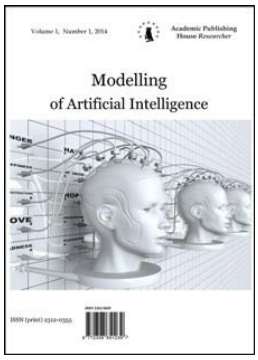
Published in the Russian Federation
Modeling of Artificial Intelligence
Has been issued since 2014.
ISSN: 2312-0355
E-ISSN: 2413-7200
Vol. 7, Is. 3, pp. 212-220, 2015

DOI: 10.13187/mai.2015.7.212
www.ejournal11.com



UDC 004.89

Projecting Intelligent Systems to Protect Information in Automated Data Processing Systems (Functional Approach)

[1] Simon Zh. Simavoryan
[2] Arsen R. Simonyan
[3] Elena I. Ulitina
[4] Rafik A. Simonyan

[1] Sochi state university, Russian Federation
Sovetskaya Str., 26 a, Sochi, Krasnodar region 354000
PhD (Technical), Associate professor
E-mail: simsim58@mail.ru
[2] Sochi state university, Russian Federation
Sovetskaya Str., 26 a, Sochi, Krasnodar region 354000
PhD (Physics and mathematical), Associate professor
E-mail: oppm@mail.ru
[3] Sochi state university, Russian Federation
Sovetskaya Str., 26 a, Sochi, Krasnodar region 354000
PhD (Physics and mathematical), Associate professor
E-mail: elenaulitina@mail.ru
[4] Kuban State University, Russian Federation
350040, Krasnodar, Stavropolskaya St., 149
E-mail: raf55@list.ru
Post-graduate student

Abstract

The article presents the general principles and functional requirements for the design of intelligent systems of information protection, intended for use in the ADPS. The study analyzes the standards and the general provisions on data protection on the basis of GOST P 52069-2003 and others. In conclusion, the authors note that the proposed approach provides the complete coverage of all technological stages of designing systems of information protection, which requires further elaboration and additional research.

Keywords: information security, intelligent systems.

Введение

Цели и принципы стандартизации в Российской Федерации установлены Федеральным законом от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании» [1], а правила применения национальных стандартов Российской Федерации установлены в

ГОСТ Р 1.02004 «Стандартизация в Российской Федерации. Основные положения» [2]. Изменения (замены) существующих стандартов целесообразно проверить на сайтах по указателям «Росстандарт» и «Национальные стандарты» [3,4], составленных по состоянию на текущий момент времени.

В настоящее время активно ведутся работы по разработке единых стандартов создания интегрированных интеллектуальных систем безопасности объектов и территории государства [5]. Согласно этому нормативному документу, обязательными условиями для интегрированных интеллектуальных систем безопасности являются: открытые коды, открытые протоколы, предоставление объекта территории в 3D-графике, привязка датчиков приборов и видеоизображения к координатам Земли, полицентрическая система и право доступа через электронную подпись - самую надежную систему защиты информации. Соблюдение этих постулатов - залог создания единой системы безопасности государства, поскольку этот стандарт создавался не под конкретную компанию, а призван быть универсальным. Проект этого стандарта еще не опубликован, поэтому в настоящей статье авторами предложен свой подход по общим принципам и функциональным требованиям по проектированию интеллектуальных систем защиты информации, предназначенных для использования в АСОД.

Материалы и методы

В рамках исследования были проанализированы система стандартов и общие положения по защите информации на основе ГОСТ Р 52069-2003 [6] и других.

Результаты и их обсуждение

Основополагающими государственными стандартами Российской Федерации в области защиты информации, с точки зрения исследуемого в данной работе вопроса, являются стандарты [6-18].

Интеллектуальная система защиты информации (ИСЗИ) представляет собой интеллектуальную управляющую систему, состоящую из подсистем защиты информации, которая объединяет все подсистемы защиты информации, в единое целое, с целью защиты информации от интеллектуального злоумышленного действия. Концептуальным требованием к таким системам является требование адаптируемости к изменениям внешней и внутренней сред, связанных с защищённостью (целостностью) информации обрабатываемой, циркулирующей и хранящейся в АСОД. ИСЗИ, в общем случае, предназначены для: 1) обеспечения эффективной защиты информации в АСОД и 2) управления защитой информации на всех уровнях борьбы с интеллектуальным злоумышленником [19, 20].

Это можно осуществить за счет интеграции подсистем защиты информации в единую интеллектуальную систему защиты информации, с интеллектуальной обработкой ситуаций, приводящих к НПИ злоумышленником. Подсистемы ИСЗИ должны выполнять следующие функции: 1) предупреждения доступа злоумышленника в зону защиты информации; 2) предупреждение наличия канала НПИ в зоне защиты информации; 3) предупреждения наличия информации в канале НПИ в момент доступа злоумышленника, 4) локализации НПИ; 5) ликвидации последствий НПИ. В обоснованных случаях в задачи объектовых ИСЗИ могут входить функции защиты информации по ГОСТ Р ИСО/МЭК 15408-2-2002 [9]. ГОСТ Р 50739 [11].

Задачи контроля ситуаций и процессов, связанных с безопасностью в чрезвычайных ситуациях, осуществляются службой защиты информации по разработанным алгоритмам принятия решений по оперативно-диспетчерскому управлению средствами защиты информации на основе методов искусственного интеллекта [21], а также на основе ГОСТ Р 22.0.07-95 [16] и ГОСТ Р 27.003-2011 [17]. С этой целью проводится мониторинг, сбор, упорядочение и анализ собранных данных о состоянии (целостности, безопасности, защищённости и т.д.) объектов АСОД. Анализируются технологические схемы обработки информации, а также воздействия от разнообразных внутренних и внешних источников дестабилизирующих факторов. По итогам мониторинга. проводится анализ защищенности информации на объектах АСОД, подготавливаются условия для принятия решений по оперативно-диспетчерскому управлению защитой информации. Проводятся мероприятия

по обеспечению координации действий службы защиты информации, которая ставит и решает задачи защиты информации, осуществляет распределение средств защиты информации, необходимых для функционирования объектов АСОД, а также подготавливает данные для задач планирования и календарно-планового руководства защитой информации в АСОД

Программно-аппаратные средства защиты информации должны обеспечивать решение следующих задач [15]:

- составление регламента и контроль обслуживания источников событий (сообщений, сигналов с датчиков состояния объектов, видео-кадров, аудио-записей и др. видов наблюдения, различного рода документов);
- регистрация событий и определение источников сообщений о событиях;
- идентификация событий и упорядочение потока событий;
- оперативная обработка событий в соответствии с заранее определенными правилами подготовки принятия решений;
- организация эффективного хранения событий и регистрации принятых по ним действий (ведение архива истории событий);
- определение корреляционных связей между зарегистрированными и обработанными событиями (поиск взаимосвязанных событий, объектов и субъектов для принятия решений, планирования мероприятий и других действий в интересах выполнения функциональных задач, иерархически связанных и/или других взаимодействующих автоматизированных информационных систем);
- принятие решений и формирование необходимых адресных сообщений для их исполнения оператором или исполнительными механизмами автоматизированных систем управления.

С технической точки зрения ИСЗИ должна функционировать круглосуточно и все её компоненты должны быть восстанавливаемыми изделиями [17]. Состав и структура ИСЗИ должны быть разработаны с учетом адаптируемости системы к изменениям внутренней и внешней сред, а также факторов, влияющих на защиту информации.

Объективная необходимость формирования полной структуры ИСЗИ с функциональной точки зрения функционального подхода становится практически абсолютным, поскольку основным концептуальным требованием к функциям является требование полноты [18, 22]. Прежде всего было установлено, что с целью формирования возможно полного подсистем защиты информации, необходимо построить строго полную классификационную их структуру. Такая структура может быть построена, если в качестве критериев классификации выбрать следующие два показателя: 1) функции защиты информации; 2) зоны защиты информации. По первому критерию будем различать функции, приведенные выше: 1) предупреждения доступа злоумышленника в зону защиты информации; 2) предупреждение наличия канала НПИ в зоне защиты информации; 3) предупреждения наличия информации в канале НПИ в момент доступа злоумышленника, 4) локализации НПИ; 5) ликвидации последствий НПИ. По второму критерию - зоны защиты АСОД: 1) внешняя, 2) территории, 3) помещений; 4) ресурсов; 5) базы данных [18].

Структура и содержание ИСЗИ приводится на рис.1. Полнота представленной классификационной структуры гарантируется тем, выбранные критерии классификации охватывают все зоны защиты информации, а приведенные функции обеспечивают полноту защиты информации, которые в обоснованных случаях можно расширить по ГОСТ Р 50739 [11].

Таким образом, получено десять подсистем защиты информации, состоящих из блоков защиты информации, словно разделенных на горизонтальные и вертикальные подсистемы.

Горизонтальные подсистемы:

1) подсистема П ПДвЗ (предупреждения доступа злоумышленника в зоны защиты информации), состоящая из объединения следующих блоков: Блок 1/1 ПДВ, Блок 1/2 ПДТ, Блок 1/3 ПДП, Блок 1/4 ПДР, Блок 1/5 ПДБД;

2) подсистема П ПНКвЗ СС2 (предупреждения наличия КНПИ в зоне защиты информации), состоящая из объединения следующих блоков: Блок 2/1 ПНКВ, Блок 2/2 ПНКТ, Блок 2/3 ПНКП, Блок 2/4 ПНКР, Блок 2/5 ПНКБД;

Признаки классификации		Зоны защиты					Подсистемы ЗИ
		1. Внешняя	2. Территории	3. Помещений	4. Ресурсов	5. Базы данных	
Функции защиты информации	1.Предупреждение доступа в зону	Блок 1/1 ПДВ	Блок 1/2 ПДТ	Блок 1/3 ПДП	Блок 1/4 ПДР	Блок 1/5 ПДБД	П ПДвЗ
	2.Предупреждение наличия канала в зоне	Блок 2/1 ПНКВ	Блок 2/2 ПНКТ	Блок 2/3 ПНКП	Блок 2/4 ПНКР	Блок 2/5 ПНКБД	П ПНКвЗ СС2
	3.Предупреждение наличия информации в канале в момент доступа к нему злоумышленника	Блок 3/1 ПНИВ	Блок 3/2 ПНИТ	Блок 3/3 ПНИП	Блок 3/4 ПНИР	Блок 3/5 ПНИБД	П ПНИвК
	4.Локализация НПИ	Блок 4/1 ЛВ	Блок 4/2 ЛТ	Блок 4/3 ЛП	Блок 4/4 ЛР	Блок 4/5 ЛБД	П ЛНПИ
	5.Ликвидация последствий НПИ	Блок 5/1 ЛПВ	Блок 5/2 ЛПТ	Блок 5/3 ЛПП	Блок 5/4 ЛПР	Блок 5/5 ЛПБД	П ЛПНПИ
Подсистемы ЗИ		ПЗ ВЗ	ПЗ ЗТ	ПЗ ЗП	ПЗ ЗР	ПЗ ЗБД	

Рис. 1. Структура и содержание ИСЗИ

3) подсистема П ПНИвК (предупреждения наличия информации в канале в момент доступа к нему злоумышленника), состоящая из объединения следующих блоков: Блок 3/1 ПНИВ, Блок 3/2 ПНИТ, Блок 3/3 ПНИП, Блок 3/4 ПНИР, Блок 3/5 ПНИБД;

4) подсистема П ЛНПИ (локализации НПИ), состоящая из объединения следующих блоков: Блок 4/1 ЛВ, Блок 4/2 ЛТ, Блок 4/3 ЛП, Блок 4/4 ЛР, Блок 4/5 ЛБД;

5) подсистема П ЛПНПИ (ликвидации последствий НПИ), состоящая из объединения следующих блоков: Блок 5/1 ЛПВ, Блок 5/2 ЛПТ, Блок 5/3 ЛПП, Блок 5/4 ЛПР, Блок 5/5 ЛБД.

Вертикальные подсистемы:

6) подсистема ПЗ ВЗ (защиты информации во внешней зоне), состоящая из объединения следующих блоков: Блок 1/1 ПДВ, Блок 2/1 ПНКВ, Блок 3/1 ПНИВ, Блок 4/1 ЛВ, Блок 5/1 ЛПВ;

7) подсистема ПЗ ЗТ (защиты информации в зоне территории объекта), состоящая из объединения следующих блоков: Блок 1/2 ПДТ, Блок 2/2 ПНКТ, Блок 3/2 ПНИТ, Блок 4/2 ЛТ, Блок 5/2 ЛПТ;

8) подсистема ПЗ ЗП (защиты информации в зоне помещений объекта), состоящая из объединения следующих блоков: Блок 1/3 ПДП, Блок 2/3 ПНКП, Блок 3/3 ПНИП, Блок 4/3 ЛП, Блок 5/3 ЛПП;

9) подсистема ПЗ ЗР (защиты информации в зоне ресурсов АСОД), состоящая из объединения следующих блоков: Блок 1/4 ПДР, Блок 2/4 ПНКР, Блок 3/4 ПНИР, Блок 4/4 ЛР, Блок 5/4 ЛПР;

10) подсистема ПЗ ЗБД (защиты информации в зоне базы данных АСОД), состоящая из объединения следующих блоков: Блок 1/5 ПДБД, Блок 2/5 ПНКБД, Блок 3/5 ПНИБД, Блок 4/5 ЛБД, Блок 5/5 ЛПБД.

Где:

Блок 1/1 ПДВ - блок предупреждения доступа злоумышленника во внешней зоне защиты АСОД;

Блок 1/2 ПДТ - блок предупреждения злоумышленника в зону территории АСОД;

Блок 1/3 ПДП - блок предупреждения доступа злоумышленника в зону помещений АСОД;

Блок 1/4 ПДР - блок предупреждения доступа злоумышленника в зону ресурсов АСОД;

Блок 1/5 ПДБД - блок предупреждения доступа злоумышленника в зону базы данных АСОД;

Блок 2/1 ПНКВ – блок предупреждения наличия канала в внешней зоне защиты АСОД;

Блок 2/2 ПНКТ – блок предупреждения наличия канала в зоне территории АСОД;

Блок 2/3 ПНКП – блок предупреждения наличия канала в зоне помещений АСОД;

Блок 2/4 ПНКР – блок предупреждения наличия канала в зоне ресурсов АСОД;

Блок 2/5 ПНКБД – блок предупреждения наличия канала в зоне базы данных АСОД;

Блок 3/1 ПНИВ – блок предупреждения наличия информации в канале в момент доступа к нему злоумышленника во внешней зоне защиты АСОД;

Блок 3/2 ПНИТ – блок предупреждения наличия информации в канале в момент доступа к нему злоумышленника в зоне территории АСОД;

Блок 3/3 ПНИП – блок предупреждения наличия информации в канале в момент доступа к нему злоумышленника в зоне помещений АСОД;

Блок 3/4 ПНИР – блок предупреждения наличия информации в канале в момент доступа к нему злоумышленника в зоне ресурсов АСОД;

Блок 3/5 ПНИБД – блок предупреждения наличия информации в канале в момент доступа к нему злоумышленника в зоне базы данных АСОД;

Блок 4/1 ЛВ – блок локализации НПИ во внешней зоне защиты АСОД;

Блок 4/2 ЛТ – блок локализации НПИ в зоне территории АСОД;

Блок 4/3 ЛП – блок локализации НПИ в зоне помещений АСОД;

Блок 4/4 ЛР – блок локализации НПИ в зоне ресурсов АСОД;

Блок 4/5 ЛБД – блок локализации НПИ в зоне базы данных АСОД;

Блок 5/1 ЛПВ – блок ликвидации последствий НПИ во внешней зоне защиты АСОД;

Блок 5/2 ЛПТ – блок ликвидации последствий НПИ в зоне территории АСОД;

Блок 5/3 ЛПП – блок ликвидации последствий НПИ в зоне территории АСОД;

Блок 5/4 ЛПР – блок ликвидации последствий НПИ в зоне ресурсов АСОД;

Блок 5/5 ЛПБД – блок ликвидации последствий НПИ в зоне базы данных АСОД.

В состав ИСЗИ должны входить следующие технические подсистемы: центр системного мониторинга и оперативного управления; охранной и тревожной сигнализации; противопожарной защиты; контроля и управления доступом; цифрового видеонаблюдения; инженерного обеспечения объекта; безопасности производственных процессов; цифровая подпись; телефонной и радиосвязи связи с компонентами объекта [5,14]. Конкретный состав функциональных блоков ИСЗИ определяется при целевой разработке в соответствии с техническим заданием на разработку АСОД. Состав и количество структурных компонентов ИСЗИ варьируется в зависимости от уровня интеллектуальности системы защиты информации [19], назначения и значимости защищаемого объекта и конкретных условий по интегрированному интеллектуальному обеспечению его безопасности. Одним из основных компонентов является центр защиты информации или центр оперативно-диспетчерского управления защитой информации со своей службой защиты информации. Особенности и характер интеллектуального противоборства злоумышленников и службы защиты информации в АСОД исследованы в работе [20]. Вопросы по разработке алгоритма

принятия решений по оперативно-диспетчерскому управлению средствами защиты информации на основе методов искусственного интеллекта исследованы в работе [21].

Заключение

В данной статье рассмотрен подход по проектированию интеллектуальных систем защиты информации, предназначенных для использования в АСОД с точки зрения функционального подхода. Предложенный подход обеспечивает полноту охвата всех технологических этапов проектирования систем защиты информации, который требует дальнейшей проработки и дополнительных исследований.

Благодарности

Работа поддержана грантом РФФИ 13-01-00544.

Примечания:

1. Федеральный закон Российской Федерации от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании» (принят ГД ФС РФ 15.12.2002) (действующая редакция от 13.07.2015). // http://www.consultant.ru/popular/techreg/. Режим доступа 01.01.2015.
2. ГОСТ Р 1.0-2004. Национальный стандарт Российской Федерации. Стандартизация в Российской Федерации. Основные положения" (утв. Приказом Ростехрегулирования от 30.12.2004 N 152-ст). // http://gostexpert.ru/gost/gost-1.0-2004/. Режим доступа 01.01.2015.
3. Росстандарт (период 1925-2015). // http://www.gost.ru/wps/portal/ Режим доступа 01.01.2015.
4. Национальные стандарты. // http://protect.gost.ru/default.aspx?control=6&month=9&year=2015 &search=&showall=-1&page=5. Режим доступа 01.01.2015.
5. Интегрированные интеллектуальные системы безопасности и мониторинга ситуаций на объектах и территориях. Архитектура и общие технические требования к оборудованию и программным средствам (Проект). // http://secuteck.ru /articles2/inegr_sistemy/edinye-standarty-sozdaniya-integrirovannyh-intellektualnyh-sistem-bezopasnosti-obektov-i-territorii-gosudarstva/. Режим доступа 01.01.2015.
6. ГОСТ Р 52069-2003. Защита информации. Система стандартов. Общие положения.
7. ГОСТ Р 50922-96. Защита информации. Основные термины и определения.
8. ГОСТ Р ИСО/МЭК 15408-1-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.
9. ГОСТ Р ИСО/МЭК 15408-2-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности.
10. ГОСТ Р ИСО/МЭК 15408-3-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности.
11. ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. // http://www.docload.ru/Basesdoc/37/37350/index.htm/. Режим доступа 01.01.2015.
12. ГОСТ Р 51275-99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.
13. ГОСТ Р 51583-00. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения.
14. ГОСТ Р 51624-00. Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования.
15. ГОСТ Р 51188-98 Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство. // http://docs.cntd.ru/document/gost-r-51188-98. Режим доступа 01.01.2015.
16. ГОСТ Р 22.0.07-95 Безопасность в чрезвычайных ситуациях. Источники техногенных чрезвычайных ситуаций. Классификация и номенклатура поражающих факторов и их параметров. // https://polyset.ru/GOST/all-doc/GOST/GOST-R-22-0-07-95/ Режим доступа 01.01.2015.

17. ГОСТ Р 27.003-2011. Надежность в технике. Управление надёжностью. Руководство по заданию технических требований к надежности. // http://protect.gost.ru/ document. aspx?control=7&id=180519. Режим доступа 01.01.2015.

18. Симаворян С.Ж., Симонян А.Р., Улитина Е.И., Симонян Р.А. Системный подход к проектированию интеллектуальных систем защиты информации. // «Известия Сочинского государственного университета», 2013, № 4-2(28), с. 128-132.

19. Simavoryan S.Sy., Simonyan A.R., Ulitina E.I., Simonyan R.A. About one Approach to a Question of Classification of Intellectual System of Information Security. // «Modeling of Artificial Intelligence», 2014, Vol (1), № 1, p. 29-44.

20. Симаворян С.Ж., Симонян А.Р., Улитина Е.И., Симонян А.Р. Исследование интеллектуального противоборства злоумышленников и службы защиты информации в АСОД. // Известия СГУ, 2014, № 4-1 (32). С 15-23.

21. Симаворян С.Ж., Симонян А.Р., Улитина Е.И., Симонян А.Р. Разработка алгоритма принятия решений по оперативно-диспетчерскому управлению средствами защиты информации на основе методов искусственного интеллекта. // «Modeling of Artificial Intelligence», 2015, Vol (5), № 1, p. 33- 41.

22. Симаворян С.Ж., Симонян А.Р., Улитина Е.И., Симонян А.Р. К вопросу о разработке методологии проектирования интеллектуальных систем защиты информации. // Материалы Международной научно-практической конференции «Актуальные задачи математического моделирования и информационных технологий», г. Сочи, 15-24 мая 2015 г./ Соч. гос. ун-т; Сочи, 2015. С. 123-125.

References:

1. Federal'nyi zakon Rossiiskoi Federatsii ot 27 dekabrya 2002 g. № 184-FZ «O tekhnicheskom regulirovanii» (prinyat GD FS RF 15.12.2002) (deistvuyushchaya redaktsiya ot 13.07.2015). // http://www.consultant.ru/popular/techreg/. Rezhim dostupa 01.01.2015.

2. GOST R 1.0-2004. Natsional'nyi standart Rossiiskoi Federatsii. Standartizatsiya v Rossiiskoi Federatsii. Osnovnye polozheniya" (utv. Prikazom Rostekhregulirovaniya ot 30.12.2004 N 152-st). // http://gostexpert.ru/gost/gost-1.0-2004/. Rezhim dostupa 01.01.2015.

3. Rosstandart (period 1925-2015). // http://www.gost.ru/wps/portal/ Rezhim dostupa 01.01.2015.

4. Natsional'nye standarty. // http://protect.gost.ru/default.aspx?control= 6&month =9&year=2015&search=&showall=-1&page=5. Rezhim dostupa 01.01.2015.

5. Integrirovannye intellektual'nye sistemy bezopasnosti i monitoringa situatsii na ob"ektakh i territoriyakh. Arkhitektura i obshchie tekhnicheskie trebovaniya k oborudovaniyu i programmnym sredstvam (Proekt). // http://secuteck.ru /articles2/inegr_sistemy/edinye-standarty-sozdaniya-integrirovannyh-intellektualnyh-sistem-bezopasnosti-obektov-i-territorii-gosudarstva/. Rezhim dostupa 01.01.2015.

6. GOST R 52069-2003. Zashchita informatsii. Sistema standartov. Obshchie polozheniya.

7. GOST R 50922-96. Zashchita informatsii. Osnovnye terminy i opredeleniya.

8. GOST R ISO/MEK 15408-1-2002. Metody i sredstva obespecheniya bezopasnosti. Kriterii otsenki bezopasnosti informatsionnykh tekhnologii. Chast' 1. Vvedenie i obshchaya model'.

9. GOST R ISO/MEK 15408-2-2002. Metody i sredstva obespecheniya bezopasnosti. Kriterii otsenki bezopasnosti informatsionnykh tekhnologii. Chast' 2. Funktsional'nye trebovaniya bezopasnosti.

10. GOST R ISO/MEK 15408-3-2002. Metody i sredstva obespecheniya bezopasnosti. Kriterii otsenki bezopasnosti informatsionnykh tekhnologii. Chast' 3. Trebovaniya doveriya k bezopasnosti.

11. GOST R 50739-95. Sredstva vychislitel'noi tekhniki. Zashchita ot nesanktsionirovannogo dostupa k informatsii. Obshchie tekhnicheskie trebovaniya. // http://www.docload.ru /Basesdoc/37/37350/index.htm/. Rezhim dostupa 01.01.2015.

12. GOST R 51275-99. Zashchita informatsii. Ob"ekt informatizatsii. Faktory, vozdeistvuyushchie na informatsiyu. Obshchie polozheniya.

13. GOST R 51583-00. Zashchita informatsii. Poryadok sozdaniya avtomatizirovannykh sistem v zashchishchennom ispolnenii. Obshchie polozheniya.

14. GOST R 51624-00. Zashchita informatsii. Avtomatizirovannye sistemy v

zashchishchennom ispolnenii. Obshchie trebovaniya.

15. GOST R 51188-98 Zashchita informatsii. Ispytaniya programmnykh sredstv na nalichie komp'yuternykh virusov. Tipovoe rukovodstvo. // http://docs.cntd.ru/document/gost-r-51188-98. Rezhim dostupa 01.01.2015.

16. GOST R 22.0.07-95 Bezopasnost' v chrezvychainykh situatsiyakh. Istochniki tekhnogennykh chrezvychainykh situatsii. Klassifikatsiya i nomenklatura porazhayushchikh faktorov i ikh parametrov. // https://polyset.ru/GOST/all-doc/GOST/GOST-R-22-0-07-95/ Rezhim dostupa 01.01.2015.

17. GOST R 27.003-2011. Nadezhnost' v tekhnike. Upravlenie nadezhnoct'yu. Rukovodstvo po zadaniyu tekhnicheskikh trebovanii k nadezhnosti. // http://protect.gost.ru /document.aspx?control=7&id=180519. Rezhim dostupa 01.01.2015.

18. Simavoryan S.Zh., Simonyan A.R., Ulitina E.I., Simonyan R.A. Sistemnyi podkhod k proektirovaniyu intellektual'nykh sistem zashchity informatsii. // «Izvestiya Sochinskogo gosudarstvennogo universiteta», 2013, № 4-2(28), s. 128-132.

19. Simavoryan S.Sy., Simonyan A.R., Ulitina E.I., Simonyan R.A. About one Approach to a Question of Classification of Intellectual System of Information Security. // «Modeling of Artificial Intelligence», 2014, Vol (1), № 1, p. 29-44.

20. Simavoryan S.Zh., Simonyan A.R., Ulitina E.I., Simonyan A.R. Issledovanie intellektual'nogo protivoborstva zloumyshlennikov i sluzhby zashchity informatsii v ASOD. // Izvestiya SGU, 2014, № 4-1 (32). C 15-23.

21. Simavoryan S.Zh., Simonyan A.R., Ulitina E.I., Simonyan A.R. Razrabotka algoritma prinyatiya reshenii po operativno-dispetcherskomu upravleniyu sredstvami zashchity informatsii na osnove metodov iskusstvennogo intellekta. // «Modeling of Artificial Intelligence», 2015, Vol (5), № 1, p. 33- 41.

22. Simavoryan S.Zh., Simonyan A.R., Ulitina E.I., Simonyan A.R. K voprosu o razrabotke metodologii proektirovaniya intellektual'nykh sistem zashchity informatsii. // Materialy Mezhdunarodnoi nauchno-prakticheskoi konferentsii «Aktual'nye zadachi matematicheskogo modelirovaniya i informatsionnykh tekhnologii», g. Sochi, 15-24 maya 2015 g./ Soch. gos. un-t; Sochi, 2015. S. 123-125.

УДК 004.89

Проектирование интеллектуальных систем защиты информации в автоматизированных системах обработки данных (функциональный подход)

[1] Симон Жоржевич Симаворян
[2] Арсен Рафикович Симонян
[3] Улитина Елена Ивановна
[4] Рафик Арсенович Симонян

[1] Сочинский государственный университет, Российская Федерация
354000, г. Сочи, Краснодарский край, ул. Советская, 26 а
Кандидат технических наук, доцент
E-mail: simsim58@mail.ru
[2] Сочинский государственный университет, Российская Федерация
354000, г. Сочи, Краснодарский край, ул. Советская, 26 а
Кандидат физ-мат. наук, доцент, доцент
E-mail: oppm@mail.ru
[3] Сочинский государственный университет, Российская Федерация
354000, г. Сочи, Краснодарский край, ул. Советская, 26 а
Кандидат физ-мат. наук, доцент
E-mail: ulitinaelena@mail.ru
[4] Кубанский государственный университет, Российская Федерация

350040, г. Краснодар, ул. Ставропольская, 149
Аспирант
E-mail: raf55@list.ru

Аннотация. В работе приведены общие принципы и функциональные требования по проектированию интеллектуальных систем защиты информации, предназначенных для использования в АСОД. В рамках исследования были проанализированы система стандартов и общие положения по защите информации на основе ГОСТ Р 52069-2003 и других. В завершении авторы отмечают, что предложенный подход обеспечивает полноту охвата всех технологических этапов проектирования систем защиты информации, который требует дальнейшей проработки и дополнительных исследований.

Ключевые слова: защита информации, интеллектуальные системы.