Таким образом, в работе определены понятия контекста, операции контекстного уточнения смысла, контекстной связки. Рассмотрена операция контекстного уточнения смысла, которая определяется на множестве смысловых значений главного слова контекстной связки, и показано, что данная операция является несимметричной. Также рассмотрены свойства и особенностей операции контекстного уточнения смысла и построено обобщенное выражение для вычисления функционала смысловыразительности контекстной связки. Теоретические построения проиллюстрированы примером.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Тестелец Я.Г.* Введение в общий синтаксис: Учебное пособие. – М.: Изд-во Российского гуманитарного университета, 2001. – 830 с.
2. *Вишняков Ю.М., Вишняков Р.Ю.* Проблемы семантического информационного поиска // Труды международных научно-технических конференций «Интеллектуальные системы» (AIS'06) и «Интеллектуальные САПР» (CAD-2006). Научное издание в 3-х томах. Т. 2. – М.: Физматлит, 2006. – С. 308-314.
3. *Вишняков Р.Ю.* Контекстное уточнение смысла слов в связанном текстовом фрагменте. // Сборник трудов Всероссийской научной школы-семинар молодых ученых, аспирантов и студентов «Семантическая интерпретация и интеллектуальная обработка текстов, их приложения в информационном поиске, хранении и обработке документов в электронных архивах и библиотеках». – Таганрог: Изд-во ТТИ ЮФУ, 2012. – С. 112-116.

Статью рекомендовал к опубликованию д.т.н., профессор В.П. Карелин.

Вишняков Ренат Юрьевич – Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Южный федеральный университет»; e-mail: rvishn.sfu.edu@gmail.com; 347928, г. Таганрог, пер. Некрасовский, 44; тел.: +78634314485; кафедра системного анализа и телекоммуникаций; ассистент.

Вишняков Юрий Муссович – e-mail: vishn@tsure.ru; факультет автоматики и вычислительной техники; декан.

Vishnyakov Renat Yur'evich – Federal State-Owned Autonomy Educational Establishment of Higher Vocational Education "Southern Federal University"; e-mail: rvishn.sfu.edu@gmail.com; 44, Nekrasovskiy, Taganrog, 347928, Russia; phone: +78634314485; the department of system analysis and telecommunication; assistant.

Vishnyakov Yurij Mussovich – e-mail: vishn@tsure.ru; the college of automation and computer engineering; dean.

УДК 004.732.056(075.8)

А.Е. Васильев, О.П. Третьяков

ГРАФОВАЯ МОДЕЛЬ КОНТРОЛЯ И АНАЛИЗА СОСТОЯНИЯ ЗАЩИТЫ ИНФОРМАЦИИ*

Рассматривается многоуровневая графовая модель для контроля и анализа состояния защиты информации. Для решения задачи, контроль предлагается проводить по точкам контроля, которые представляют собой возможные существующие недостатки по проверяемому направлению и имеют между собой определенную взаимосвязь и при выявлении уязвимости защиты информации, позволит быстро определить направления ее распространения.

* Работа выполнена при финансовой поддержке РФФИ (проект № 12-01-00474).

Предполагается, что результаты позволят уменьшить временные затраты на осуществление контроля защиты информации и повысит качество проводимых проверок, при ограниченном количестве контролирующих лиц.

Точки контроля; реперные точки контроля; весовые коэффициенты; уязвимости.

A.E. Vasilyev, O.P. Tretyakov

GRAPH MODEL MONITORING AND ANALYSIS OF DATA PROTECTION

We consider a multi-level graph model to monitor and analyze the state of information security. To solve the problem, proposed to take control of the points of control, which is a possible existing deficiencies on the checked direction and have a definite correlation between the detection of vulnerability and protection of information, you can quickly identify areas of its distribution.

It is assumed that the results will reduce the time spent on control of information security and improve the quality of audits, with a limited number of supervisors.

Point of control; the reference points of control; weights; vulnerability.

Введение. С развитием информационного общества все большее значение приобретают проблемы, связанные с защитой информации (ЗИ).

Защита информации является неотъемлемой составной частью общей проблемы информационной безопасности, роль и значимость которой во всех сферах жизни и деятельности общества и государства на современном этапе неуклонно возрастают.

В связи с этим, проблема защиты информации стала предметом острой озабоченности руководителей органов государственной власти, предприятий, организаций и учреждений независимо от их организационно-правовых форм и форм собственности.

Анализ положения дел в области информатизации и информационной безопасности позволяет сделать следующие выводы [1]:

1. В настоящее время одним из главных стратегических национальных ресурсов, основой экономической и оборонной мощи государства становятся информация и информационные технологии.
2. Информация в современном мире является таким атрибутом, от которого в решающей степени зависит эффективность жизнедеятельности современного общества.
3. Информационные технологии принципиально изменили объём и важность информации, обращающейся в технических средствах её хранения, обработки и передачи.
4. Всеобщая компьютеризация основных сфер деятельности привела к появлению широкого спектра внутренних и внешних угроз, нетрадиционных каналов утечки информации и несанкционированного доступа к ней.
5. Массовое оснащение государственных учреждений, предприятий, организаций и частных лиц средствами вычислительной техники и включение их в мировое информационное пространство таит в себе реальную угрозу создания разветвлённых систем регулярного несанкционированного контроля за информационными процессами и ресурсами, злоумышленного вмешательства в них.

Анализ контроля состояния защиты информации. В настоящее время объемы задач, стоящие перед службой безопасности отдельно взятой организации, постоянно растут, вопросы контроля состояния ЗИ, как никогда актуальны. Однако, как показывает практика, времени для выполнения поставленных задач контроля защиты информации штатной категорией в 1–2 человека, при наличии большого числа подчиненных филиалов, недостаточно.

Доктрина информационной безопасности РФ определяет, что одним из основных направлений научных исследований и технических разработок по совершенствованию системы ЗИ, является совершенствование системы контроля, анализа и оценки эффективности защиты информации, что определяет **актуальность** необходимости автоматизации данного процесса.

Одним из элементов эффективной работы системы ЗИ, является действенный и систематический контроль, что ведет к необходимости совершенствования системы контроля состояния ЗИ в рамках отведенного бюджета времени.

В настоящее время контроль системы ЗИ осуществляется статистическим методом, т.е., организуется сбор информации за определенный период о состоянии ЗИ. Затем проводится изучение результатов контроля и оценка состояния ЗИ [1], как отдельно по филиалам, так и, в общем, за организацию.

Типовая организация включает порядка 12–15 филиалов, в каждом из которых обрабатывается информация, подлежащая защите и организованы подсистемы ЗИ. Контроль данных подсистем осуществляет служба безопасности информации организации, имеющая в штате 1–2 сотрудников.

Для осуществления контроля состояния защиты информации [2] в филиалах, бюджет времени, выделяемый руководством организации, как правило, составляет 8–16 часов в год (1–2 рабочих дня с учетом времени прибытия и убытия).

Существующая практика показывает, что для действенного контроля состояния ЗИ необходимо порядка 24 часов (3 рабочих дней).

Таким образом, недостаток временного ресурса отрицательно сказывается на полноте и соответственно качестве проводимых проверок. В результате чего имеющие место нарушения в области ЗИ, вскрываются не в полной мере и, способствуют утечке защищаемой информации.

Исходя из данных фактов, возникает вопрос, каким образом организовать работу по проверке состояния ЗИ, чтобы система работала эффективно и без нарушений?

Анализировать состояние ЗИ следует по различным направлениям $\{H_{1,..} H_n\}$ в качестве которых могут быть, например, пропускная система, ведение конфиденциального документооборота и другие. Условно их можно выделить порядка 7–8. Для анализа [3] каждого направления деятельности предлагается определить точки контроля (ТК), в которые предполагается отобразить возможные недостатки, образующие, так называемые, «бреши» в защите информационных ресурсов организации (филиала), наличие которых, создает предпосылки для реализации угроз безопасности защищаемой информации.

Графовая модель контроля и анализа защиты информации. Для реализации контроля и анализа состояния ЗИ, построим многоуровневую графовую модель состояний, вершинами которой являются точки контроля (ТК), а ребрами – связи между ними. Точки контроля будут размещаться условно на трех уровнях (Z_1 Z_2 Z_3), которые соответствуют категории нарушений (1, 2, 3) проверяемого вопроса в данной ТК.

Наиболее критичные состояния информационных ресурсов (наиболее важные проверяемые вопросы) определим, как реперные точки контроля (РТК). Реперная точка контроля – точка, имеющая наибольшее количество взаимных связей с другими ТК, и при положительном результате проверки которой, существенно снижается вероятность наличия недостатка в смежных точках. При отрицательном же результате, соответственно, увеличивается вероятность наличия недостатка в смежных проверяемых точках.

Точки контроля и реперные точки контроля размещены в графе на трех различных уровнях, они представляют собой возможные существующие недостатки по каждому направлению, список которых формируется изначально, и каждому недостатку, присваивается весовой коэффициент [4] по категории нарушений, путем проведения экспертных оценок.

Корнями графа являются сформулированные направления анализа состояния ЗИ $\{H_1, H_2, \ldots, H_n\}$ (рис. 1).

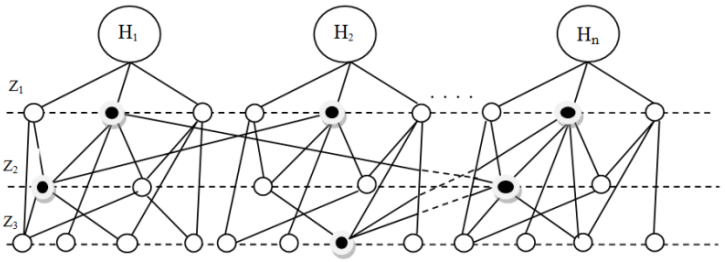

Рис. 1. Граф состояния защиты информации

На графе обозначены:

- вершины ○ – точки контроля (ТК) (возможные недостатки);
- вершины ● – реперные точки контроля (наиболее критичные состояния информационных ресурсов);
- корни графа (H1) – направления проверки;
- уровни Z – места размещения ТК и РТК.

Предполагается, что все точки контроля находятся на трех уровнях и будут соответствовать одной из трех категорий нарушений. Наличие определенного количества точек контроля и реперных точек контроля (недостатков) соответствующей категории, в свою очередь будет отнесено определенной оценке состояния защиты информации (табл. 1).

Таблица 1

Оценка по проверке	Категория оценок (количество недостатков)		
	1 категория	2 категория	3 категория
5 – соответствует	-	-	5
4 – в основном соответствует	-	-	15
3 – не в полной мере соответствует	-	1	20
2 – не соответствует	1	2	30

Заключение. Таким образом, на основе проведенного анализа сформулированы выводы в области информатизации и информационной безопасности о необходимости автоматизации контроля и анализа состояния защиты информации в организациях (филиалах). Проведен анализ существующей системы состояния контроля и анализа ЗИ, определены основные недостатки.

Предложена графовая модель контроля и анализа состояния защиты информации в организациях и их филиалах, которая позволит автоматизировать процесс осуществления контроля и анализа ЗИ, сократить сроки проводимых проверок и прогнозировать в дальнейшем состояние защиты информации в целом.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1 *Домарев В.В.* Безопасность информационных технологий. Методология создания систем защиты информации. – 2008. – С. 508-525. Электронный ресурс:URL: http://domarev.com.ua/d-book-2/ch_25.pdf (дата обращения: 05.08.2013).
2 *Чумаков А.А.* Разработка и оптимизация региональной подсистемы технического контроля в интересах обеспечения информационной безопасности. – Воронеж: 5 ЦНИИИ МО РФ, 1999.
3 *Царегородцев А.В., Петручук С.О.* Анализ функций защиты для проектирования платформ безопасности: Электронный ресурс: URL: http://nit.miem. edu.ru/2003/tezisy/articles/129.htm, (дата обращения: 28.05.2013).
4 *Коробов В.Б.* Организация проведения экспертных опросов при разработке классификационных моделей // Социологические исследования. – 2003. – № 11. – С. 102-108.

Статью рекомендовал к опубликованию д.т.н., профессор Ю.О. Чернышев.

Васильев Андрей Евгеньевич – Военная академия связи (филиал г. Краснодар); e-mail: vasandevg@mail.ru; 350035, г. Краснодар, ул. Красина, 4; тел.: 89182480113; преподаватель кафедры; соискатель.

Третьяков Олег Павлович – e-mail: tretoleg3@mail.ru; тел.: 89181939073; начальник кафедры; к.т.н.

Vasilyev Andrey Evgenevich – Military Academy of Telecommunications (branch Krasnodar); e-mail: vasandevg@mail.ru; 4, Krasina street, Krasnodar, 350035, Russia; phone: +79182480113; teacher of the department; applicant.

Tretyakov Oleg Pavlovich – e-mail: tretoleg3@mail.ru; phone: +79181939073; head of department; cand. of eng. sc.

УДК 523.985.3

И.А. Скороходов, С.В. Тасенко, П.В. Шатов, И.В. Гецелев, М.В. Подзолко

УЧЕТ ВЛИЯНИЯ ГЕОМАГНИТНЫХ БУРЬ ПРИ ПРОЕКТИРОВАНИИ РАЗЛИЧНЫХ СИСТЕМ

В настоящее время большое внимание уделяется влиянию на надежность различных систем. Геомагнитные бури оказывают значительное влияние на многие системы, как на Земле, так и в околоземном космическом пространстве. Поэтому весьма важно учесть эти влияния при проектировании различных систем. Наиболее эффективным и оперативным предвестником магнитной бури является приход частиц солнечных протонных событий (СПС). Для прогноза СПС нами была создана база данных, состоящая из ≈400 событий за 19–24 циклы солнечной активности.

Анализ данных выявил существенную неравномерность распределения источников СПС по долготе Кэррингтона. Особого внимания заслуживает интервал «пассивных долгот», протяженный по долготе (≈90–170°).

Геомагнитная буря; солнечное протонное событие; долгота Кэррингтона; пассивные долготы.

I.A. Skorohodov, S.V. Tasenko, P.V. Shatov, I.V. Getselev, M.V. Podzolko

ACCOUNTING FOR THE EFFECTS OF GEOMAGNETIC STORMS IN DESIGNING THE VARIOUS SYSTEMS

At present great attention is paid to influence the reliability of the various systems. Geomagnetic storms have a significant impact on many systems, both on Earth and in outer space. Therefore, it is very important to consider these effects in designing the various systems. The most