Раздел II. Защита информационных процессов в компьютерных системах

УДК 681.322

Чл.-корр. РАН Ю.В. Бородакий,
А.Ю. Добродеев, Б.П. Пальчун, М.Н. Болдина

ИНСАЙДЕРОЛОГИЯ – НАУКА О НЕЛЕГИТИМНОСТИ В КОМПЬЮТЕРНОЙ ИНФОСФЕРЕ

В настоящее время одним из основных условий существования человечества является развитость техносферы нашей цивилизации, основу которой составляют высокотехнологичные производства и системы. Это обстоятельство является источником одной из основных коллизий современности, с одной стороны, высокие технологии обеспечивают жизнедеятельность человечества и его прогрессивное и комфортное развитие, с другой стороны, являются источником техногенных катастроф, угрожающих не только безопасности человеческой цивилизации, но и самому её существованию [1].

Основные проблемы глобального масштаба возникают при эксплуатации и обеспечении безопасности так называемых критических систем, к которым относятся энергетические системы (особенно атомные), транспортные системы, системы связи, военно-технические системы, финансовые системы, медицинская и биологическая промышленность, экологически опасные производства, системы управления государством, в особенности силовыми структурами, и ряд других.

Такие критические системы, несмотря на явные различия, имеют в наше время одну общую для всех особенность – все они имеют системы управления с использованием компьютерной обработки информации. То есть, безопасность самих критических систем непосредственным образом зависит от цифровых электронных вычислительных машин со всем их содержимым и в первую очередь от совокупности общих и специальных программных средств создания, обработки и хранения компьютерных данных, и собственно компьютеризированных данных на любых типах носителей информации, от всего того, что сейчас принято называть «компьютерной инфосферой» [2].

Именно состояние компьютерной инфосферы критических систем (которые можно в этом случае называть также критическими объектами информатизации) определяет все позитивные и негативные составляющие функционирования этих систем. Кроме того, в настоящее время существует большое количество факторов угроз безопасности самой компьютерной инфосферы, которые подробно расписаны в Доктрине информационной безопасности Российской Федерации.

Таким образом, реально существует ещё одна глобальная коллизия современности – с одной стороны, без компьютеризации (без компьютерной инфосферы и её развития) не возможен прогресс человечества в сфере высоких технологий, с другой – компьютерная инфосфера представляет собой неиссякаемый источник угроз техносфере цивилизации и, в принципе, самой цивилизации тоже.

Как уже указывалось все современные системы критических приложений, как правило, компьютеризированы и имеют соответствующее программное обеспечение, а более точно – компьютерные программы (КП) и базы данных (БД). Компьютерная инфосфера критических систем – это совокупность КП и БД всех сущест-

вующих ЭВМ (универсальных, специализированных, встроенных, персональных, супер-ЭВМ и микропроцессоров), влияющая на обеспечение безопасности систем критических приложений и на обеспечение жизнеспособности страны в целом [1,2].

В связи с этим, важно обеспечивать безопасность самой компьютерной инфосферы. Для решения этой проблемы существует достаточно развитой нормативно-правовой базис: Доктрина информационной безопасности Российской Федерации (Пр-№ 1895 от 9 сентября 2000 года), Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», руководящие документы ФСБ России и ФСТЭК России. На данную тему проведены многочисленные научные исследования, и накоплен большой практический опыт по защите информации в различных конкретных компьютерных инфосферах.

Следует отметить, что в области информационной безопасности наибольшее внимание организации уделяют, как правило, защите от внешних атак, поэтому почти все средства, выделяемые на обеспечение безопасности, направляются на защиту уязвимых точек периметра сети предприятия. Сложившаяся ситуация нашла соответствующее отражение и на рынке решений ИТ-безопасности – в последние годы предлагается широкий спектр различных средств защиты от вирусов, червей, троянцев и прочих угроз извне. Однако постепенно владельцы объектов информатизации начинают осознавать новую опасность. Она исходит не от хакеров, не от спама или случайных вирусов, а от собственных сотрудников так называемых инсайдеров. Этот термин давно используется в экономике (точнее, в экономической безопасности): инсайдер (от англ. *inside* – внутри) – любое лицо, имеющее доступ к конфиденциальной информации о делах фирмы благодаря своему служебному положению и родственным связям. Понятно, раз инсайдеры находятся внутри самой организации и наделены вполне легальными полномочиями, то им гораздо проще получить доступ к интересующей их информации, чем любому злоумышленнику со стороны, то есть легитимные фигуранты наиболее эффективно могут заниматься нелегитимными действиями.

В настоящее время этой проблеме посвящено уже много публикаций, в частности, в КомпьютерПресс (А. Доля, В. Ульянов, О. Зайцев, В. Ершов и др.) [3-9]. Имеется в данной области даже специализированная компания InfoWatch. Аналитики этой компании в результате проведенного исследования (в котором приняли участие представители 315 отечественных коммерческих и государственных организаций) сделали следующие основные выводы [3]:

- российские компании и организации озабочены проблемами внутренних угроз ИТ-безопасности намного больше, чем внешними атаками. При этом самыми опасными инсайдерскими угрозами являются кража конфиденциальной информации и халатность сотрудников;
- все 100% респондентов согласились с тем, что нарушение конфиденциальности информации является важнейшей внутренней угрозой;
- несмотря на высокую степень озабоченности данной проблемой, российские организации все еще затрудняются в оценке масштабов и последствий утечки конфиденциальных данных: подавляющее большинство (96%) либо регистрировали реальные утечки, либо допускают их существование, однако ни одна компания не оценивала свой ущерб в результате такого инцидента;
- сегодня лишь 2% респондентов используют решения для выявления и предотвращения утечек, и 83% организаций планируют их внедрение в течение последующих 3 лет;

- в целом по профессиональному подходу к обеспечению ИТ-безопасности Россия опережает средний общемировой уровень: около 40% отечественных организаций имеют выделенные отделы или специальных сотрудников в сфере ИТ-безопасности, тогда как общемировой показатель составляет в этом случае 27%.

Но, несмотря на такое большое внимание к проблеме инсайдерства на наш взгляд данная проблема всё же значительно зауживается. Так, по усреднённому мнению зарубежных и отечественных специалистов (рис. 1) наиболее опасными угрозами сегодня являются кража информации инсайдерами (64%), вредоносные программы (49%), хакерские атаки (48%), спам (45%) и халатность сотрудников (43%) [4-7].

Рис. 1. Усредненные долевые угрозы компьютерной инфосфере

Хотя здесь на первое место поставлена инсайдерская угроза, на самом деле инсайдерский фактор существенно более весомый, так как он влияет фактически на все вышеприведённые угрозы, кроме разве что спама. Эффективные вредоносные программы невозможно создать без инсайдеров, поскольку такие программы должны быть исключительно целенаправленными, учитывающими эксклюзивные «тонкости» поражаемых фрагментов компьютерной инфосферы (как КП, так и БД) конкретного объекта информатизации. Практически все успешные и широко известные хакерские атаки были осуществлены с участием инсайдеров, обвиняемые в этих атаках студенты-хакеры – это либо элемент исполнительного механизма операции, проводимой по «наводке» инсайдеров, либо маскирующее «прикрытие» этой операции. Что же касается халатности сотрудников, то эта халатность является, с одной стороны, благоприятной средой как для эффективной деятельности инсайдеров, с другой – весьма благоприятной базой для вербовки инсайдеров, а также появления инсайдеров-инициативников. А при введении термина «инсайдер по неосторожности» (что вполне логично, так как недобросовестный сотрудник зачастую хуже врага, особенно для важных систем критического применения), этот фактор фактически целиком будет иметь инсайдерский характер. И даже спам, который имеет внешнее происхождение, может быть использован для обеспечения инсайдерской деятельности, например, для маскировки инсайдерских устремлений.

Таким образом, практически все угрозы безопасности компьютерной инфосферы критических систем при их эксплуатации осуществляются с участием инсайдеров, под которыми понимаются нелегитимные (как преднамеренные, так и

случайные) действия собственных сотрудников организации. Но и это ещё не всё, так как следует учесть, что кроме проблемы обеспечения эксплутационной безопасности компьютерной инфосферы, существует ещё более сложная проблема обеспечения технологической безопасности компьютерной инфосферы, т.е. обеспечение безопасности и надёжности КП (и, естественно, БД) на стадии их разработки.

Сложилось так, что главная угроза безопасности компьютерной инфосферы, вызванная действиями самих разработчиков КП, фактически маскируется под угрозу компьютерного «хулиганства», как более наглядную и внешне эффективную (принося при этом действительно большой вред, особенно компьютерной ширпотребной продукции). Но для компьютерной инфосферы систем критических приложений, в особенности оборонных, по утверждению «US News and World Report» (31.10.1983 г.), «угрозу значительно большую, нежели подростки-программисты, представляют свои же служащие» [10].

В связи с этим необходимо построение единой концепции обеспечения безопасности компьютерной инфосферы, включающей в себя как этап разработки КП (технологическая безопасность КП), так и этап ее эксплуатации (эксплутационная безопасность КП). В целом, признавая важность проблемы защиты компьютерной инфосферы на этапе эксплуатации, отметим, что внедрить на этом этапе вирус, изменяющий семантику КП практически невозможно. В то же время обеспечить такой семантический разрыв в КП на этапе разработки вполне реально, и сделать это может один из разработчиков КП. Так, в немецкой научно-технической литературе приведены примеры ошибок программирования, большинство из которых целенаправленно создается программистами в результате актов саботажа или для собственной выгоды. При этом для сокрытия этих диверсионных программных закладок затрачиваются большие интеллектуальные усилия. Сенаторы США не доверяют полностью высококомпьютеризованной библиотеке Конгресса и самые важные сведения записывают по старинке в обычные записные книжки, а не в специально выделенные личные и «глубоко защищенные» базы данных.

Анализ всех этих фактов свидетельствует о достаточно реальных возможностях преднамеренного ввода программных дефектов и компьютерных вирусов в КП средств управления систем критических приложений (АЭС, экологически опасные производства, космические аппараты, самолёты и т.п.) как на этапе сборки и отладки, так и в процессе эксплуатации. При этом можно заранее предусмотреть желаемое нарушение в работе аппаратных средств за счет ввода вируса, а сам вирус можно замаскировать под обычную непреднамеренную ошибку программирования [11].

Наряду с таким экстраординарным методом внедрения прорабатываются и другие, более эффективные способы поражения КП, например, путем проникновения на этапе производства. Учитывая характер и перспективность всех этих работ, в зарубежных странах предпринимаются меры по конфиденциализации масштабов исследований и их результатов. Тем не менее по результатам анализа имеющейся информации можно констатировать, что в основе подобных исследований лежит понятие – «программный дефект диверсионного типа». Дефекты этого типа преднамеренно (из криминальных соображений) вносятся в КП самим программистом (одним из коллектива разработчиков-программистов) на этапе разработки КП, что и создаёт проблему технологической безопасности КП. Ординарные (обычные) программные дефекты, вносимые в КП любыми (потенциально всеми) разработчиками-программистами на том же этапе приводят к проблеме обеспечения надёжности КП, то есть здесь тоже идёт речь о нелегитимных (как преднамеренных,

так и случайных) действиях собственных сотрудников (программистов) организации [12, 13].

Даже из этого краткого описания проблемы обеспечения технологической безопасности компьютерной инфосферы ясно, что в основе самого появления такой проблемы находится фигура инсайдера, а попросту – программиста-злоумышленника (агента, предателя, диверсанта и т.п.), что, собственно, и обуславливает широкое применение криминально-уголовной терминологии в инсайдерской проблематике. Отсюда следует, что исследование проблемы инсайдерства должно охватывать все этапы жизненного цикла КП (и БД), включая и этап их создания, и этап их эксплуатации. И это исследование целесообразно проводить в рамках новой единой научной дисциплины – инсайдерологии компьютерной инфосферы (рис.2), которая, в частности, должна включать в себя положения теории информационной безопасности, дефектологии КП криминальной дефектологии компьютерной инфосферы, теории программных агентов, психологии программистов, метрологии информационных рисков [14-16].

Рис. 2. Структура инсайдерологии компьютерной инфосферы

Наиболее важным и наиболее структурно разработанным из этих научных направлений являются дефектология (рис. 3) и криминальная дефектология компьютерной инфосферы [17, 18].

Так, для исследования программных дефектов диверсионного типа предлагается следующая их классификация: по способу активации – командные, автономные, комбинированные; по методу приведения в боеготовое состояние – априорные, апостериорные, адаптивные; по выражающему фактору – разрушающие, искажающие, информирующие.

Наиболее опасными из них являются автономные, апостериорные, искажающие дефекты КП. Автономные – значит не зависящие от внешних воздействий,

которые, в принципе, могут быть нейтрализованы. Апостериорные – автоматически генерируют активные (поражающие) части закладки в процессе эксплуатации КП, то есть возможность обнаружения таких дефектов снижается. Искажающие – также трудно обнаружимы, так как нет явных следов их конкретного проявления, хотя в результате этих искажений может быть не выполнена основная задача функционирования всей системы (что и является целью внедрения искажающих дефектов).

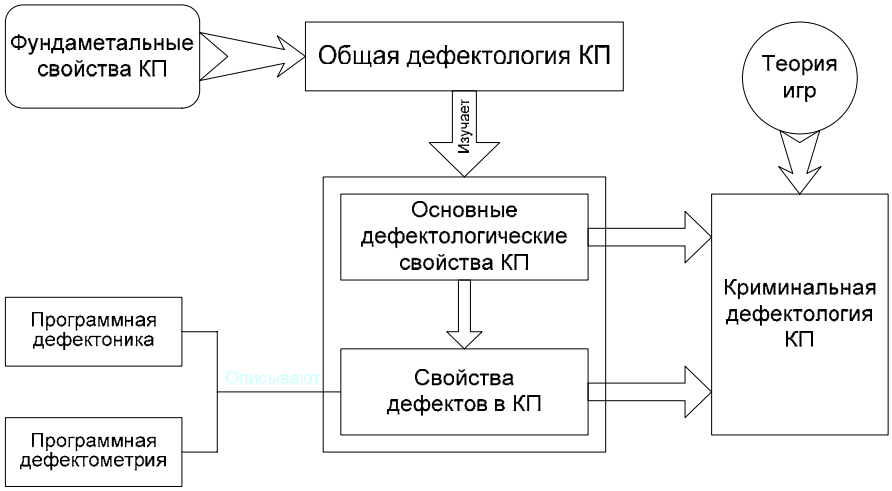

Рис. 3. Дефектология компьютерных программ

Опасными являются также информирующие (разведывательные) дефекты, которые обеспечивают скрытую утечку информации без нарушения нормального функционирования КП и системы в целом.

Теоретической основой технологической безопасности КП, обеспечивающей исследования преднамеренных программных дефектов диверсионного типа, является, как и в случае с надёжностью КП, дефектология КП, которая в рамках теоретического программирования изучает все свойства КП, связанные с дефектами в программах, и все свойства самих программных дефектов. Дефектология КП базируется на фундаментальных свойствах самой КП: полирутности («ветвистости»), энтропийной сложности, идентичной копируемости и локальной стабильности. Основными дефектологическими свойствами КП являются следующие: дефектоскопичность, дефектабельность, дефектогенность, дефектомобильность, дефектодиагностируемость, дефектокорректируемость, дефектоустойчивость.

Для описания свойств самих дефектов в КП служат такие дисциплины, как программная дефектоника и программная дефектометрия. Дефектоскопичность – это свойство КП проявлять дефекты в некоторых условиях эксплуатации. Дефектабельность – это имманентное свойство КП содержать дефекты. Дефектогенность – это свойство КП быть поражаемой дефектами (при этом, естественно, учитываются и технологическая, аппаратная и антропогенная среда).

Дефектомобильность, дефектодиагностируемость, дефектокорректируемость, дефектоустойчивость описывают возможности передвижения в КП, обнаружения дефектов в КП, устранения обнаруженных дефектов из КП, противодействия (компенсации) негативных последствий дефектов, проявляющихся в процессе эксплуатации соответственно.

Дефектоника и дефектометрия изучают структурные свойства программных дефектов и степень их негативного влияния на ход вычислительного процесса. Разделом общей дефектологии КП является криминальная дефектология, изучающая, в частности, такие свойства КП, как диверсионная дефектогенность, активная дефектабельность, латентная дефектоскопия и управляемая дефектомобильность.

Дефектология КП составляет основу нового научного направления – дефектологии компьютерной инфосферы (здесь должны быть добавлены исследования соответствующих системных связей между составляющими частями компьютерной инфосферы и интерфейса со всей инфосферой). В целом это научное направление сейчас находится в стадии становления, отдельные его разделы неравномерно (наиболее широко представлена в научно-технической литературе дефектоскопия, которая является основной базой для современной теории надежности КП). Следует также учесть, что дефектология КП является единственной научно обоснованной методологической базой при организации страхового дела применительно к компьютерной инфосфере, а также при создании так называемых «доверительных» КП.

Перспективным для развития дефектологии компьютерной инфосферы и ее разделов, а также и решение на этой базе проблемы как технологической, так и эксплуатационной безопасности КП (включая, разумеется, и проблему надёжности КП) может быть более глубокое использование результатов, полученных в рамках теоретического программирования. Так, для диверсионной дефектогенности весьма эффективным может стать положение, согласно которому всякая развитая программная система имеет склонность к расползанию, самодеструкции и к неконтролируемой репликации своих частей. Это было предсказано Дж. Фон Нейманом в теореме о том, что конечный автомат, достигший определенного уровня сложности, может реплицировать себя.

Особенно это актуально для интеллектуальных компьютерных программ (ИКП), которые являются в общем случае одним из видов нестабильных КП [19]. Нестабильность вызывается совокупностью экзо- и эндофакторов и внешне (для пользователя) проявляется в виде невозможности получить (в отличие от стабильных КП) идентичный прежнему результат функционирования КП при идентичных входных условиях. Те нестабильные КП, в результате функционирования которых имманентно (без участия программиста) улучшается интегральный показатель качества КП, необходимый пользователю (точность, быстродействие, номенклатура решаемых задач и т.п.), т.е. повышается их «интеллект», называются ИКП.

Дефектология ИКП существенным образом усложняется из-за фактического наличия в ИКП многоконтурности, которая необходима для соответствующей адаптации и самообучения. Известными представителями ИКП являются КП, построенные по принципу нейронных сетей. В связи с этим дефектология ИКП включает в себя все вышеприведённые номинации (включая и криминальную) дефектологии ординарных КП, но, во-первых, все для каждого контура в отдельности, во-вторых, с учётом особенностей и специфики каждого контура, в-третьих, при иерархическом примате как, естественно, и самих контуров высшего уровня, так и всех дефектогенных номинаций соответствующего контура, в-четвёртых, при наличии инверсного влияния дефектологических характеристик разноуровневых контуров, в-пятых, в условиях повышения чувствительности к экзодеструктивным влияниям (типа «вирусной инфекции») и, в-шестых, с учётом симультативной взаимосвязи («дефектологического симбиоза») всех дефектологических факторов в ИКП.

Исследования по этим направлениям дефектологии компьютерной инфосферы позволят создать научно обоснованный базис для построения многофакторной инсайдерологии компьютерной инфосферы. Особое (прикладное) значение инсайдерологии имеет разработка методологии противодействия инсайдерской деятельности. Методы такого противодействия должны носить как технологический, так и антропологический характер, но, как правило, они будут комбинированными, например, методы обфускации, криптопрограммирования, применения полиграфов и тепловизоров. Также следует иметь в виду, что эффективной инсайдерология может стать только тогда, когда она будет иметь соответствующее метрологическое обеспечение [20].

Кроме того, в основе инсайдерлогической и соответственно антиинсайдерлогической деятельности лежит человеческий фактор, который по большому счёту может регулироваться только законодательным образом (рис. 4).

Название	Степень готовности
Федеральный закон **«О противодействии инсайдерским угрозам»**	Разрабатывается
Федеральный закон (Общий технический регламент) **«Обеспечение безопасности при использовании критических систем с компьютерной обработкой информации»**	Проект разработан и обсуждён *Опубликован в «Вестнике технического регулирования» №1(2), январь, 2004 г.*
Федеральный закон **«О применении полиграфа»**	Внесён в Государственную Думу в качестве законопроекта

Рис. 4. Минимальный правовой базис противодействия инсайдерским угрозам

В этой связи весьма действенным нормативно-правовым инструментарием, юридически связывающим существующее законодательство, в том числе и в правоохранительной сфере, с комплексной проблемой обеспечения безопасности компьютерной инфосферы, является институт технических регламентов [2, 21, 22].

В целом, создание, развитие и применение инсайдерологии позволит эффективно и целенаправленно проводить мероприятия по обеспечению информационной безопасности систем критических приложений в части предотвращения нелегитимных действий собственных сотрудников.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Бородакий Ю.В., Добродеев А.Ю., Пальчун Б.П.* Безопасность и терроройстойчивость критической техносферы России. Известия Кабардино-Балкарского научного центра РАН, 2005 год, ноябрь, – № 2 (14). – С. 134 – 146.

2. *Бородакий Ю.В., Пальчун Б.П.* Техническое регулирование и компьютерная

инфосфера. Труды Конференции «Информационная безопасность России в условиях глобального информационного общества» (Москва, «ИНФОФОФУМ-5» 20 октября 2003г.). – М., 2003.

3. Внутренние ИТ-угрозы в России. 2005 г. – http://www.infowatch.ru/threats? chapter=147151396&id=178488463.

4. *Доля А.* Защита от инсайдеров в российских компаниях. – М.: КомпьютерПресс, 2006. – № 3.

5. Доля А. Серебряная пуля от инсайдеров. – М.: КомпьютерПресс, 2006. – № 9.

6. *Зайцев О.* Угрозы для корпоративной сети и рекомендации по разработке корпоративной политики информационной безопасности. – М.: КомпьютерПресс, 2006. – № 9.

7. Ульянов В. Защита от инсайдеров: от поставщиков к заказчикам. – М.: КомпьютерПресс, 2007. – № 3.

8. *Ершов В.* Инсайдеры. Свежий взгляд на известную проблему. – М.: Information Security/Информационная безопасность, 2008. – № 4.

9. Пять классов средств защиты от инсайдерских угроз. – М.: Агентство «Монитор» // Вестник информационной безопасности, 2006. – № 11 (32).

10. *Пальчун Б.П., Ефимов А.И.* О технологической безопасности компьютерной инфосферы. – М.: Журнал «Вопросы защиты информации», 1995. – №3(30). – С. 86-88.

11. *Пальчун Б.П., Спиридонов А.В.* К вопросу о технологической безопасности компьютерной инфосферы. В кн. Тезисы докладов IV Международной конференции «Комплексная защита информации», (Республика Беларусь, Раубичи, 29 февраля – 2 марта 2000 г.). – Минск.: Институт технической кибернетики НАН Беларуси, 2000. – 152 с.

12. *Пальчун Б.П., Ефимов А.И.* Концептуальные вопросы дефектологии программного обеспечения. – В кн.: Тез. докл. Международного научно-технического семинара «Надёжность, отказоустойчивость и производительность информационных систем» (г. Туапсе, 1993). – Краснодар: НПО РЭС им. Попова,1993. – 65с.

13. *Пальчун Б.П.* Проблема взаимосвязи надежности и безопасности информации. В кн.: Сб. тезисов докл. конференции «Методы и средства обеспечения безопасности информации». – СПб., 1996. – С.184-185.

14. *Бородакий Ю.В., Белый А.Ф., Пальчун Б.П., Болдина М.Н.* Об инсайдерологии компьютерной инфосферы. Материалы X Международной научно-практической конференции. Ч. 2. – Таганрог: Изд-во ТТИ ЮФУ, 2008. – С. 287.

15. *Бородакий Ю.В., Горелкин Г.А., Добродеев А.Ю., Коротков С.В., Пальчун Б.П.* Фундаментальные проблемы теории информационной безопасности автоматизированных систем. Сборник материалов VIII международной конференции «Комплексная защита информации», 23-26 марта 2004. – Валдай, 2004.

16. *Пальчун Б.П., Нащёкин П.А.* Метрология информационных рисков В кн.: Труды III Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России (ИБРР – 2003)» (Санкт-Петербург, 25-27 ноября 2003 г.) – СПБ.: Изд-во СПИИ РАН, 2003. – 367 с.

17. *Пальчун Б.П.* Дефектология программного обеспечения и технологическая безопасность компьютерной инфосферы. – М.: Журнал «Надёжность», 2003. – № 3 (6).

18. *Бородакий Ю.В., Пальчун Б.П., Белый А.Ф.* О криминальной дефектологии компьютерных программ. Сборник трудов VI Межведомственной научно-технической конференции «Проблемы комплексного обеспечения защиты информации и совершенствования образовательных технологий подготовки специалистов в области информационной безопасности». Т. I. – Краснодар, 2007.

19. *Пальчун Б.П.* Основные положения дефектологии интеллектуальных компьютерных программ. Журнал «Вопросы защиты информации», 2007. – № 1. – С. 46-50.

20. *Бородакий Ю.В., Пальчун Б.П., Болдина М.Н.* О метрологических аспектах систем обеспечения информационной безопасности. Материалы XI Международной конференции «Комплексная защита информации». 20-23 марта 2007 года, г. Новополоцк (Республика Беларусь).

21. *Бородакий Ю.В. ,Добродеев А.Ю., Пальчун Б.П.* Система технических регламентов для критических объектов информатизации. Журнал «Information Security/Информационная безопасность», 2004. – №3.

22. *Бородакий Ю.В. ,Добродеев А.Ю., Пальчун Б.П.* Общий технический регламент по обеспечению безопасности компьютерной инфосферы. Журнал «Information Security/Информационная безопасность», 2004. – № 5.

УДК 681.018

С.Н. Смирнов

МЕТОД ПРОЕКТИРОВАНИЯ СИСТЕМ ОБРАБОТКИ ДАННЫХ С ЗАДАННЫМИ ХАРАКТЕРИСТИКАМИ ДОСТУПНОСТИ

Введение

Целью данной работы является разработка математической модели и метода получения временных характеристик процесса обработки данных в системе обработки данных как функции от известных параметров системы. В качестве математической модели автоматизированной системы обработки данных используется система массового обслуживания с одним обслуживающим прибором [1,2].

Основные результаты теории массового обслуживания связаны с получением вероятностных характеристик времен прохождения требований в системе при заданных характеристиках входящего потока и процесса обслуживания. При проектировании автоматизированных систем обработки информации обычно возникает, в некотором смысле, обратная задача, когда по заданным характеристикам входящего потока и заданным ограничениям на характеристики времен выполнения запросов, необходимо определить параметры процесса обслуживания, обеспечивающие выполнение заданных ограничений. В техническом здании на разработку системы обычно указываются допустимые средние задержки сообщений или квоты сообщений, время прохождения которых не должно превышать заданного порогового значения. Проектировщику необходимо за счет выбора управляемых параметров обеспечить реализацию временных характеристик обработки сообщений, которые определены требованиями технического задания.

В данной работе предполагается, что для входящих потоков запросов в систему известны интенсивности их поступления. Неопределенность представления проектировщика о входящем потоке отражается в предположении о дисперсии временного интервала между поступлениями соседних запросов, относимых к одному классу. Искомыми характеристиками системы массового обслуживания, моделирующей проектируемые АСОД, являются интенсивности обработки сообщений. Значения иных вероятностных характеристик времен обработки сообщений априорно неизвестны и проектировщик должен сформулировать некоторые предположения, необходимые для решения задачи определения интенсивности обработки сообщений, гарантирующей выполнение заданных временных ограничений.

Предположения проектировщика о вероятностных характеристиках времен обработки сообщений предлагается формулировать в форме задания единственной характеристики – коэффициента вариации соответствующей случайной величины. Предельное – нулевое – значение коэффициента вариации на содержательном уровне означает, что проектировщик предполагает одинаковое время обработки