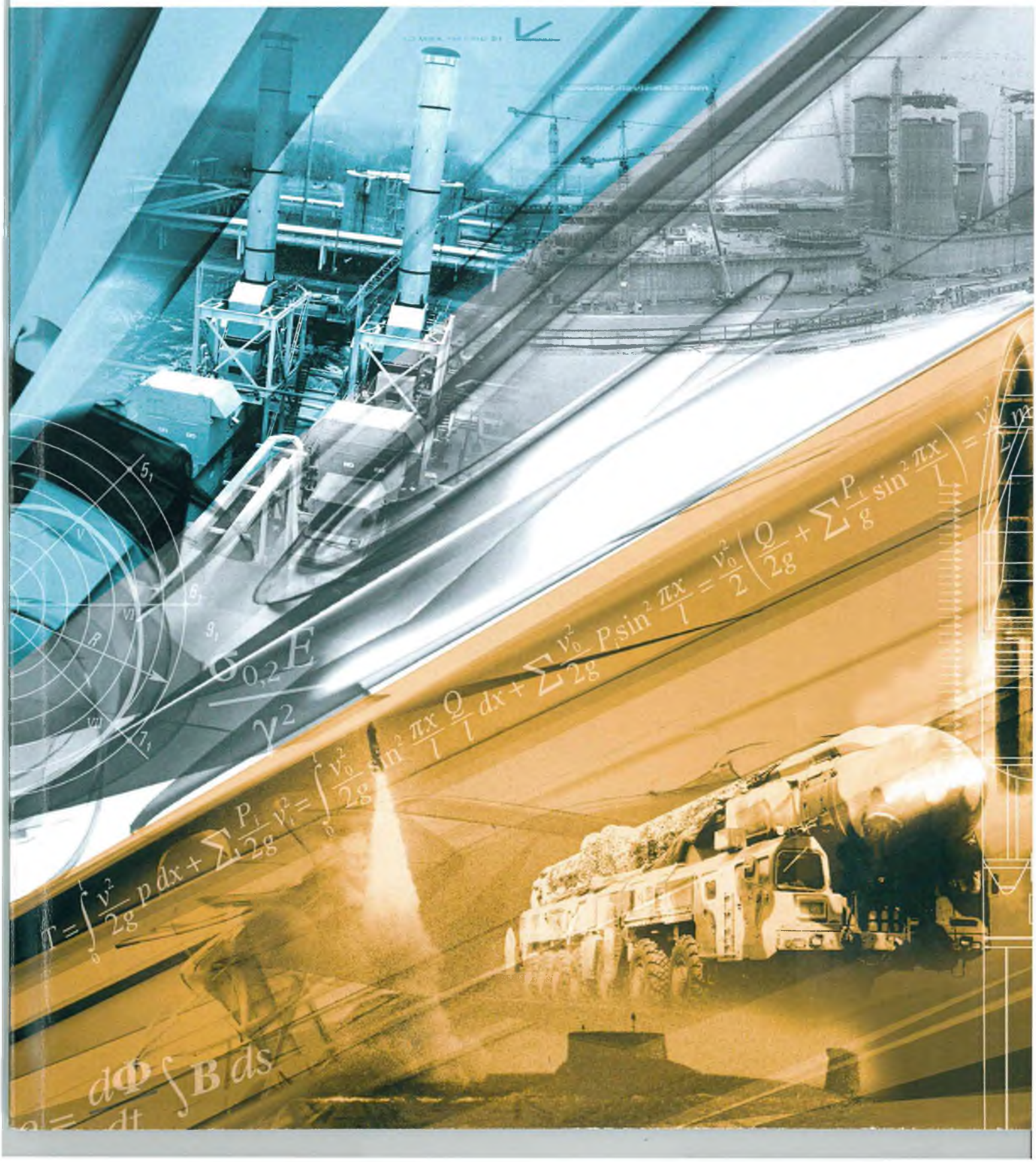
ВОЕННО-ИНЖЕНЕРНАЯ КОРПОРАЦИЯ
РОССИЙСКАЯ ИНЖЕНЕРНАЯ АКАДЕМИЯ
Секция «Инженерные проблемы стабильности и конверсии»

ISSN 1680-2780

Двойные технологии

№ 2
2019



III. ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

Мистров Л.Е., Белоцерковский И.О., Плотников С.Н.
О структурно-параметрическом синтезе информационных систем обеспечения конфликтной устойчивости применения организационно-технических систем..... 72

Полтавский А.В., Федянина В.А.
Алгоритмизация энтропийного анализа символьной информации сетевых вычислительных систем..... 79

Глухов А.П., Василенко В.В., Сидак А.А.
Определение уровней критичности информационных и программно-технических ресурсов объектов критической информационной инфраструктуры железнодорожного транспорта..... 83

Сидак А.А.
Вопросы применения профилей защиты..... 88

Самаров Е.К.
Синтез алгоритма подавления аддитивного шума в изображениях на основе дискретного варианта фильтрации Колмогорова-Винера..... 92

Кулишов А.Р.
Архитектура и принципы организации распределенной адаптивной системы файлового информационного взаимодействия потребителей и центров обработки данных различного целевого назначения..... 95

ДВОЙНЫЕ ТЕХНОЛОГИИ №2 (87) 2019

РОССИЙСКАЯ ИНЖЕНЕРНАЯ АКАДЕМИЯ
СЕКЦИЯ «ИНЖЕНЕРНЫЕ ПРОБЛЕМЫ СТАБИЛЬНОСТИ И КОНВЕРСИИ»

АКЦИОНЕРНОЕ ОБЩЕСТВО
«ВОЕННО–ИНЖЕНЕРНАЯ КОРПОРАЦИЯ»

Издается с сентября 1997 г.
Свидетельство о регистрации
ПИ №77-3609 от 05.06.2000 г.
ISSN 1680-2780

Выходит 4 раза в год

Журнал включен
в «Перечень ведущих периодических изданий» ВАК
и систему РИНЦ

Научно-технический журнал
Наукоемкие технологии, проекты двойного использования комплексов вооружений, техногенная и другие виды безопасностей эксплуатации военных систем, экологический мониторинг.

Группы специальностей: авиационная и ракетно-космическая техника (05.07.00); радиотехника и связь (05.12.00); информатика, вычислительная техника и управление (05.13.00) (технические, физико-математические науки).

СОДЕРЖАНИЕ

I. АВИАЦИОННАЯ И РАКЕТНО-КОСМИЧЕСКАЯ ТЕХНИКА

Ващенко В.И., Чаплинский В.С.
Многопутевые траекторные измерения космических объектов с орбитальным фазированием и синхронизацией..... 3

Данилин С.Б., Знак В.А., Казаков Г.В., Мочалов В.В.
Оценивание решений в задачах поиска оптимальных маневренных стратегий управляемых летательных аппаратов по минимаксному критерию..... 6

Лукин В.Л., Сухорученков Б.И., Окороков М.В., Швед Е.В.
Планирование периода контрольных испытаний технических систем для подтверждения требований к безотказности..... 10

Сафронов С.А.
Метод линейного оценивания, устойчивый к сбоям..... 15

Ермаков В.Ю.
Применение наноматериалов в устройствах ракетно-космической техники..... 20

Захаров Н.С., Корчинский Н.А.
Эрозионная стойкость высокоплотных углеродных материалов при воздействии аэродинамических и лучистых тепловых потоков..... 24

Семячков Д.А.
Использование аналитических методов для оценки температурного поля в многослойных конструкциях..... 31

Сова А.Н., Воробьев Е.В.
Методика и результаты оценки безопасности создания и эксплуатации заправочного оборудования наземных комплексов на основании анализа рисков потенциально опасных ситуаций..... 35

Ерусланкин С.А., Петербургский Н.А.
Результаты анализа характеристикрабочих жидкостей с учетом влияния их свойств на энергоемкость гидротрансформатора..... 39

Герасимчук В.В.
Построение динамической модели конструкции пространственного многозвенного механизма..... 44

Пронин А.Ю., Леонов А.В.
Методический инструментарий оценки готовности изделий высокотехнологичной продукции к промышленному производству..... 48

Теодорович Н.Н., Кручинина С.А., Панасенко Д.В.
Технологии частотного мультеплексирования применительно к системам умного дома..... 53

II. РАДИОТЕХНИКА И СВЯЗЬ

Балабанов В.В., Кузнецов В.В., Никишин В.В., Ткачев А.В.
Методика оценки эффективности подсистемы деструктивного воздействия на системы спутниковой связи..... 57

Кукушкин С.С., Светлов Г.В.
Методы распределенных структурно-алгоритмических преобразований данных, сообщений и цифровых сигналов, ориентированных на различные информационные сечения тракта формирования передаваемой информации..... 60

Драников А.В., Мещеряков В.М.
Способ поиска и устранения ступенчатых изменений систематических погрешностей при обработке измерений по фазе несущей частоты, излучаемой навигационными космическими аппаратами ГЛОНАСС и GPS..... 66

редную формулу

$$H(x,y) = H(x) + H_x(y) = H(y) + H_y(x). \quad (6)$$

Энтропия $H_y(x)$ в ИС характеризует среднюю неопределенность принимаемых сообщений или потерю информации, вызванную наличием ошибок (учитываемые помехи сетевой ИС). При полном отсутствии ошибок передачи сообщения из множества символов вероятность $P(i,j)=0$, тогда

$$H_y(x) = -\sum_{(i,j)} P(i,j)\log_2 P_i(i) = 0$$

и энтропия характеризует, что соблюдается условное «идеальное равновесие» и равенство как $H(x,y)=H(y)=H(x)$. Источники текстовых сообщений, у которых отсутствует коррелятивная связь, называют эргодическими, а выдаваемые ими последовательности (множества) символов называют эргодическими последовательностями. Для эргодического источника сообщений существует конечное число состояний, в которых он может находиться, причем условная вероятность появления очередного символа зависит от того, в каком состоянии находится в этот момент источник. Кроме понятия энтропии на символ текста в ИС имеет место и понятие поток информации – это скорость сообщений как энтропия источника, приходящаяся на единицу времени [1,2,8]

$$H'(x) = \frac{H(x)}{\overline{\tau}}, \quad (7)$$

где $\overline{\tau}$ – средняя длительность символа в секундах.

Заключение

Информатизация образования – это непрерывный управляемый процесс обеспечения системы образования методами и средствами современных информационных технологий. Наблюдаемая эволюция [4–10] применяемых в образовательном процессе различных видов ИС (мониторинговых, фактографических, документальных, экспертных, информационно-аналитических и др.) направлена на широкий охват средств и методов информационного управления. Защита информации в компьютерной сети ИС – это вынужденные меры, направленные против несанкционированного доступа к данным, хранящимся в памяти компьютера. Одним из основных способов защиты данных, хранящихся в сетевых ВС, является использование символов для паролей, которые в итоге имеют цифровой код. Эффективными методами защиты информации в сетевых ВС являются методы, основанные на различных подходах криптографии, они включают комплекс алгоритмов преобразования информации, обеспечивающие скрытность из смыслового содержания данных. К защите информации можно также отнести организацию учета потери информации в процессе ее преобразования и передачи по каналам сетевой ВС. Современные телекоммуникационные и программные средства ИС текстовых переводов с одного языка на другой имеют различный уровень точности [9], т.е. такая работа над «приемлемыми» алгоритмами их идентификации – актуальная проблема информационного обеспечения в достижении желаемого уровня.

Литература

1. Пугачев В.С. Теория случайных функций и ее применение к задачам автоматического управления. М., «Наука», 1962.
2. Шеннон К.Э. Работы по теории информации и кибернетике (с предисловием академика А.Н. Колмогорова). Издательство иностранной литературы, 1963 г. – М.: – С. 824.
3. Полтавский А.В. Программные средства вычислительных систем. Часть I. ЭВМ первых поколений. Учебное пособие. – М.: МГПУ, 2014 – 87 с.
4. Полтавский А.В. Программные средства вычислительных систем. Часть II. ЭВМ третьего и четвертого поколений. Учебное пособие. – М.: МГПУ, 2016 – 96 с.
5. Полтавский А.В. Основы математической обработки информации вычислительных систем. Учебное пособие. – М.: МГПУ, 2017 – 97 с.
6. Полтавский А.В. [и др.]. Устройство для оценки качества обучения работе с компьютером. Патент РФ № 2330323, кл. МПК G06F 17/18- 2008.
7. И.И. Кочегаров, А.В. Полтавский, Н.К. Юрков. Эволюция вычислительных систем. Учебное пособие.– Пенза.: Издательство ПГУ, 2015 – 124 с.
8. Патент на изобретение № 2568272 «Устройство содержательного анализа текстовой информации». Авторы и патентообладатель (ли): Полтавский А.В. [и др.]. Зарегистрирован от 16.10.2015 г.
9. Полтавский А.В., Федянина В.А. Информационная модель случайного процесса // Информационные войны. 2018. №3 (47). С. 98-101.
10. Юрков Н.К., Русяева Е.Ю., Полтавский А.В. Взгляд на теорию алгоритмов с позиций философии. Надежность и качество сложных систем. 2014. № 2 (6). С. 40-45.
11. www.wicipedia.org.
12. www.intuit.ru «Введение в математику».
13. www.intuit.ru/ «Основы сетей передачи данных».
14. www.intuit.ru/ «Работа в программе Microsoft Word XP».
15. www.intuit.ru/ «Работа в программе Microsoft Excel XP».
16. www.intuit.ru/ «Офисное программирование».
17. www.intuit.ru/ «Основы теории вероятности».
18. www.intuit.ru/ «Введение в HTML».
19. www.intuit.ru/ «Основы XML».
20. www.intuit.ru/ «Основы информационной безопасности».

Материал поступил в редакцию 17. 03. 2019 г.

УДК 004.056

© Глухов А.П., Василенко В.В., Сидак А.А.
© Glukhov A., Vasilenko V., Sidak A.

ОПРЕДЕЛЕНИЕ УРОВНЕЙ КРИТИЧНОСТИ ИНФОРМАЦИОННЫХ И ПРОГРАММНО-ТЕХНИЧЕСКИХ РЕСУРСОВ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

DETERMINATION OF CRITICALITY LEVELS OF INFORMATION AND SOFTWARE AND HARDWARE RESOURCES OF CRITICAL INFORMATION INFRASTRUCTURE OBJECT OF RAILROAD TRANSPORT

Аннотация. *Рассмотрены вопросы определения информационных и программно-технических ресурсов корпоративных информационных систем и систем железнодорожной автоматики и телемеханики, а также количественных уровней их критичности для обеспечения безопасности функционирования. Определение уровней критичности информационных и программно-технических ресурсов предложено проводить с использованием метода анализа иерархий, для реализации которого предложены иерархические структуры и определены их основные элементы.*

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 17-20-03048.

Abstract. *The issues of determination of corporate information systems and railroad automatics and telemechanics systems information and software and hardware resources, as well as the quantitative levels of their criticality to ensure the security of operation are considered. It was proposed to determine the criticality levels of information and software and hardware resources of railroad automatics and telemechanics systems using the hierarchy analysis method, for the implementation of which the hierarchical structures are proposed and their main elements were determined.*

The study was carried out with the financial support of the Russian Foundation for Basic Research in the framework of the research project No. 17-20-03048.

Ключевые слова. *Риск-ориентированное управление, информационная безопасность, железнодорожная автоматика и телемеханика, автоматизированная система управления, технологический процесс, информационный ресурс, уровень критичности, метод анализа иерархий.*

Key words. *Risk-oriented management, information security, railroad automation and telemechanics, automated process control system, information resources, level of criticality, hierarchy analysis method.*

Информационная инфраструктура железнодорожного транспорта представляет собой совокупность автоматизированных систем управления производственными и технологическими процессами и обеспечивающих их взаимодействие информационно-телекоммуникационных сетей, а также информационных систем и сетей связи (далее – автоматизированных информационных и телекоммуникационных систем), предназначенных для решения задач управления перевозочным процессом, маркетингом, экономикой и финансами, инфраструктурой железнодорожной транспортной системы, непроизводственной сферой, обеспечением движения поездов и безопасности.

Основной целью управления информационной безопасностью железнодорожного транспорта (ЖТ) является обеспечение гарантированной безопасности информационной инфраструктуры, ее автоматизированных информационно-телекоммуникационных систем (АИТС) и, в первую очередь, объектов критической информационной инфраструктуры ЖТ, к которым могут относиться как корпоративные информационные системы (КИС), так и системы железнодорожной автоматики и телемеханики [1].

Основы управления информационной безопасностью (ИБ) ЖТ базируются на системе принципов, подходов и положений, в число которых входят:

1. Принцип и методология базирования на рисках и обеспечения приемлемого риска, при котором соотношение между проектным риском (риском, оцененным при проектировании), фактическим риском (риском, рассчитанным на этапе функционирования системы, ее эксплуатации) и приемлемым (допустимым) риском и будет определять различные сценарии управления риском ИБ ЖТ.

Глухов Александр Петрович *– доктор технических наук, доцент кафедры «Информатика и информационная безопасность», ФГБОУ ВО «Петербургский государственный университет путей сообщения императора Александра I», e-mail: gala606@rambler.ru;*
Василенко Владимир Васильевич *– доктор технических наук, профессор, заместитель председателя, ООО «Центр безопасности информации», e-mail: v.vasilenko@cbi-info.ru;*
Сидак Алексей Александрович *– кандидат технических наук, старший научный сотрудник, заместитель председателя, ООО «Центр безопасности информации», e-mail: sidak@cbi-info.ru.*

Glukhov Alexander *– doctor of technical sciences, docent of department, PGUPS, e-mail: gala606@rambler.ru.*
Vasilenko Vladimir *– doctor of technical science, professor, deputy chairman, Information Security Center, e-mail: v.vasilenko@cbi-info.ru;*
Sidak Aleksey *– candidate of technical science, senior researcher, deputy chairman, Information Security Center, e-mail: sidak@cbi-info.ru.*

Задача управления информационной безопасностью в этом случае – обеспечить, чтобы проектный и фактический риски были не выше допустимого.

2. Принцип определения и управления критическим ресурсом – основным и чувствительным к воздействиям ресурсом системы – или некоторой совокупностью критических ресурсов, определяющих выполнение функциональной задачи АИТС. Эффективность применения (функционирования) АИТС, то есть достижение системой положительного эффекта, в этом случае связывается с состоянием и поведением (динамикой) критического ресурса под влиянием воздействий (как деструктивно-негативных, разрушающих ресурс, так и воздействий, пополняющих критический ресурс или создающих его резерв) и, прежде всего, с исчерпанием (деградацией) критического ресурса при деструктивных воздействиях. Тогда управление функциональными рисками информационной безопасности АИТС сводится к задаче оценки и управления состоянием критического ресурса в условиях негативных информационных воздействий.

Для каждой конкретной системы АИТС определяется свой наиболее критический ресурс (набор критических ресурсов).

В связи с этим одним из основных этапов анализа рисков ИБ информационной инфраструктуры ЖТ является определение важности (категорирование) АИТС [2] и оценка уровней критичности их информационных, программных, технических и людских ресурсов (активов) АИТС (критичность ресурсов определяется величиной ущерба, наносимого в случае нарушения конфиденциальности, целостности или доступности этого ресурса) [3, 4].

Для оценки уровней критичности (значимости) ресурсов можно использовать следующую последовательность шагов оценки:

1) определение уровней критичности информационных ресурсов;

2) определение уровней критичности программно-технических ресурсов:

- автоматизированных рабочих мест (АРМ);
- сервисов информационных технологий (ИТ-сервисов);
- серверов;
- телекоммуникационного оборудования и др.

Целью определения уровней критичности информационных ресурсов является определение факторов безопасности, оказывающих наибольшее влияние на негативные последствия, отраженные в показателе – обеспечение эффективности процессов, реализуемых с использованием КИС и систем железнодорожной автоматики и телемеханики (ЖАТ).

В качестве метода, который может быть положен в основу решения указанной задачи, предлагается использовать метод анализа иерархий (МАИ) [5], преимущества которого проанализированы и обоснованы в работах [2, 4, 6].

Рассмотрим возможный подход к определению уровней критичности информационных ресурсов КИС и систем ЖАТ КИИ ЖТ с учетом особенностей обеспечения информационной безопасности [1,7,8].

Определение уровней критичности информационных ресурсов корпоративных информационных систем КИИ ЖТ

В состав защищаемых ресурсов КИС КИИ ЖТ в первую очередь входят информационные ресурсы (базы данных, выборки из баз данных, электронные документы, системные файлы, резервные копии), оборудование (АРМ, серверы, телекоммуникационное оборудование) и ИТ-сервисы (программное обеспечение, прежде всего предназначенное для функционирования КИС в части предоставления пользователям ресурсов информационных технологий для обеспечения выполнения ими своих бизнес-функций).

Защищаемые ресурсы для каждой категорированной КИС могут быть определены на основании проектной и эксплуатационной документации, а оценка значимости (критичности) разнотипных защищаемых ресурсов должна проводиться с учетом их взаимодействия в составе АИТС (хранения и обработки информации на конкретных АРМ и серверах, предоставление информации посредством конкретных ИТ-сервисов, реализацию ИТ-сервисов на базе конкретных АРМ, серверов и телекоммуникационного оборудования).

Общий вид иерархии для определения количественных оценок уровней критичности информационных ресурсов КИС КИИ ЖТ представлен на рис. 1.

Рис.1. Общий вид иерархии для определения уровней критичности информационных ресурсов КИС КИИ

В данной иерархии:

1-*й уровень* – показатель – обеспечение эффективности критического процесса, реализуемого с использованием КИС КИИ ЖТ;

2-*й уровень* – КИС, обеспечивающие выполнение критического процесса;

3-*й уровень* – виды информации (ВИ) в КИС КИИ ЖТ;

4-*й уровень* – факторы безопасности (К – конфиденциальность, Ц – целостность, Д – доступность).

Определение уровней критичности информационных ресурсов систем ЖАТ

Под системой железнодорожной автоматики и телемеханики (ЖАТ) понимается совокупность технических средств (ТС), обеспечивающих контроль и управление с установленным уровнем безопасности движения стационарными путевыми и подвижными объектами ЖТ [9].

Под устройствами ЖАТ понимаются ТС автоматизации управления процессами железнодорожных перевозок, обеспечивающие безопасность движения поездов и заданные пропускную и перерабатывающую способности.

В системы ЖАТ входят устройства и системы, обеспечивающие интервальное регулирование движением поездов на станциях и перегонах, такие как:

- автоматическая и полуавтоматическая блокировки;
- электрическая централизация стрелок и светофоров;
- автоматическая локомотивная сигнализация;
- устройства контроля схода подвижного состава;
- диспетчерская централизация и диспетчерский контроль и др.

Возможность выделить в системах ЖАТ информационные, автоматические системы и исполнительные устройства показывает их схожесть со структурой автоматизированных систем управления технологическим процессами (АСУ ТП), имеющей 3 уровня [10]:

- уровень операторского (диспетчерского) управления (верхний уровень);
- уровень автоматического управления (средний уровень);
- уровень ввода (вывода) данных исполнительных устройств (нижний (полевой) уровень).

При этом система ЖАТ может включать:

а) на уровне операторского (диспетчерского) управления: операторские (диспетчерские), инженерные автоматизированные рабочие места, промышленные серверы (SCADA-серверы) с установленным на них общесистемным и прикладным программным обеспечением, телекоммуникационное оборудование (коммутаторы, маршрутизаторы, межсетевые экраны, иное оборудование), а также каналы связи;

б) на уровне автоматического управления: программируемые логические контроллеры, иные ТС с установленным программным обеспечением, получающие данные с нижнего (полевого) уровня, передающие данные на верхний уровень для принятия решения по управлению объектом и (или) процессом и формирующие управляющие команды (управляющую (командную) информацию) для исполнительных устройств, а также промышленная сеть передачи данных;

в) на уровне ввода (вывода) данных (исполнительных устройств): датчики, исполнительные механизмы, иные аппаратные устройства с установленными в них микропрограммами и машинными контроллерами.

Все деструктивные воздействия на системы ЖАТ являются производными трех наиболее общих: нарушение доступности (отказ в обслуживании) критически важной информации; нарушение целостности (модификация) критически важной информации; нарушение конфиденциальности (утечки) критически важной информации. Здесь под критически важной информацией будем понимать закрепленную в документации на систему ЖАТ «технологическую» информацию, уничтожение, блокирование или искажение которой может привести к нарушению функционирования системы ЖАТ, а также информацию «о системе ЖАТ и технологическом процессе», которая в случае ее хищения (ознакомления с ней) может быть непосредственно использована для деструктивных информационных воздействий на систему ЖАТ. Под «технологической» информацией понимается:

- оперативная (динамическая) информация (телеметрия, телеизмерения, телеуправление);
- архивная (статическая) информация (нормативно-техническая документация, параметры и другая архивная информация).

В общем случае в системе поддерживается сегментирование данных и разделение информационных потоков на два параллельных потока:

- поток динамических (оперативных) данных;
- поток статических (архивных) данных.

Поток динамических данных служит для оперативного отображения текущих данных на экранных формах и управления технологическим процессом. При этом выделяются 3 типа переменных:

- выходные переменные, определяющие состояние технологического процесса;
- управляющие воздействия, с помощью которых можно влиять на протекание технологического процесса;
- другие возмущения (контролируемые и неконтролируемые).

Поток динамических данных между различными компьютерами при несанкционированном разрыве связи прекращается. Динамические данные за время отсутствия связи теряются.

Поток статических данных должен поддерживаться средствами системы управления базами данных (СУБД), гарантирующими надежную доставку информации даже при сбоях в линиях связи. Передача потока архивных данных между компьютерами внутри распределенной СУБД должна осуществляться с использованием механизма распределенных транзакций, который обеспечивает возможность продолжения работы при отказах оборудования, отсутствии доступа к серверам, изменении показателей загрузки и производительности различных серверов-участников. Архивные данные за время отсутствия связи накапливаются в исходной базе данных на мастер-компьютере.

Таким образом, критическим информационным ресурсом в системе ЖАТ является «технологическая» ин-

формация (данные) о производственном и (или) технологическом процессе, управляемом (контролируемом) объекте (в том числе данные о параметрах (состоянии) управляемого (контролируемого) объекта или процесса, входная (выходная) информация, команды управления, контрольно-измерительная информация.

Общий вид иерархии для определения уровней критичности информационных ресурсов ЖАТ в соответствии с МАИ представлен на рис. 2.

Рис.2. Общий вид иерархии для определения уровней критичности информационных ресурсов ЖАТ

В данной иерархии:

1-*й уровень* – показатель – обеспечение эффективности технологического процесса, реализуемого с использованием системы ЖАТ;

2-*й уровень* – критерии оценки уровней критичности информационных ресурсов систем ЖАТ;

3-*й уровень* – свойства технологического процесса, определяющие его безопасность;

4-*й уровень* – виды информации в системе ЖАТ;

5-*й уровень* – факторы безопасности (К – конфиденциальность, Ц – целостность, Д – доступность).

В результате применения алгоритма МАИ на основе разработанной иерархии может быть получен вектор приоритетов, каждый элемент которого (после нормирования) можно будет интерпретировать, как уровень влияния фактора безопасности в конкретной системе ЖАТ на последствия, отраженные в значениях показателя обеспечения эффективности системы ЖАТ (для которого построена иерархия).

Таким образом, отработав алгоритм МАИ, можно будет на основе мажоритарного принципа определить уровни критичности информационных ресурсов КИС КИИ ЖТ и систем ЖАТ, что позволит определять соответствующие уровни критичности программно-технических ресурсов, выбирать первоочередные объекты защиты и реализовывать элементы управления ресурсами и рисками ИБ КИИ ЖТ.

Полученные значения уровней критичности информационных и программно-технических ресурсов можно также использовать для эшелонированного и дифференцированного построения систем безопасности объектов КИИ ЖТ, корпоративных сегментов системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (СОПКА) [11] и систем мониторинга информационной безопасности [12] информационной инфраструктуры ЖТ.

Литература

1. Глухов А.П., Ададуров С.Е., Диасамидзе С.В., Корниенко А.А., Сидак А.А. Особенности обеспечения информационной безопасности информационной инфраструктуры железнодорожной транспортной системы // Естественные и технические науки. 2017. № 11. – С. 258-267.

2. Сидак А.А., Корниенко А.А., Глухов А., Диасамидзе С.В. Категорирование и оценка значимости объектов критической информационной инфраструктуры железнодорожного транспорта // Двойные технологии. 2019. № 1. – С. 88-93.

3. Корниенко А.А., Глухов А.П., Диасамидзе С.В. Методика детализированной оценки значимости категорированных объектов критической информационной инфраструктуры железнодорожного транспорта. Труды Седьмой научно-технической конференции «Интеллектуальные системы управления на железнодорожном транспорте. Компьютерное и математическое моделирование» (ИСУЖТ-2018). 2018. – С. 136-139.

4. Сидак А.А. Оценка значимости информации, обрабатываемой в автоматизированных системах, при формировании требований безопасности // Двойные технологии. 2018. № 1. – С. 70-72.

5. Саати Т. Принятие решений. Метод анализа иерерхий. – М.: Радио и связь, 1993. – 312 с.

6. Сидак А.А Применение метода анализа иерархии при определении критических процессов для категорирования объектов критической информационной инфраструктуры Российской Федерации // Информационные войны. 2018. № 2. – С. 79-82.

7. Глухов А.П. Особенности обеспечения информационной безопасности системы организации движения поездов // Транспорт Урала, 2015. № 3. – С. 32-40.

8. Ададуров С.Е., Глухов А.П., Сидак А.А., Рулёв А.С., Петрейко А.В. Реагирование на инциденты информационной безопасности в микропроцессорных системах железнодорожной автоматики и телемеханики // Двойные технологии. 2018. № 2. – С. 76-81.

9. ГОСТ 33894-2016 Система железнодорожной автоматики и телемеханики на железнодорожных станциях. Требования безопасности и методы контроля. – М.: Стандартинформ, 2017. – 26 с.

10. Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды (ред. от 09.08.2018), утв. приказом ФСТЭК России от 14.03.2014 № 31: [Электронный ресурс] // ФСТЭК России, 2019. URL: https://fstec.ru/index?id=868:prikaz-fstek-rossii-ot-14-marta-2014-g-n-31 (Дата обращения: 31.01.2019).

11. Василенко В.В., Сидак А.А Установление требований и синергия системы обнаружения, предупреждения и ликвидации последствий компьютерных атак // Информационные войны. 2019. № 1. – С. 68-72.

12. Аксененко Ю.И., Василенко В.В., Сидак А.А. Методологический подход к построению комплексных систем мониторинга и реагирования на инциденты информационной безопасности // Стратегическая стабильность. 2018. № 1. – С. 64-67.

Материал поступил в редакцию 12. 04. 2019 г.

УДК 004.056

© Сидак А.А.
© Sidak A.

ВОПРОСЫ ПРИМЕНЕНИЯ ПРОФИЛЕЙ ЗАЩИТЫ

USAGE ISSUES OF PROTECTION PROFILES

Аннотация. *В статье освещены вопросы применения в Российской Федерации профилей защиты как формы выражения требований безопасности, предъявляемых к изделиям информационных технологий и автоматизированным системам. Рассмотрены проблемные вопросы, касающиеся данного инструментария, перспективы развития на международном уровне и возможности дальнейшего использования в Российской Федерации. Обосновано применение профилей защиты как формы аксиологического представления для увеличения эквифинальности изделий информационных технологий и снижения энтропии предъявляемых к ним требований безопасности.*

Abstract. *The article highlights the issues of the use of protection profiles in the Russian Federation as a form of expressing security requirements for information technology products and operational systems. The problematic issues relating to this construction, development prospects at the international level and the possibility of further use in the Russian Federation are considered. The use of protection profiles as a form of axiological representation to increase the equifinality of information technology products and reduce the entropy of security requirements imposed on them has been substantiated.*

Ключевые слова. *Профиль защиты, аксиологическое представление, эквифинальность, требование безопасности, пакет требований, семейство профилей защиты, энтропия, каузальное представление.*

Key words. *Protection profile, axiological representation, equifinality, security requirement, requirement package, families of protection profiles, entropy, causal representation.*

При всей неоднозначности отношения в Российской Федерации к профилям защиты, разрабатываемым по ГОСТ Р ИСО/МЭК 15408, они, несомненно сыграли большую роль в развитии нормативных правовых актов и методических документов по защите информации в первые два десятилетия XXI века. Этому способствовало принятие в 2002 г. комплекса стандартов ГОСТ Р ИСО/МЭК 15408, гармонизированных с соответствующими международными стандартами.

Согласно национальному стандарту [1] профиль защиты – это независимое от реализации изложение потребностей в безопасности для некоторого типа изделий информационных технологий (ИТ) или автоматизированных систем (АС). Таким образом, профили защиты делятся на профили защиты для изделий ИТ [1] и профили защиты для автоматизированных систем [2].

В отличие от каузального представления требований безопасности (без употребления понятия «цели») профили защиты являются формой аксиологического (в терминах «целей») представления требований безопасности. В частности, профиль защиты содержит следующую взаимосвязанную информацию об изделии ИТ или АС:

• описание проблемы безопасности в терминах актуальных угроз безопасности информации (БИ), политики безопасности и предположений (ограничений/условий применения);

• изложение целей безопасности, направленных на снижение риска реализации угроз БИ и реализацию политики безопасности;

• функциональные требования безопасности и требования доверия к безопасности, которые направлены на решение изделием ИТ или АС проблемы безопасности и удовлетворение целей безопасности.

В первое десятилетие XXI века профили защиты, как правило, были инициативными разработками. Были разработаны профили защиты для АС железнодорожной отрасли [3], для АС ряда государственных органов власти, профили защиты для некоторых типов изделий ИТ [4]. Некоторые из указанных профилей защиты прошли процедуру сертификации в ФСТЭК России. В то же время эти профили защиты имели локальное применение.

Во втором десятилетии XXI века профили защиты стали активно применяться ФСТЭК России для определения требований безопасности к различным видам и типам изделий ИТ уже в общегосударственном масштабе. В частности, были разработаны профили защиты для следующих видов изделий ИТ: операционных систем, межсетевых экранов, средств антивирусной защиты, средств доверенной загрузки, средств контроля съемных машинных носителей информации, систем обнаружения вторжений. 50 профилей защиты, при разработке которых использовались результаты исследований автора настоящей статьи и ООО «Центр безопасности информации», доступны на сайте ФСТЭК России (https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/120-normativnye-dokumenty).

Сидак Алексей Александрович *– кандидат технических наук, старший научный сотрудник, заместитель председателя, ООО «Центр безопасности информации», e-mail: sidak@cbi-info.ru.*

Sidak Aleksey *– candidate of technical science, senior researcher, deputy chairman, Information Security Center, e-mail: sidak@cbi-info.ru.*

Использование профилей защиты позволило поднять на новый уровень процесс сертификации средств защиты информации по требованиям безопасности информации [5]. На изделие ИТ, подлежащее сертификации, разрабатывалось задание по безопасности (ЗБ) [1] – документ, близкий по структуре профилю защиты. В ЗБ указывалось соответствие одному или нескольким профилям защиты. В отличие от сертификации на технические условия, которые у разных заявителей могли быть абсолютно разными и несопоставимыми, сертификация на ЗБ со ссылкой на утвержденные профили защиты давала исчерпывающее представление о функциональных возможностях безопасности изделия ИТ, о методах и процедурах испытаний, которым оно было подвергнуто.

В профилях защиты требования безопасности в явном виде дифференцированы на следующие виды:

• функциональные требования безопасности (ФТБ), определяющие функциональные возможности безопасности изделия ИТ или АС, направленные на удовлетворение целей безопасности и решение проблемы безопасности;

• требования доверия к безопасности (ТДБ), включающие требования к разработчику (заявителю), требования к документированным материалам для оценки (свидетельствам), требования к действиям по оценке (испытаниям) и определяющие, таким образом, степень уверенности в правильности реализации изделием ИТ или АС функциональных возможностей безопасности.

При разработке профилей защиты ФСТЭК России для задания ФТБ и ТДБ активно использовались шаблоны (компоненты) требований из каталогов ГОСТ Р ИСО/МЭК 15408-2 и ГОСТ Р ИСО/МЭК 15408-3 соответственно. Для выражения необходимых требований безопасности над компонентами выполнялись конкретизирующие операции (назначение, выбор, уточнение). С учетом развития ИТ текущего каталога ГОСТ Р ИСО/МЭК 15408-2 для задания ФТБ в профилях защиты ФСТЭК России было явно недостаточно. Поэтому в профили защиты включались авторские (так называемые «расширенные») компоненты (обозначались как «EXT»). Таких компонентов было много. С учетом накопленного опыта сертификационных испытаний средств защиты информации в России для выражения ТДБ каталогов ГОСТ Р ИСО/МЭК 15408-3 было также недостаточно. Исходя из этого, также активно использовались расширенные компоненты.

Разработка профилей защиты сопровождалась научными исследованиями и разработкой поддерживающих национальных стандартов [4, 6-10].

Фактически совокупность профилей защиты ФСТЭК России для некоторого вида изделий ИТ представляет собой семейство профилей защиты. При разработке документа ФСТЭК России «Руководство по формированию семейств профилей защиты» [11] планировалась некоторая композиционность формирования требований безопасности [8]:

• определялся функциональный пакет (промежуточная конструкция ФТБ) для вида изделий ИТ;

• в рамках вида изделий ИТ выделялись типы;

• для каждого типа изделий ИТ также определялся функциональный пакет;

• для каждого класса защиты изделия ИТ определялся пакет доверия;

• при формировании профиля защиты для конкретного типа изделия ИТ в него включались функциональные пакеты вида и типа изделий ИТ, а также пакет доверия, соответствующий классу защиты изделия ИТ (класс защиты определяется возможностью использования изделия ИТ в АС соответствующего класса защищенности).

С использованием данного подхода в целом и были разработаны профили защиты ФСТЭК России, хотя в явном виде функциональные пакеты не разрабатывались и в профилях защиты не выделялись.

При разработке каждого нового семейства профилей защиты ФСТЭК России совершенствовались (добавлялись расширенные, уточнялись выбранные из ГОСТ Р ИСО/МЭК 15408-3) требования доверия, включаемые в профили защиты, по следующим направлениям:

• реализации (исполнению) изделия ИТ;

• поддержке доверия в процессе эксплуатации изделий ИТ;

• анализу уязвимостей;

• контролю обновления программного обеспечения;

• контролю обновления служебных баз данных изделия ИТ (решающих правил, признаков вирусов);

• требованиям к среде функционирования;

• требованиям к испытанию аппаратной платформы;

• регламентации состава представляемых документированных материалов (свидетельств).

Таким образом, пакеты требований доверия постоянно развивались и адаптировались под потребности сертификации по требованиям безопасности информации. На определенном уровне развития требования доверия были обобщены и изложены единообразно для всех типов изделий ИТ в новом документе ФСТЭК России «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий». В соответствии с информационным сообщением ФСТЭК России [12] эти новые требования применяются взамен ТДБ, включенных в профили защиты.

Заслуживающим внимание направлением развития профилей защиты на международном уровне стало создание международных технических сообществ (iTC), которые разрабатывают так называемые общие (или квалифицированные) профили защиты (cPP).

Также в пересматриваемую редакцию ISO/IEC 15408 включена новая часть стандарта, посвященная пакетам требований безопасности. Существенно расширен каталог функциональных компонентов ISO/IEC 15408-2, в том числе за счет включения расширенных компонентов, впервые определенных в различных профилях защиты и ЗБ. В этих новациях разработки профилей защиты были учтены предложения российской делегации, изложенные на заседании рабочей группы

WG3 «Security evaluation, testing and specification» (РГ 3 «Оценка, тестирование и спецификация безопасности») 27 подкомитета Международной организации по стандартизации (ISO), проходившем в России в 2007 г.

Несмотря на то, что ФСТЭК России с учетом требований [12] в ближайшее время не планируется разработка новых методических документов в форме профилей защиты, инструментарий профилей защиты может применяться как промежуточное представление для научного-технического обоснования требований безопасности к изделиям ИТ, которые в дальнейшем в документах ФСТЭК России могут излагаться в более простом виде по аналогии с руководящими документами 90-х годов XX столетия, но в некоторой более усовершенствованной форме. Данное применение профилей защиты обеспечит корректное использование существующих каталогов требований безопасности, позволит учесть угрозы БИ, взаимосвязи между отдельными ФТБ, охватить все ФТБ действиями по сквозному аудиту событий безопасности и управлению параметрами изделия ИТ. В дальнейшем, являясь основой набора требований безопасности, профиль защиты может использоваться для корректировки данного набора требований, в том числе для демонстрации полноты и взаимной согласованности результирующего набора требований безопасности, предъявляемых к изделиям ИТ.

Требования безопасности должны не только регулировать текущие функциональные возможности изделия ИТ, но и обеспечивать достижение изделием ИТ предельных функциональных возможностей обеспечения безопасности (эквифинальности) в условиях развития изделия ИТ, выпуска обновлений и управления конфигурацией. Требования безопасности, изложенные в произвольном (упрощенном) виде, не позволяют этого достичь в силу следующих причин: с одной стороны, если они максимально конкретны, то не допускают каких-либо изменений в изделии ИТ, с другой стороны, если формулировки требований являются достаточно общими, то их реализация будет обладает большой энтропией, определяемой выражением (1), а сами требования в этом случае нельзя будет считать эффективными

$$H=\log\Omega, \quad (1)$$

где Ω – число сочетаний значений факторов реализации требований безопасности в изделии ИТ или АС, приводящих к соответствию выбранному представлению требований безопасности.

Применение профилей защиты, хотя бы и на промежуточном уровне формирования требований безопасности, позволяет определить в формулировках требований безопасности различные допустимые диапазоны параметров, предполагая, что впоследствии могут быть назначены или выбраны их необходимые значения. Таким образом, с одной стороны, эквифинальность изделия ИТ в жизненном цикле не будет необоснованно ограничена, а с другой стороны, за счет четкой регламентации диапазонов допустимых значений параметров требований и операций по выбору конкретных их значений для изделий ИТ будет максимально снижена энтропия требований безопасности.

Таким образом, дальнейшее применение профилей защиты позволяет увеличить эквифинальность изделий ИТ в жизненном цикле, и в то же время значительно снизить энтропию требований безопасности.

После включения требований к формальному моделированию политик безопасности (компонент ADV_SPM.1 «Формальная модель политики безопасности объекта оценки» из ГОСТ Р ИСО/МЭК 15408-3–2013) в профили защиты для изделий ИТ четвертого класса защиты появился целый ряд публикаций на эту тему, пока ограниченных моделированием политик управления доступом. При этом представление политик безопасности носит преимущественно каузальный характер. Общими недостатками существующих подходов, вне зависимости от используемого математического аппарата и инструментария моделирования, является отсутствие методического обеспечения обоснования соответствия:

- элементов формальной модели неформальным требованиям по управлению доступом;
- реализации в изделии ИТ формальной модели.

Все, что могут предложить авторы публикаций, это некоторое неформальное обоснование. Вместе с тем, профили защиты (с использованием структурированного языка описания ФТБ на основе компонентов ГОСТ Р ИСО/МЭК 15408), как форма аксиологического представления, могут стать тем связующим звеном, которое поможет преодолеть имеющие недостатки обоснования соответствия.

Применение концепции профилей защиты также имеет определенные перспективы и для АС. В работах [13, 14] в явном виде изложены требования по учету актуальных угроз безопасности информации, прежде всего, на основе Банка данных угроз безопасности информации, поддерживаемого ФСТЭК России. Также при формировании требований безопасности необходим учет структурно-функциональных характеристик автоматизированных систем [13]. При этом структура профиля защиты является подходящей для сопоставления результирующих требований безопасности с характеристиками АС и среды функционирования, а также с угрозами безопасности информации.

Литература

1. ГОСТ Р ИСО/МЭК 15408-1 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. М.: Стандартинформ, 2014.

2. ГОСТ Р ИСО/МЭК ТО 19791-2008-2008 Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем. М.: Стандартинформ, 2010.

3. Корниенко А.А., Глухов А.П., Диасамидзе С.В., Сидак А.А. Профили защиты и задания по безопасности корпоративных информационных систем и сетей железнодорожного транспорта: учебное пособие. СПб.: Петербургский государственный университет путей сообщения Императора Александра I, 2014. – 94 с.

4. Бетелин В.Б., Галатенко В.А., Кобзарь М.Т., Сидак А.А., Трифаленков И.А. Обзор профилей защиты, построенных на основе «Общих критериев». Специфические требования к сервисам безопасности // Безопасность информационных технологий. 2003. № 3, С. 30.

5. Сидак А.А. Особенности сертификации продуктов и ИТ-систем на основе Общих критериев // Защита информации. Инсайд 2005. № 4. – С. 51-53.

6. Трубачев А.П., Егоркин И.В., Кобзарь М.Т., Сидак А.А. Общие критерии оценки безопасности информационных технологий // Защита информации. Конфидент. 2002. № 2. – С. 54-59.

7. Кобзарь М.Т., Сидак А.А. О Руководстве по разработке профилей защиты на основе Общих критериев// Jet Info. 2000. №2. – С. 18-20.

8. Сидак А.А. Композиционный подход к формированию требований к изделиям, реализующим функции безопасности в информационных системах. Семейства профилей защиты// Стратегическая стабильность. 2013. № 3. – С. 40-42.

9. Сидак А.А. Обоснование требований по защите информации в автоматизированных системах // Стратегическая стабильность. 2009. № 4. – С. 7-9.

10. ГОСТ Р 57628-2017 Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности. М.: Стандартинформ, 2017.

11. Руководящий документ. Безопасность информационных технологий. Руководство по формированию семейств профилей защиты. Гостехкомиссия России, 2003: [Электронный ресурс] // ФСТЭК России, 2019. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/120-normativnye-dokumenty/401-rukovodyashchij-dokument-gostekhkomissiya-rossii-2003-god2 (Дата обращения: 31.03.2019).

12. Информационное сообщение ФСТЭК России от 29 марта 2019 г. № 240/24/1525 «О требованиях по безопасности информации, устанавливающих уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий»: [Электронный ресурс] // ФСТЭК России, 2019. URL: https://fstec.ru/normotvorcheskaya/informatsionnye-i-analiticheskie-materialy/1812-informatsionnoe-soobshchenie-fstek-rossii-ot-29-marta-2019-g-n-240-24-1525 (Дата обращения: 07.04.2019).

13. Приказ ФСТЭК России от 11.02.2013 № 17 (ред. от 15.02.2017) «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», зарегистрирован в Минюсте России 31.05.2013 г. №28608 // СПС КонсультантПлюс.

14. Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации», зарегистрирован в Минюсте России 26.03.2018 г. №50524 // СПС КонсультантПлюс.

Материал поступил в редакцию 12. 04. 2019 г.