

## КОРПОРАТИВНЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ: ОБЕСПЕЧЕНИЕ ЖИВУЧЕСТИ

---

**Abstract:** Analysis of corporate information systems from the point of view of survivability maintenance is carried out. Tasks of survivability maintenance system for different components of corporate information systems are considered. Basic structure of survivability maintenance system for corporate information system is proposed.

**Key words:** corporate information system, survivability maintenance system, corporation, survivability, methods of survivability improving, structure of survivability maintenance system, hardware, software, infoware, information protection.

**Анотація:** Проводиться аналіз корпоративних інформаційних систем з точки зору забезпечення їх живучості. Розглядаються задачі системи забезпечення живучості для різних забезпечень корпоративної інформаційної системи. Запропонована базова структура системи забезпечення живучості корпоративної інформаційної системи.

**Ключові слова:** корпоративна інформаційна система, система забезпечення живучості, корпорація, живучість, методи підвищення живучості, структура системи забезпечення живучості, апаратне забезпечення, програмне забезпечення, інформаційне забезпечення, захист інформації.

**Аннотация:** Проводится анализ корпоративных информационных систем с точки зрения обеспечения их живучести. Рассматриваются задачи системы обеспечения живучести для различных обеспечений корпоративной информационной системы. Предложена базовая структура системы обеспечения живучести корпоративной информационной системы.

**Ключевые слова:** корпоративная информационная система, система обеспечения живучести, корпорация, живучесть, методы повышения живучести, структура системы обеспечения живучести, аппаратное обеспечение, программное обеспечение, информационное обеспечение, защита информации.

### 1. Введение

Одной из наиболее эффективных форм хозяйствования в условиях рыночной экономики является такая организационная форма предприятия, как корпорация, – целевое объединение предприятий для повышения эффективности их совместного функционирования. Деятельность любой современной корпорации базируется на информационных технологиях, где основной перерабатываемой продукцией является информация [1]. Особую роль среди информационных технологий играет технология организационного управления. Можно определить информационную технологию как методы обработки и организационно-управленческие концепции формирования и использования информации, а также совокупность всех видов информационной техники; единство процедур сбора, накопления, хранения, обработки и передачи данных с использованием определенного комплекса технических средств [2].

Поэтому наряду с понятием «корпорация» появилось и широко используется такое понятие, как «корпоративная информационная система» (КИС).

Строго сформулировать определение КИС достаточно сложно, так как слишком широким является само понятие «корпорация», поэтому в дальнейшем будем подразумевать, что рассматривается информационная система, пронизывающая все составляющие, которые определяют функционирование корпорации. В частности, КИС включает распределенный корпоративный комплекс технических средств, корпоративную коммуникационную сеть, распределенную корпоративную базу данных, корпоративную подсистему документооборота, корпоративную подсистему поддержки принятия решений и т.д. Другими словами, определим КИС

как комплексную систему методических, программно-аппаратных, информационных и организационных средств, обеспечивающих жизнедеятельность корпорации.

В современных условиях жизнедеятельность корпорации немислима без использования КИС. Неэффективная организация работы КИС грозит значительными убытками для корпорации. Поэтому одним из важнейших свойств, которыми должна обладать КИС, – это живучесть. КИС, обладающая свойством живучести, при возникновении нештатных ситуаций позволяет использовать необходимые элементы защиты своего функционирования и обеспечить стабильную работу корпорации [3].

В данной работе описаны основные пути придания КИС свойства живучести и приводится общее описание предназначенной для этого системы.

## **2. Свойство живучести КИС**

В классическом определении свойство живучести системы – это ее способность адаптироваться к новым изменившимся и, как правило, непредвиденным ситуациям, противостоять неблагоприятным воздействиям, выполняя при этом свою целевую функцию за счет соответствующего изменения структуры и поведения системы [2]. Живучесть можно рассматривать как свойство, характеризующее способность системы эффективно функционировать при получении повреждений (разрушений) или восстанавливать данную способность в течение заданного времени [4]. Другими словами, техническое, программное, информационное, методическое, лингвистическое и организационное обеспечение КИС должно содержать такие средства, которые позволили бы определенным образом отреагировать на возникновение ситуации, приводящей к ухудшению качества функционирования, и обеспечить сохранение работоспособности КИС.

Ввиду сложности задачи обеспечения живучести её решение разовыми конкретными мероприятиями невозможно. Необходима непрерывная направленная система определенных действий, которые выполнялись бы на всем протяжении жизненного цикла КИС [5]. Сложность придания КИС свойства живучести объясняется во многом еще и сложностью бизнес-процессов, протекающих в корпорации, и, как следствие, – сложностью современных информационных систем, которые предназначены для автоматизации этих бизнес-процессов.

В простейшем случае понятие живучести является синонимом отказоустойчивости, надежности и защиты аппаратных средств и программного обеспечения системы. Однако в полной мере свойство живучести проявляется тогда, когда исчерпываются ресурсы этих свойств. Таким образом, понятие живучести включает в себя понятия надежности, безопасности и отказоустойчивости, но не ограничивается этими понятиями.

Обеспечение живучести усложняется еще и потому, что в современных условиях современная система может сама порождать новые функции, которые не были заложены ни в техническом задании, ни в проекте системы, не говоря уже о неадекватной реакции на возникновение различных непредвиденных ситуаций. Это объясняется, например, такими факторами, как:

- значительная рассредоточенность аппаратных средств;
- многие рассредоточенные точки взаимодействия с пользователем;
- широкие возможности взаимодействия пользователя с системой;

- взаимодействие с другими автоматизированными системами;
- взаимодействие с системами с децентрализованным управлением и администрированием, такими, как Интернет.

В подобных условиях обеспечить живучесть КИС можно только специальными средствами, органически вписанными в саму КИС.

Рассмотрим подробнее критически важные места КИС, где должны в нужный момент вступать в действие средства обеспечения живучести.

С точки зрения структуры, КИС состоит из подсистем, каждая из которых имеет архитектурное строение самостоятельной системы (рис. 1) [5].



Рис. 1. Компоненты подсистемы КИС

Свойство живучести КИС должно дифференцироваться по каждой подсистеме и обеспечиваться на уровне каждой ее компоненты. При этом обеспечение живучести на уровне каждой компоненты подсистемы не должно проводиться автономно, без учета механизмов обеспечения

живучести для других компонент подсистемы и для КИС в целом.

Свойство живучести КИС предполагает наличие функционирующих по технологическому циклу, представленному на рис. 2, специальных средств обеспечения живучести для каждой компоненты системы.

Рассмотрим подробнее этапы этого технологического цикла:

*Сбор информации*

На этом этапе собирается информация двух типов:

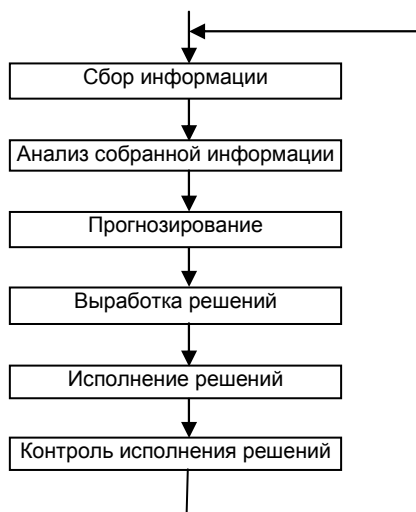


Рис. 2. Технологический цикл функционирования средств обеспечения живучести КИС

- 1) информация о внутреннем состоянии КИС, такая как статистика загруженности и сбоев аппаратного и программного обеспечения, наличие свободных ресурсов коммуникационных сетей, устройств хранения информации, целостность и непротиворечивость информации, хранимой в базах данных, и т.п.;
- 2) информация о внешней среде, в которой функционирует КИС, о воздействиях внешней среды на КИС и КИС на внешнюю среду. Собирается такая информация как статистика активных подключений к системе, информация, передаваемая из внешней среды в систему, информация, исходящая из системы во внешнюю

среду.

Вся собранная информация централизованно формализуется, классифицируется и подготавливается к следующему этапу.

#### *Анализ собранной информации*

Входными данными для этого этапа является собранная на первом этапе информация. Целью данного этапа является статистическая и экспертная обработка и анализ входных данных для получения оценки текущего состояния отдельных обеспечений, модулей и подсистем КИС, КИС в целом и внешней среды по некоторым специализированным критериям. Кроме того, оцениваются отклонения текущего состояния системы от предусмотренного проектом.

#### *Прогнозирование*

На этом этапе прогнозируется динамика изменения состояния обеспечений, программно-технических комплексов и подсистем КИС, а также КИС в целом. Кроме того, вырабатываются прогнозы изменения состояния внешней среды и ее взаимодействие с КИС. Прогнозирование выполняется на основе оценок текущих состояний КИС и внешней среды, а также отклонений КИС от проектного состояния, которые были получены на предыдущем этапе технологического цикла.

#### *Выработка решений*

На этом этапе происходит подготовка решений по противодействию внешним и внутренним неблагоприятным воздействиям как наблюдаемым, так и спрогнозированным на третьем этапе технологического цикла. Подготовленные решения могут определять меры как по реорганизации, реконфигурации и реконструкции внутреннего строения составляющих системы и системы в целом, так и меры по изменению порядка и правил взаимодействия с внешней средой, включая получение и предоставление информации. В первую очередь, система должна быть в состоянии вырабатывать превентивные решения на основании данных, полученных на этапе прогнозирования. Такие решения позволили бы избежать последствий большинства неблагоприятных воздействий на систему и обеспечить штатные условия ее функционирования.

#### *Исполнение решений*

На данном этапе специальными средствами обеспечения живучести производится исполнение решений, выработанных на предыдущем этапе технологического цикла КИС. Основными требованиями на этом этапе являются оперативность и надежность работы средств исполнения решений.

#### *Контроль исполнения решений*

Заключительным этапом технологического цикла функционирования средств обеспечения живучести КИС является контроль исполнения решений. На этом этапе анализируется качество исполнения решений и собираются первичные данные о реакции внутренней и внешней среды КИС на эти решения. На базе этих данных за несколько итераций технологического цикла может проводиться адаптация КИС и ее средств обеспечения живучести к новым условиям функционирования.

Средства обеспечения живучести КИС должны функционировать постоянно и непрерывно. Это требование определяется постоянным изменением условий функционирования КИС и

возникновением непредвиденных воздействий как со стороны внешней, так и внутренней среды КИС.

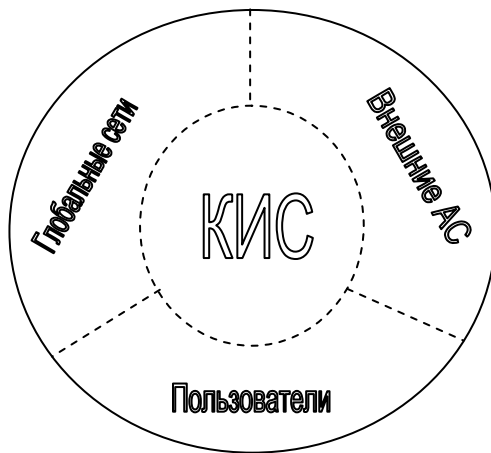


Рис. 3. Внешняя среда функционирования

Для определения и систематизации средств обеспечения живучести необходимо, в первую очередь, рассмотреть технологический процесс функционирования КИС. Само понятие «корпоративная информационная система» предполагает наличие внешней среды и взаимодействия с ней (рис. 3). Понятие «внешняя среда» включает в себя:

- глобальные сети, к которым подключена КИС, т.е. сети, соединенные с КИС некоторыми каналами связи, но не подчиняющиеся внутренней административной политике КИС;

- пользователей системы как внешних, взаимодействующих с системой посредством глобальных сетей, точки входа которых не подчиняются внутренней административной политике КИС, так и внутренних, точки входа которых являются частью внутренней сети КИС и полностью подчиняются ее административной политике;

- внешние автоматизированные системы, с которыми взаимодействует КИС, например, информационные системы корпораций-партнеров, которые имеют свою внутреннюю административную политику, не совпадающую с административной политикой КИС.

КИС не функционирует автономно, она является как потребителем, так и поставщиком информации по отношению к внешней среде. Таким образом, КИС можно представить как информационную резервацию, обладающую внутренними информационными потоками, бизнес-правилами, подчиняющуюся определенной административной политике. Внешняя среда, в которой функционирует такая информационная резервация, не подчиняется ее административной политике и таким образом может вырабатывать негативные или непредвиденные воздействия на КИС, а также негативно или непредвиденно реагировать на воздействия КИС на нее. Для обеспечения живучести КИС необходимо, с одной стороны, контролировать и корректировать ее взаимодействие с внешней средой (реакцию КИС на воздействия внешней среды, реакцию КИС на последствия ее воздействий на внешнюю среду). А, с другой стороны, необходимо контролировать и корректировать внутреннее состояние КИС, связанное с функционированием аппаратного и программного обеспечения и состоянием информационного обеспечения. Для определения путей построения системы обеспечения живучести КИС рассмотрим, прежде всего, типовой технологический процесс функционирования КИС.

Упрощенно технологический процесс функционирования КИС может быть представлен следующей схемой (рис. 4):

На этой схеме показаны ключевые объекты, по отношению к которым должны применяться средства обеспечения живучести:

1. Входящая информация.
2. Процесс обработки информации.
3. Процесс хранения информации.
4. Исходящая информация.

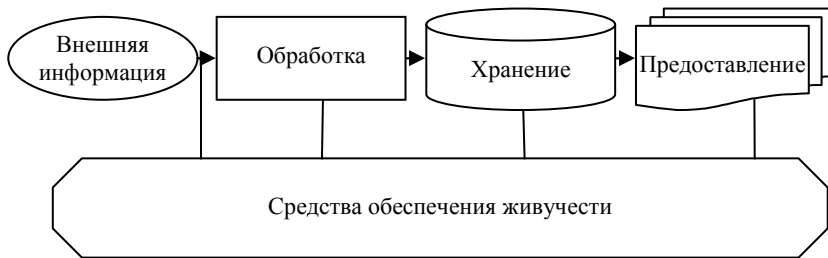


Рис. 4. Применение средств обеспечения живучести в технологическом процессе функционирования КИС

Таким образом, свойство живучести придает КИС непрерывной направленной системой определенных действий на всех этапах ее жизненного цикла. На этапе создания КИС разрабатываются специальные средства обеспечения

живучести, органически интегрируемые в КИС. В дальнейшем будем говорить о них как о системе обеспечения живучести (СОЖ) КИС. Свойство живучести КИС базируется на решении задач обеспечения живучести каждой компоненты КИС с целью достижения стабильного технологического процесса функционирования КИС в целом. Ниже будут рассмотрены задачи, которые должна решать система обеспечения живучести КИС.

### 3. Задачи системы обеспечения живучести КИС

Определим понятие «обеспечение» живучести, поскольку в литературе в основном встречается понятие «повышение» живучести. Дело в том, что речь идет о системе обеспечения живучести в составе КИС (фактически подсистеме КИС), создаваемой одновременно с КИС с самого начала её построения [5]. То есть все, что обеспечивает живучесть КИС, выполняется в рамках системы обеспечения живучести. Термин «повышение» живучести правомерно употребляется тогда, когда КИС уже создана и функционирует, т.е. уже обладает более или менее развитым свойством живучести. В этом случае применяются дополнительные методы и средства по повышению живучести КИС, не предусмотренные ранее в плане развития системы обеспечения живучести, т.е. требующие внесения изменений в обеспечение подсистем КИС или технологический цикл функционирования КИС. Развитие системы обеспечения живучести тоже можно трактовать как повышение живучести КИС.

Разделим задачи системы обеспечения живучести на две группы:



Рис. 4. Применение средств обеспечения живучести в технологическом процессе

1. Предотвращение возникновения нештатных ситуаций.
2. Обеспечение выхода из нештатных ситуаций.

К первой группе относятся задачи анализа и, в случае необходимости, коррекции функционирования КИС с целью обеспечения ее стабильной работы. Вторая группа задач – это обеспечение выхода из нештатной ситуации, если таковая все же случилась, на основе методов реконфигурации, реконструкции, реорганизации и адаптации.

В настоящей главе будут подробно рассмотрены методы и средства решения задач первой группы. Общий подход к решению задач второй группы и пример решения типовой частной задачи обеспечения живучести при разрушении каналов связи изложены в [3, 7]. Предотвращение возникновения нештатных ситуаций решается как двуединая задача при создании КИС: во-первых, это наличие у разработчика современной системы управления качеством создаваемой продукции и получение соответствующего сертификата качества на разработанную КИС, а во-вторых, это разработка специальных аппаратно-программных средств СОЖ как подсистемы КИС, позволяющих службе администрирования КИС проводить профилактику нештатных ситуаций.

Решение задач первой группы обеспечивается следующими функциями СОЖ:

1. Защита:

- защита от негативных воздействий входящей информации;
- защита от несанкционированных воздействий обслуживающего персонала;
- защита от несанкционированных воздействий внешней среды;
- защита от неисправностей и сбоев аппаратуры;
- защита от неисправностей и сбоев программного обеспечения;

2. Поддержка функционирования:

- поддержка процессов взаимодействия с внешней средой;
- поддержка процессов накопления информации;
- поддержка процессов обработки информации;
- поддержка технологии хранения данных;
- поддержка внутренних информационных потоков КИС;

3. Корректировка отклонений:

- реорганизация;
- реконфигурация;
- реконструкция;
- адаптация.

Функции корректировки отклонений в основном служат для решения задач второй группы путем нормализации состояния системы.

Рассмотрим задачи СОЖ для основных видов обеспечения КИС.

*Задачи по обеспечению живучести технического обеспечения КИС*

Техническое обеспечение КИС включает в себя:

1. Устройства хранения информации.
2. Аппаратное обеспечение серверов обработки информации.

3. Аппаратное обеспечение рабочих мест пользователей системы.
4. Коммуникационные каналы и оборудование для передачи информации.

Задачей СОЖ для технического обеспечения является профилактика и предотвращение сбоев его компонентов и минимизация влияния возможных сбоев на функционирование системы. СОЖ должна обеспечивать постоянное наблюдение за состоянием всех составляющих технического обеспечения системы, прогнозировать возможные сбои и заранее применять меры по выходу из сложившейся ситуации.

Для обеспечения прогнозирования сбоев необходимо, во-первых, производить проверку корректности функционирования всех компонентов технического обеспечения, например, проводить регулярные проверки поверхностей дисков, запоминающих элементов оперативной памяти и т.п. Во-вторых, практически все современные устройства предоставляют достаточно полную информацию о своем состоянии, такую как температура и скорость вращения дисков, температура и тактовая частота процессоров, скорость вращения охлаждающих вентиляторов и т.п. Анализ динамики изменения такой информации позволит выявлять ее возможные отклонения от нормы и заранее принимать меры по корректировке.

Кроме того, все техническое обеспечение имеет определенный ресурс, определяемый производителем. СОЖ должна отслеживать остаток ресурса для всех компонентов технического обеспечения и своевременно предоставлять информацию о необходимости замены или восстановления.

Для минимизации негативного влияния возможных сбоев аппаратного обеспечения СОЖ должна обеспечивать постоянную готовность системы к возможной реорганизации, реконфигурации и реконструкции системы. Например, при повышении вероятности выхода из строя некоторого устройства хранения информации должна быть сделана его зеркальная копия на другом, возможно, более медленном устройстве или на свободных участках других устройств. При повышении вероятности выхода из строя некоторого сервера обработки информации СОЖ должна, по возможности, максимально разгрузить этот сервер за счет неиспользуемых резервных ресурсов КИС, тем самым подготовив его к ремонту или замене.

#### *Задачи по обеспечению живучести программного обеспечения КИС*

Программное обеспечение КИС включает в себя:

1. Системное программное обеспечение.
2. Прикладное программное обеспечение.
3. Серверы управления базами данных.
4. Экспертные системы.
5. Аналитические информационные системы.
6. Системы планирования и контроля.

Задачей СОЖ для программного обеспечения является контроль корректности работы программного обеспечения и минимизация ущерба функционированию системы, наносимого возможными ошибками в программных модулях. В данном случае задачи СОЖ можно разделить на два подмножества:



1. Контроль качества программного обеспечения (проводится на этапе разработки и сопровождения).

2. Контроль целостности программных модулей, которые исполняются в системе.

Задачи первого подмножества предполагают наличие системы оценки качества разработки программного обеспечения. Этот процесс должен включать в себя такие работы, как автоматизированное тестирование, верификация, валидация, совместные просмотры. Программное обеспечение, разрабатываемое и выбираемое для построения КИС, должно гарантировать надежность функционирования, корректную обработку ошибочных ситуаций, давать средства для мониторинга его функционирования.

Задачи второго подмножества предполагают наличие инструментария для наблюдения за процессом функционирования программного обеспечения и его корректировки. СОЖ должна обеспечивать контроль цифровых подписей и контрольных сумм программных модулей, установленных на серверах и рабочих станциях КИС, наличие только предусмотренных программных пакетов на серверах КИС, соответствие набора операций, исполняемых программными модулями, утвержденным шаблонам. Кроме того, СОЖ должна обеспечивать выполнение политики обновлений программного обеспечения, входящего в состав КИС.

При обнаружении некорректности функционирования или состава программного обеспечения некоторого узла КИС СОЖ должна изолировать его, проведя реконфигурацию и реорганизацию системы, а также реконструкцию функций этого узла за счет свободных ресурсов других узлов системы, подготовив его к восстановлению программного обеспечения и выяснению причин нарушения его целостности. Кроме того, СОЖ должна подготовить другие узлы, содержащие похожие наборы программного обеспечения к возможной изоляции или обновлению в случае возникновения в них схожих проблем.

#### *Задачи по обеспечению живучести информационного обеспечения КИС*

Информационное обеспечение – это информация, хранимая, обрабатываемая и циркулирующая в КИС. Вся информация, находящаяся в системе, может быть разделена на так называемую «полезную» (знания, получаемые, обрабатываемые и хранимые в системе) и «технологическую» (управляющая информация, внутренние таблицы маршрутизации и т.п.).

Целью СОЖ информационного обеспечения является обеспечение безопасности хранимой и обрабатываемой в системе информации и обеспечение безопасности КИС и ее внешней среды при работе с этой информацией.

Для информационного обеспечения задачи СОЖ делятся на три подмножества:

1. Фильтрация входящей информации с целью отсеивания информации, не удовлетворяющей требованиям интерфейса (эта информация накапливается для дальнейшего анализа).

2. Фильтрация исходящей информации путем цензурирования с целью отсеивания неблагоприятной для внешнего мира информации.

3. Обеспечение безопасности хранимой и циркулирующей в системе информации и восстановление ее в случае сбоев.

Задачи первого подмножества предполагают наличие развитого периметра безопасности, обладающего как централизованным, так и децентрализованным управлением, который был бы в состоянии производить оценки входящей информации (служебной и «полезной») и исключать информацию небезопасного содержания. Оценки входящей информации должны производиться на базе внутренней административной политики КИС, сигнатур вредоносного программного обеспечения, шаблонов поведения вредоносного программного обеспечения и т.п.

Частично решение задач второго подмножества может базироваться на обеспечении безопасности конфиденциальной информации, однако такие методы, во-первых, не покроют весь класс задач, а, во-вторых, потребуют значительных затрат и, таким образом, будут неприемлемыми. В данном случае выбор методов защиты должен базироваться на том, что неблагоприятная для внешней среды информация не добывается ею целенаправленно, с помощью специальных средств. Действенным методом в этом случае будет создание средств цензурирования информации, попадающей во внешнюю информационную среду. Причем правила цензурирования должны постоянно дополняться на основе реакции внешней среды на исходящую из системы информацию.

Задачи третьего подмножества предполагают структурирование всей информации, находящейся в системе, с точки зрения требований по ее доступности, а также связей между различными блоками информации:

- необходимо выделить некоторое множество критической информации, которая должна быть доступна в любой ситуации. Для остальной информации необходимо задать максимальное время доступа, которое может зависеть от текущей ситуации (штатная, нештатная и т.п.). При потерях информации необходимо обеспечить возможность частичного (или полного) восстановления информации на основе оставшейся. Минимизировать «косвенные» потери, т.е. невозможность использования информации, связанной с утерянной, из-за несамодостаточности оставшейся информации;

- информация, хранимая в КИС, должна быть ранжирована по уровню важности. К условиям хранения и обработки наиболее важной информации должны быть предъявлены особые требования. Кроме того, информация может быть ранжирована по максимальному времени доступа к ней в различных ситуациях;

- выделение связей между данными позволит сформировать требования к хранению различных блоков информации, предотвратить возможные «косвенные» потери информации, выработать рациональный подход к внесению избыточности при хранении данных в КИС.

#### **4. Общая структура системы обеспечения живучести КИС**

Достижение системой обеспечения живучести (СОЖ) своей цели – формирование условий функционирования КИС для выполнения ею своей основной функции, требует, прежде всего, анализа и контроля состояния КИС в режиме реального времени. Реализуется это двумя путями:

1. Оперативным получением информации и выработкой управляющих воздействий в критических, с точки зрения возможности возникновения нештатных ситуаций, точках технологического цикла функционирования КИС.

2. Регулярным целенаправленным анализом, контролем и корректировкой состояния программного и информационного обеспечений КИС.

Оперативное получение информации обеспечивается включением специальных «резидентных» программ (фильтров) СОЖ как в операционную систему (ОС), так и в программное обеспечение подсистем КИС. Включение фильтров СОЖ в ОС выполняется с использованием предоставляемых ОС интерфейсов. В качестве примеров таких программ можно назвать фильтры файловых систем, сетевые фильтры, перехватчики системных вызовов.

Включение «резидентных» программ СОЖ в программное и информационное обеспечение подсистемы КИС выполняется непосредственно при разработке КИС в соответствии с ее техническим проектом. Как уже было отмечено выше, СОЖ – это часть КИС, разрабатываемая одновременно с КИС, и разработка всех видов обеспечений КИС должна учитывать требования технического проекта СОЖ.

Анализ, контроль и корректировка состояния КИС, с точки зрения возможного отклонения от штатного режима функционирования, проводятся специализированными программно-методическими комплексами (ПМК) по направлениям:

- а) пакеты исполняемых программных модулей;
- б) базы данных;
- в) протоколы работы программного обеспечения;
- г) журналы событий ОС;
- д) статистика загрузки каналов связи;
- е) статистика сбоев каналов связи;
- ж) статистика загрузки аппаратного обеспечения;
- з) статистика сбоев аппаратного обеспечения;
- и) входные данные;
- к) выходные данные.

Все задачи СОЖ целесообразно условно разделить на группы и строить СОЖ в виде взаимодействующих подсистем, каждая из которых предназначена для решения конкретной группы задач. Например, целесообразно вынести в отдельную группу задачи технической защиты информации или задачи защиты от возникновения нештатных ситуаций, которые могут привести к искажению информационного или программного обеспечения и тем самым косвенно или прямо повлечь ухудшение качества функционирования КИС. Четкое разделение СОЖ на подсистемы по типам задач упростит логику как СОЖ, так и КИС, и тем самым повысит ее надежность, уменьшит трудоемкость разработки, сроки создания и стоимость, а в дальнейшем облегчит и сопровождение эксплуатации КИС.

Решение задач обеспечения выхода из нештатных ситуаций выполняют специализированные ПМК, например, такой, как описан в [7]. Общий подход к разработке алгоритмов этого класса ПМК описан в [3].

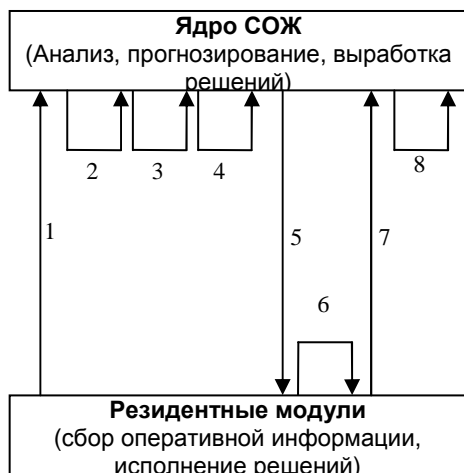
Функционально СОЖ состоит из двух основных блоков:

- а) ядро СОЖ, отвечающее за анализ собранной информации, прогнозирование, выработку решений и контроль исполнения решений;

б) блок «резидентных» модулей, интегрированных в аппаратное и программное обеспечение КИС и отвечающих за сбор оперативной информации и исполнение решений, выработанных ядром СОЖ.

На рис. 5 показана диаграмма взаимодействия блоков СОЖ.

Ядро СОЖ включает следующие программно-методические комплексы (ПМК):



1. Предоставление оперативной информации.
2. Анализ.
3. Прогнозирование.
4. Выработка решений.
5. Выдача решений.
6. Исполнение решений.
7. Предоставление оперативной информации.
8. Контроль качества исполнения решений.

1) ПМК взаимодействия с резидентными модулями, предназначенный для получения предоставляемой ими информации и передачи ее другим ПМК ядра;

2) ПМК анализа полученной от резидентных модулей информации, предназначенный для оценки текущего состояния системы и влияния на него выработанных решений;

Рис. 5. Диаграмма взаимодействия блоков СОЖ

3) ПМК прогнозирования динамики состояния системы на базе статистики и анализа текущего состояния;

4) ПМК выработки решений на базе полученных прогнозов;

5) ПМК взаимодействия с администратором, обеспечивающий возможность административного управления и конфигурирования СОЖ в целом; и использует специализированные базы данных:

1) база статистики, которая ведется и используется ПМК анализа, прогнозирования и выработки решений;

2) база настроек и правил, которая ведется ПМК взаимодействия с администратором и используется для конфигурирования ПМК, входящих в состав ядра СОЖ и резидентных модулей.

На рис. 6 представлена структурная схема ядра СОЖ.

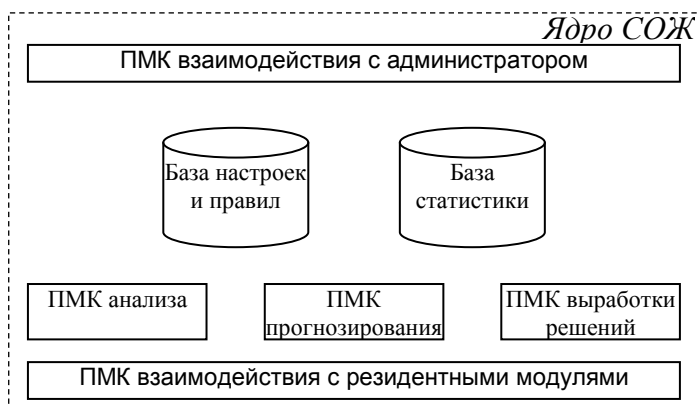


Рис. 6. Структурная схема ядра СОЖ

Блок резидентных модулей содержит компоненты, интегрированные в программно-аппаратные комплексы КИС, обеспечивающие:

- взаимодействие с внешней средой;
- обработку данных;
- хранение информации;
- передачу информации в пределах КИС.

Одной из главных задач СОЖ

является обеспечение адаптации КИС к условиям эксплуатации. Информационной основой адаптации является статистика частоты и времени выполнения программных модулей, доступа к базам данных, загрузки каналов связи, сбоев аппаратного обеспечения и т.д. Учет статистики позволяет перераспределять ресурсы КИС, графики выполнения программ контроля состояния КИС, дополнить базу данных СОЖ новыми правилами и т.д.

## 5. Заключение

В настоящее время информационные технологии вышли на достаточный уровень для того, чтобы разработка КИС могла не начинаться с нуля. Существует множество профессионально разработанных готовых решений, которые могут быть использованы при автоматизации бизнес-процессов корпорации. Из этого множества всегда можно выбрать наиболее подходящее решение и адаптировать его под конкретные нужды. Такой подход значительно удешевляет разработку и дает гарантии ее успешного и своевременного завершения. Существует множество готовых компонентов, таких, как СУБД, ОС, системы хранения данных, которые можно применять при построении новой КИС.

Таким образом, все современные, профессионально разработанные КИС обладают схожей структурой, состоят из схожих компонентов, обладают схожим технологическим циклом и выполняют схожие функции. СОЖ для таких КИС также будут обладать общими чертами. Это обстоятельство позволяет разработать шаблонное решение для СОЖ, описать ее типовые задачи, структуру, методику построения, а также определить средства, входящие в ее состав.

Однако каждая корпорация является по-своему уникальной, обладающей специфичными только для нее чертами. Это является залогом ее конкурентоспособности. Такая уникальность требует построения КИС для каждой корпорации индивидуально, что, в свою очередь, требует индивидуального подхода к разработке СОЖ для каждой конкретной КИС. СОЖ должна разрабатываться непрерывно и параллельно с КИС и в полной мере учитывать ее специфику. Только при этом условии можно достичь максимально эффективного функционирования СОЖ, КИС и корпорации в целом.

## СПИСОК ЛИТЕРАТУРЫ

1. Глушков В.М. Основы безбумажной информатики. – 2-е изд. – М.: Наука. Гл.ред. физ.-мат. лит., 1987. – 552 с.
2. Додонов А.Г., Горбачик Е.С., Кузнецова М.Г. Живучесть информационно-аналитических систем в аспекте информационной безопасности // Збірник наукових праць «Інформаційні технології та безпека». – 2003. – Вип. 4. – С. 27– 31.
3. Додонов А.Г., Флейтман Д.В. К вопросу живучести корпоративных информационных систем // Реєстрація, зберігання і обробка даних. – 2004. – Т. 6, № 2. – С. 33 – 41.
4. Стекольников Ю.И. Живучесть систем. Теоретические основы.–Санкт-Петербург: Политехника, 2002.– 155 с.
5. Флейтман Д.В. Жизненный цикл и живучесть корпоративных информационных систем // Реєстрація, зберігання і обробка даних. – 2004. – Т. 6, № 3. – С. 74 – 84.
6. Додонов А.Г., Флейтман Д.В. К вопросу безопасности информационных систем // Збірник наукових праць «Інформаційні технології та безпека». – 2004. – Вип. 6. – С. 26 – 29.
7. Флейтман Д.В. Решение задачи обеспечения живучести корпоративных информационных систем при частичном разрушении каналов связи // Реєстрація, зберігання і обробка даних. – 2005. – Т. 7, №1. – С. 52– 61.
8. Проектирование Информационных систем: Посібник / За ред. В.С. Пономаренка. – К.: Академія, 2002. – 488 с.