).
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 желательно обращать внимание на наличие выходных данных работ и избегать повторных указаний одной и той же работы под разными номерами.
7. Ссылки на законы, нормативные акты, конфенции и прочее желательно указывать по установленной форме: Закон РФ «__» от х месяца хххх г. № ___. Ст. ___.
8. Иноязычные слова, термины и фамилии, написание которых допускает варианты, просьба писать в пределах одной статьи одинаково.

Заранее спасибо,
редакционная коллегия

AUTHOR GUIDELINES

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).

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 шоссе, 31, Москва, 115409, Россия
Тел.: +7 (495) 788 5699, тоновый режим 9216 или 9087.
Факс: +7 (499) 324-86-00.
Editorial address: Kashirskoe shosse, 31, Moscow, 115409, Russia
Tel. +7 (495) 788 5699, tone mode set 9216 or 9087.
Fax: +7 (499) 324-86-00.
E-mail: BIT@mephi.ru
https://bit.mephi.ru

Периодичность выхода - 4раза в год / Periodicity - 4 times a year

Подписка на журнал
производится на почтовых отделениях связи
по каталогу «Пресса России»

Подписной индекс 29226

Цена в продаже свободная / Price selling free

Технический редактор Т.В. Волвенкова
Корректор Е.Г. Станкевич
Верстка Г.А. Бобровой

Подписано в печать 06.03.2018. Формат 60x84 1/8.
Печ.л. 15,5. Уч.-изд.л. 15,5.

Национальный исследовательский ядерный университет «МИФИ»
Каширское шоссе, 31, Москва, 115409, Россия

National Research Nuclear University MEPHI
Kashirskoe shosse, 31, Moscow, 115409, Russia

Типография ООО «Клуб печати»
127018, Москва, Марьиной Рощи 3-й проезд, 40