УДК 681.3

Д. В. Флейтман
Институт проблем регистрации информации НАН Украины
ул. Н. Шпака, 2, 03113 Киев, Украина

Жизненный цикл и живучесть корпоративных информационных систем

Рассмотрена комплексная система мероприятий повышения живучести корпоративных информационных систем (КИС) на всем протяжении ее жизненного цикла. Описаны методы повышения живучести в привязке к структуре и стадиям жизненного цикла КИС. Приведено общее описание архитектуры программно-информационных средств повышения живучести в составе КИС.

Ключевые слова: *корпоративная информационная система, корпорация, жизненный цикл, живучесть, методы повышения живучести, архитектура программного обеспечения, структура информационной системы.*

Введение

Корпоративная информационная система (КИС) — это инструмент повседневной деятельности коллектива корпорации, объединенного решением общих задач. Специфика корпорации такова, что ее административные и производственные площади могут быть территориально распределены, предприятия, входящие в корпорацию, связаны между собой многими сотнями динамичных информационных потоков, а время подготовки, обмена и анализа информации должно соответствовать реалиям современного бизнеса. В этих условиях задачей КИС является создание комфортной среды для выполнения корпорацией ее основных задач.

Можно сказать, что КИС соответствует требованиям Заказчика, если она обладает двумя качествами: «незаменимости» и «незаметности». То есть, с одной стороны, в случае сбоев КИС начинает «лихорадить» и корпорацию, а в случае стабильной работы пользоваться ею также естественно, как ставшими привычными достижениями цивилизации — телевизором, телефоном, домашним компьютером или даже горячей водой. Одним из основных условий «незаметности» КИС является «живучесть» — способность адаптироваться к новым изменившимся и, как правило, непредвиденным ситуациям, противостоять неблагоприятным воз-

действиям, выполняя при этом свою целевую функцию, за счет соответствующего изменения структуры и поведения системы [1].

Понятие живучести системы — это комплексное понятие, включающее в себя множество дисциплин различных областей. Живучесть нельзя обеспечить с заданным уровнем выполнения, как, например, надежность или отказоустойчивость. Методы обеспечения живучести должны создать *определенные* средства КИС, позволяющие ей функционировать в, как правило, *непредвиденных* ситуациях. В этом и заключается сложность придания КИС свойства живучести в определении [1].

Будем считать, что реально эксплуатируемая КИС обязательно обладает некоторым уровнем живучести, поэтому, для придания КИС свойства живучести в трактовке [1] будем употреблять термин «повышение» живучести.

Повышение живучести КИС — не одноразовое мероприятие, проводимое на какой-либо из стадий ее жизненного цикла, а *непрерывная направленная система действий*, основанная на определенных методах, *выполняемая на всем протяжении жизненного цикла КИС*.

В настоящей работе сделана попытка описать методы повышения живучести КИС в привязке к ее структуре и стадиям жизненного цикла.

Чтобы не останавливаться на вопросах обеспечения КИС минимально необходимого уровня живучести, сразу оговоримся, что рассматриваемая КИС профессионально спроектирована и, с точки зрения, функциональности, эргономических характеристик интерфейсов и эксплуатационных характеристик работы в заданных условиях полностью удовлетворяет требованиям Заказчика. Поэтому в дальнейшем будем говорить об общих методах *повышения* живучести этого класса систем.

Структура КИС

Как любая сложная система КИС состоит из подсистем, обладающих, с точки зрения их архитектуры, всеми свойствами системы и создаваемых как самостоятельные системы. По назначению подсистемы КИС можно условно разделить на два вида: обработки и хранения информации и обслуживающие. Подсистемы обработки хранения информации выполняют процедуры и операции в части информационно-аналитической поддержки принятия управленческих решений. Обслуживающие подсистемы обеспечивают поддержку работоспособности подсистем обработки и хранения информации, например, подсистема построения графиков и диаграмм, подсистема документирования, подсистема информационного поиска, подсистема управления, подсистема диагностики и т.д.

В зависимости от отношения к объекту управления различаются два вида подсистем обработки информации: объектно-ориентированные (объектные) и объектно-независимые (инвариантные) [5]. Объектные подсистемы выполняют одну или несколько процедур или операций, непосредственно зависимых от конкретного объекта управления. Инвариантные подсистемы выполняют унифицированные процедуры и операции.

Подсистема состоит из компонентов информационной системы (далее — компонентов), объединенных общей для данной подсистемы целевой функцией и

обеспечивающих функционирование этой подсистемы. Компонент представляет собой элемент обеспечения, выполняющий определенную функцию в подсистеме. Можно условно определить следующие виды обеспечений [4]:

– методическое — документы, в которых отражены состав, правила отбора и эксплуатации средств автоматизации информационно-аналитической поддержки принятия управленческих решений;

– лингвистическое — языки управления, терминология;

– математическое — методы, математические модели, алгоритмы;

– программное — документы с текстами программ, программы на машинных носителях и эксплуатационные документы;

– техническое — устройства вычислительной и организационной техники, средства передачи данных, измерительные и другие устройства или их сочетания;

– информационное — документы, содержащие описания стандартных информационно-аналитических процедур, типовых решений, типовых бизнес-процессов, типовых алгоритмов и др., а также файлы и базы данных на машинных носителях с записью указанных документов;

– организационное — положения, инструкции, приказы, штатные расписания, квалификационные требования и другие документы, регламентирующие организационную структуру подразделений и их взаимодействие с комплексом средств автоматизации информационно-аналитической поддержки принятия управленческих решений.

Введение структурного понятия «компонент» как некоторого элементарного «кирпичика», позволяет раскрыть внутреннюю структуру подсистемы и указать конкретные связи между подсистемами не только иерархические, но и методические, информационные и т.д.

Структурное единство подсистемы обеспечивается связями между компонентами различных средств обеспечения, образующими подсистему, а структурное объединение подсистем в КИС — связями между однотипными компонентами, входящими в различные подсистемы.

Жизненный цикл КИС и обеспечение живучести

Жизненный цикл КИС — это совокупность взаимоувязанных процессов последовательного изменения ее состояния от начала исследования и обоснования разработки до окончания эксплуатации [4].

Стадии жизненного цикла КИС — часть жизненного цикла, характеризующаяся определенным состоянием КИС, совокупностью видов предусмотренных работ и их конечными результатами.

Определим следующие стадии жизненного цикла КИС.

1. «Создание системы» («Создание»):

– обследование корпорации и обоснование необходимости создания КИС;

– формирование требований пользователя к КИС;

– тактико-техническое задание;

– изучение корпорации;

– проведение необходимых научно-исследовательских работ;

– разработка вариантов концепции КИС и выбор варианта концепции, удовлетворяющего требованиям пользователя;

– разработка и утверждение технического задания (ТЗ) на создание КИС;

– разработка предварительных проектных решений по КИС и ее компонентам;

– разработка документации на КИС и ее компоненты;

– разработка и оформление документации на поставку изделий для комплектования КИС и (или) технических требований (технических заданий) на их разработку;

– разработка заданий на проектирование в смежных частях проекта;

– разработка рабочей документации на систему и ее компоненты;

– разработка или адаптация программ.

2. «Ввод в эксплуатацию» («Ввод»):

– подготовка корпорации к вводу КИС в действие;

– подготовка персонала;

– комплектация КИС поставляемыми изделиями (программными и техническими средствами, программно-техническими комплексами, информационными изделиями);

– пусконаладочные работы;

– проведение предварительных испытаний;

– проведение опытной эксплуатации;

– проведение приемочных испытаний.

3. «Эксплуатация»:

– использование по назначению;

– сопровождение;

– модернизация;

– совершенствование;

– расширение;

– видоизменение;

– адаптация.

Подобная формализация стадий жизненного цикла удобна для дальнейшего описания системы мероприятий повышения живучести КИС. Для работ по созданию КИС, например для конфигурационного управления, необходимо понимать, что при создании сложных систем описанные выше стадии будут пересекаться и перекрываться уже в самом начале работ. Например, подсистемы КИС, входящие в пилотный (содержащий минимально необходимое для начала эксплуатации количество функций) комплекс, будут проходить эти стадии раньше других подсистем. То есть, говоря о КИС в целом, нельзя однозначно определить на какой стадии жизненного цикла она находится, необходимость постоянного развития и доработок компонентов КИС также не позволит в дальнейшем, после внедрения всей КИС в соответствии с ТЗ, однозначно определить для нее стадию жизненного цикла т.к. появятся дополнения к ТЗ. В то же время, некоторые виды работ, например, подготовка корпорации, подготовка персонала стадии «Внедрение» более рационально будет начинать на более ранних стадиях и т.д.

Как уже говорилось выше, повышение живучести — это система мероприятий, пронизывающая весь жизненный цикл КИС. На каждой стадии жизненного

цикла КИС существуют наиболее эффективные методы придания ей свойства живучести. На рис. 1 показаны три принципиальных направления повышения живучести КИС на всем протяжении ее жизненного цикла.

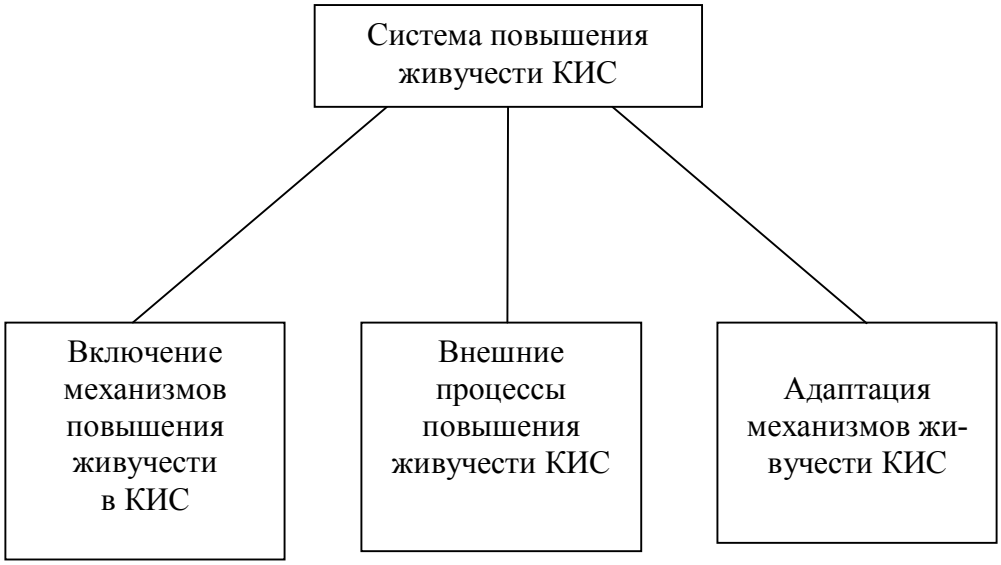

Рис. 1. Основные направления повышения живучести КИС

На ранних стадиях жизненного цикла КИС в процессе проектирования и разработки ее компонент механизмы обеспечения живучести реализуются как неотъемлемая часть каждой компоненты КИС. Можно сказать, что механизмы живучести сохраняют работоспособность КИС, когда средства обеспечения отказоустойчивости и надежности бессильны. Говоря упрощенно, живучесть КИС — это ее защита от множества нештатных ситуаций, предвидеть которые практически невозможно. Поэтому механизмы повышения живучести КИС, в первую очередь, должны быть нацелены на обнаружение малейших отклонений не только функционирования КИС от заданных режимов, но и воздействий на КИС внешней среды обеспечения эксплуатации. Учитывая неопределенность поражающих воздействий, наиболее эффективной будет комплексная защита КИС, т.е. включение механизмов повышения живучести во все компоненты КИС. Охарактеризуем коротко работы по живучести КИС на всех стадиях жизненного цикла.

Стадия **«Создание»**. На всех этапах работ вплоть до технического задания должна проводиться работа независимой группой специалистов по подготовке раздела ТЗ «требования по живучести». Независимость группы специалистов должна определяться непредвзятым отношением к объему и стоимости закладываемых требований по живучести относительно общей стоимости проекта КИС. При подготовке технического задания решаются вопросы придания свойства живучести компонентам КИС: методическому, лингвистическому, математическому, программному, техническому, информационному, организационному обеспечениям и КИС в целом. При разработке системы создаются средства противодействия возникновению нештатных ситуаций, их распознавания и восстановления функционирования КИС.

На дальнейших стадиях жизненного цикла «введении» и «эксплуатации», придание живучести наряду с механизмами в составе КИС поддерживают внешние *процессы повышения живучести*.

На стадии **«Ввод»** процесс повышения живучести — это обеспечение адекватной оценки того, что компоненты КИС и системы в целом удовлетворяют определенным требованиям по живучести, заложенным в ТЗ. Как и на стадии «создание» организация процесса должна обеспечить непредвзятость выполняемой его группы специалистов, как к самому проекту КИС, так и к Заказчику, и к Разработчику. Процесс повышения живучести на этой стадии жизненного цикла включает процессы верификации, валидации (проверки соответствия системы тактико-техническому заданию), совместных просмотров, аудитов.

На стадии **«Эксплуатация»** процесс повышения живучести выполняется в рамках процесса сопровождения эксплуатации КИС. Процесс включает в комплексе с механизмами живучести КИС такие мероприятия:

– распознавание нештатных ситуаций в случае их возникновения;

– противодействие возникновению нештатных ситуаций;

– восстановление функционирования КИС в условиях нештатной ситуации.

На стадии «Эксплуатация» накапливается опыт функционирования КИС с учетом специфики корпорации, специфики внешней среды, сезонных нагрузок, интенсивности эволюции КИС и т.д. Накопленный опыт эксплуатации КИС в виде статистики выполнения различных типовых операций, действий обслуживающего персонала в нештатных ситуациях, частоты и типов отказов технических средств, объемов нагрузок в разное время суток, кварталов и т.д. — основа совершенствования механизмов живучести. В этих условиях система повышения живучести должна включать мероприятия по *адаптации механизмов живучести* КИС. Эти мероприятия включают как настройку параметров механизмов живучести, корректировку и дополнение информации базы данных, так и внесение изменений в компоненты КИС, в части повышения живучести.

Таким образом, повышение живучести КИС — это непрерывное совершенствование системы как в автономном режиме (автоматически), так и с привлечением специалистов различных областей (системных аналитиков, проектировщиков, программистов, методистов, лингвистов, эксплуатационников и т.д.) на всех стадиях жизненного цикла КИС (рис. 2).

Классификация методов повышения живучести КИС

Как уже говорилось выше, описание системы мероприятий повышения живучести КИС проводится по отношению к профессионально проектируемой системе, т.е. проект КИС обладает такими свойствами как «безопасность», «надежность», «отказоустойчивость». И все же при этом необходимо повышать живучесть. Поэтому, прежде чем проводить классификацию методов повышения живучести, определим их взаимосвязь с классическими методами обеспечения безопасности, надежности и отказоустойчивости.

Рис. 2. Методы обеспечения живучести на различных этапах жизненного цикла КИС

Классические методы обеспечения безопасности КИС базируются на принципе «устойчивости» — информационная система должна представлять собой «крепость», т.е. все усилия по обеспечению безопасности направлены на то, чтобы не допустить вторжения в систему, выхода из строя важных программно-технических компонентов системы, частичной или полной потери информации. Эти средства опираются на понятия отказоустойчивости, надежности, защищенности. Часто, при вторжении в систему либо возникновении другой нештатной ситуации, не существует формализованной, а тем более автоматизированной процедуры восстановления системы.

В настоящее время КИС становятся настолько масштабными, что применение классических методов обеспечения безопасности становится нецелесообразным и не всегда возможным из-за отсутствия централизованного административного управления, огромного количества угроз, которые необходимо учесть при по-

строении системы, невозможности контролировать огромное количество информации, приходящей от межсетевых экранов и систем отражения атак.

В отличие от классических методов обеспечения безопасности, методы обеспечения и повышения живучести базируются на четырех основных принципах [2]: 1) распознавания, 2) противодействия, 3) восстановления, 4) адаптации и включают в себя методы обеспечения безопасности, надежности и отказоустойчивости и являются их надмножеством.

Принцип распознавания [6, 7] заключается в способности системы обнаруживать атаки, успешные вторжения, повышение риска выхода из строя важных компонентов системы, риски потери или искажения информации. Этот принцип основывается на методах:

– *диагностики* — внесения в систему аппаратно-программных средств, позволяющих отслеживать нежелательные отклонения в работе системы и ее отдельных компонентов;

– *оповещения* — внесения в систему аппаратно-программных средств, позволяющих уведомлять пользователей и системных администраторов о нежелательные отклонения в работе системы и ее отдельных компонентов;

– *регистрации событий* — сбора и хранения информации о действиях различных пользователей и компонентов системы;

– *анализа шаблонов поведения пользователей* — сравнения последовательности действий пользователей и компонентов системы с известными шаблонами атак и некорректного использования.

Результаты применения этого принципа служат базой для применения активного противодействия (при обнаружении успешных атак или появлении новых рисков) и адаптации.

Принцип противодействия [6, 7] частично позаимствован из дисциплины безопасности информационных систем, и реализуется ее классическими методами:

– *идентификацией* — доказательством того, что пользователь системы действительно является тем, за кого себя выдает. Для идентификации могут применяться такие средства как имя пользователя и пароль, карты доступа (smart cards), отпечатки пальцев и т.п.;

– *авторизацией*— набором прав того или иного пользователя на выполнение затребованных им операций;

– *ограничением привилегий пользователей* — разделением пользователей системы на группы, каждая из которых определяет свой набор прав доступа, например, право на чтение информации, право на запись информации, право на доступ к определенным частям баз данных и т.п.;

– *установкой межсетевых экранов* — физическим отделением системы от внешней среды;

– *внесением избыточности в систему* — установкой резервного аппаратного и программного обеспечения, а также архивов информации.

Кроме того, к этому же принципу можно отнести и такие методы как:

– *реконфигурация* — обеспечение функционирования системы при выходе из строя ее ресурсов за счет изменения путей передачи и обработки информации;

– *реорганизация* — обеспечение функционирования системы при выходе из строя ее ресурсов за счет переопределения функций вышедших из строя компонентов системы между работоспособными компонентами;

– *реконструкция* — обеспечение функционирования системы при выходе из строя ее ресурсов за счет компенсации потерянной функциональности частично вышедших из строя компонентов функциональностью работоспособных компонентов;

– *диверсификация* — непрерывное планомерное изменение конфигурации системы, направленное на усложнение организации атак на систему.

Перечисленные выше методы относятся к, так называемому, активному противодействию.

Целью принципа противодействия является поддержание штатных условий функционирования и минимизация ущерба, наносимого переходом системы в нештатный режим функционирования.

Принцип восстановления [6, 7] заключается в способности системы восстанавливать свою функциональность и работоспособность компонентов после отражения атаки. Этот принцип реализуется методами:

– *поддержки баз данных изменений* — сбором сведений обо всех изменениях и дополнениях информации, хранимой в системе, в таком объеме, который предполагает возможность отказа от каждого конкретного изменения и определения источника каждого конкретного изменения;

– *организацией безопасного хранения информации* — использованием при хранении информации надежных и отказоустойчивых технологий, которые обеспечивали бы сохранность и доступность информации с заданными показателями качества;

– *поддержки транзакционности процессов* — организацией работы процессов изменения информации в системе таким образом, чтобы в любой момент времени можно было гарантировать целостность данных, хранимых в системе.

Основная цель этого принципа заключается в построении формализованной автоматизированной процедуры возвращения системы в штатные условия функционирования.

Принцип адаптации [6, 7] заключается в способности системы «обучаться», т.е. развиваться на основании информации об успешных атаках, возникновении нештатных ситуаций, изменении условий функционирования системы. Целью принципа адаптации является, во-первых, создание надежной защиты от отраженных и неизвестных ранее атак, во-вторых, приспособление к новым изменившимся условиям функционирования системы и обеспечение выполнения всех функций системы в таких условиях функционирования.

Следует отметить, что грани между описанными принципами не являются четкими, некоторые методы (или комбинации методов) можно относить к различным принципам. За счет этого достигается общая целостность методологии обеспечения и повышения живучести КИС.

Архитектура системы повышения живучести КИС

Построение системы повышения живучести КИС (рис. 3) — это разработка двух программно независимых, но взаимосвязанных методически и информационно автоматизированных систем: подсистемы повышения живучести (ППЖ) КИС и внешней системы обеспечения живучести (СОЖ) КИС. Дальнейшие работы в этом направлении — это адаптация и развитие ППЖ и СОЖ.

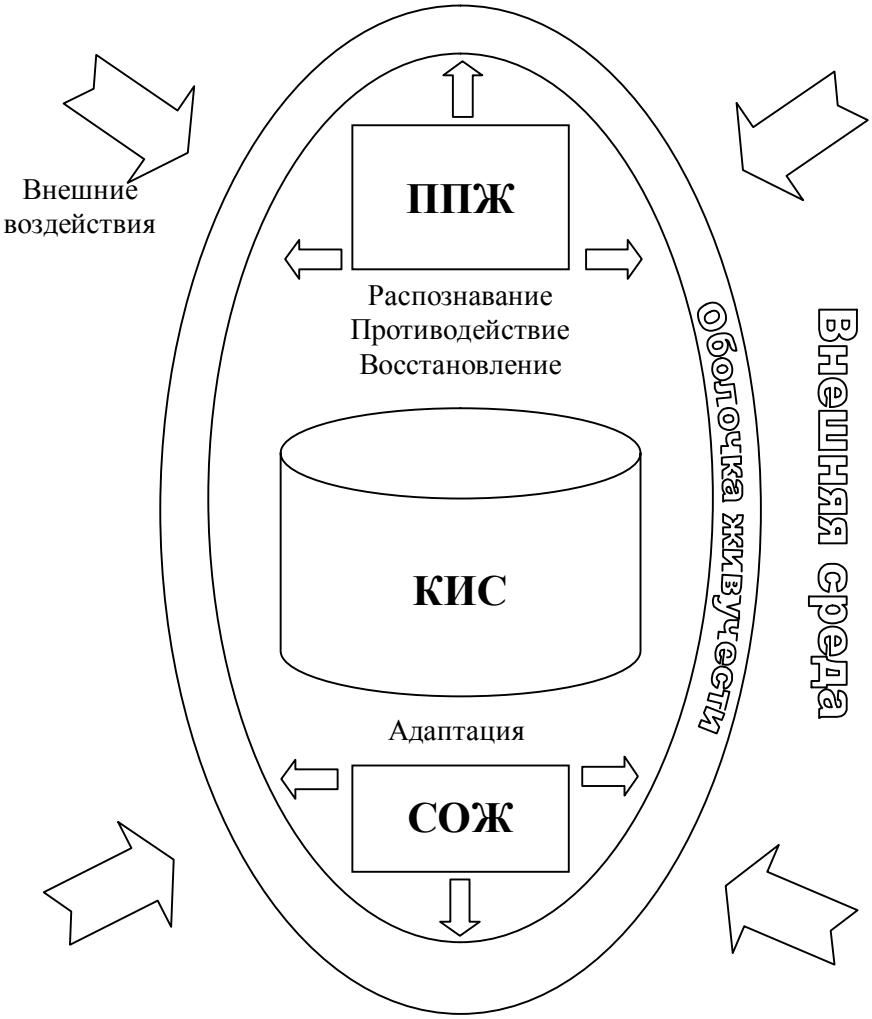

Рис. 3. Архитектура системы повышения живучести КИС

ППЖ КИС является ее неотъемлемой частью, и поэтому каждая стадия жизненного цикла КИС должна включать в себя соответствующие стадии жизненного цикла ППЖ. Эта подсистема должна проектироваться, разрабатываться, внедряться и сопровождаться как неотъемлемая часть КИС.

СОЖ — это самостоятельная система. Она должна создаваться разработчиками, не участвующими непосредственно в создании КИС. Методической базой создания СОЖ должны быть только принципы и методы, описанные выше.

Стадии жизненного цикла СОЖ должны опережать соответствующие стадии жизненного цикла КИС (и соответственно ее ППЖ), а, говоря точнее, опережать стадии жизненного цикла пилотного комплекса КИС. Наличие СОЖ на стадии «ввода в эксплуатацию» КИС значительно повысит эффективность ее внедрения.

В результате двойственности взаимодействия системы с окружающей средой живучесть определяется как воздействием внешней среды на систему, так и воздействием системы на внешнюю среду. Предположим, что в КИС создается и хранится информация, потенциально опасная для внешней среды, например для корпорации, которая занимается тестированием и сертификацией систем безопасности, это могут быть компьютерные вирусы, планы тестовых атак и т.п. В случае утечки такой информации из системы, она может быть использована для организации реальных атак. Окружающая среда будет бороться с КИС, которая допускает утечки такой информации, что, несомненно, приведет к гибели системы.

Описанные выше методы предназначены для обеспечения реагирования на воздействия внешней среды на КИС. Необходимо ввести также группу методов, которые обеспечивали бы управление воздействием КИС на внешнюю среду, т.е. контроль исходящей информации. Для этого можно применять, так называемое цензурование, т.е. набор правил, по которым проверяется вся исходящая информация. На момент внедрения системы, она должна уже обладать некоторым базовым набором правил цензурования, а в процессе эксплуатации этот набор правил должен постоянно расширяться на основе экспертных оценок реакции внешней среды на новые типы информации, которые производятся системой, а также реальной реакции внешней среды на исходящую из системы информацию [3].

1. *Додонов А.Г., Горбачик Е.С., Кузнецова М.Г.* Живучесть информационно-аналитических систем в аспекте информационной безопасности // Зб. наук. пр. «Інформаційні технології та безпека». — Вип. 4. — К., 2003.

2. *Додонов А.Г., Кузнецова М.Г.* Проблемы и тенденции создания живучих вычислительных систем: Метод. Разработки. — К.: Наук. думка, 1981.

3. *Додонов А.Г., Флейтман Д.В.* К вопросу безопасности информационных систем // Зб. наук. пр. «Інформаційні технології та безпека». — Вип. 6. — К., 2004.

4. Словарь по кибернетике: Св. 2000 ст. / Под ред. В.С. Михалевича. — 2-е изд. — К.: Гл. ред. УСЭ им. М.П. Бажана, 1989 — 751 с.

5. Справочник по САПР / Под ред. В.И. Скурихина. — К.: Техника, 1988.

6. *Linger R.C., Mead N.R., Lipson H.F.* Requirements Definition for Survivable Network Systems. — http://www.cert.org/archive/pdf/icre.pdf

7. *Robert J. Ellison, David A. Fisher, Richard C. Linger, Howard F. Lipson, Thomas A. Longstaff, Nancy R. Mead.* Survivability: Protecting Your Critical Systems. — http://www.cert.org/archive/html/protect-critical-systems.html

Поступила в редакцию 08.09.2004