УДК 654.1(045)

В.М. Чуприн, Г.Ф. Конахович, В.Г. Потапов, А.Н. Сухопара

ПРИНЦИП ПОСТРОЕНИЯ СИСТЕМ УПРАВЛЕНИЯ КОМПЛЕКСАМИ СРЕДСТВ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ В ЦИФРОВЫХ КОММУТАЦИОННЫХ СИСТЕМАХ СВЯЗИ

Рассмотрена проблема создания систем управления комплексами средств технической защиты информации с целью поддержания заданного уровня защищенности информационных ресурсов цифровых коммутационных систем связи. Предложена адаптивная схема управления такими комплексами.

Одним из основных принципов технической защиты информации (ТЗИ) является принцип непрерывности защиты, в соответствии с которым требуемый уровень защищенности информационных ресурсов цифровой коммутационной системы (ЦКС) необходимо поддерживать на всех стадиях ее жизненного цикла, т.е. на всех этапах обработки вызовов, во всех режимах функционирования и предоставления услуг связи [1]. Стадия создания систем ТЗИ, обеспечивающих заданный уровень защищенности ЦКС, регламентирована национальной нормативной базой Украины (см., например, документ [2]), а для стадии технической эксплуатации соответствующие нормативные документы (НД) отсутствуют. Однако в реальных условиях эксплуатации среда функционирования ЦКС с позиций ТЗИ подвергается существенным текущим изменениям (например, выполняется текущая реконфигурация программно-аппаратных средств системы, изменяются состав и полномочия пользователей, меняются элементы технологической среды функционирования ЦКС, параметры модели угроз для информации, характеристики моделей нарушителей и т.д.). Поэтому, если даже в какие-либо дискретные моменты периода эксплуатации t_i, $i = 1,\ldots, n$ в результате известных организационно-технических мероприятий [2] защищенность ЦКС и будет соответствовать требуемому нормативному уровню (например, уровню доверия Е3 [3], [4]), то в промежутках между t_i можно с уверенностью предположить, что текущий уровень защищенности будет существенно отличаться от требуемого нормативного уровня. Следовательно, защита ЦКС должна предусматривать создание систем управления (СУ) комплексами средств (КС) ТЗИ, позволяющих осуществлять непрерывный контроль эффективности защиты и поддержку заданного уровня защищенности информационных ресурсов ЦКС.

В качестве методологической основы используемого здесь подхода к построению СУ КС ТЗИ в ЦКС приняты единые (унифицированные) для Европейского Союза "Критерии оценки безопасности систем информационной техники" (ITSEC, версия 1.2), отраженные в украинских НД ТЗИ [1]– [4] применительно к ЦКС.

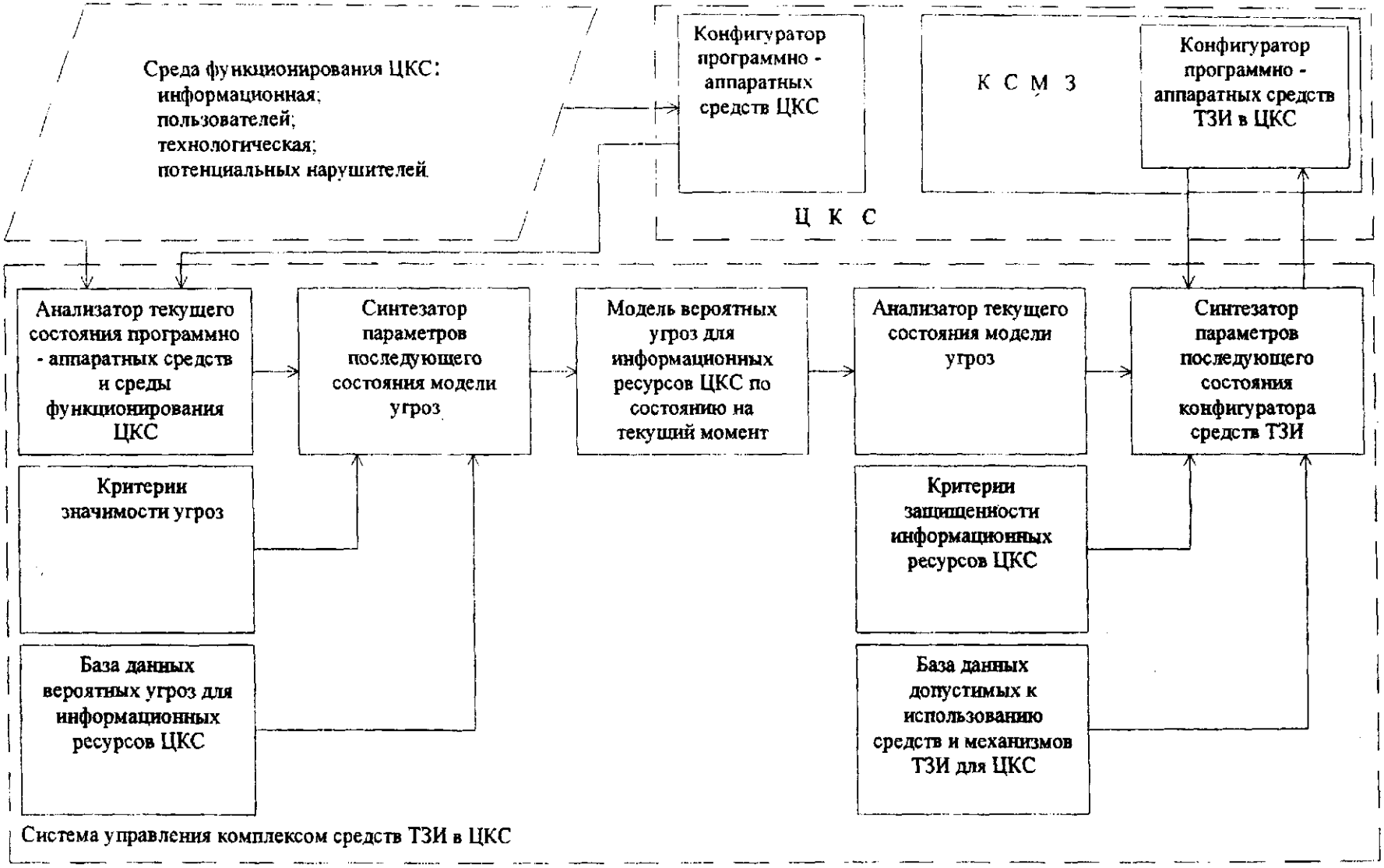
Согласно принятой в вышеназванных документах методологии рассматриваются три основных вида программно реализуемых логически связанных объектов: конфигуратор программно-аппаратных средств (ПАС) защищаемой ЦКС, модель вероятных угроз (МВУ) для информации в ЦКС и конфигуратор ПАС комплекса средств и механизмов защиты (КСМЗ), используемого в защищаемой ЦКС с целью обеспечения заданного уровня защищенности ее информационных ресурсов.

Суть предлагаемого способа построения СУ КС ТЗИ заключается в реализации процессов адаптации, которые поддерживают в реальном времени взаимное соответствие конкретных выборок совокупностей параметров и их значений вышеназванных трех логически связанных объектов на стадии эксплуатации защищаемой ЦКС.

Принцип действия СУ заключается в следующем (см. рисунок). Любое значимое изменение среды функционирования ЦКС в соответствии с принятой технологией эксплуатации отражается в конфигураторе ПАС ЦКС. Как правило, такие изменения в конфигураторе выполняет обслуживающий персонал через системную консоль. Любое изменение аппаратных и программных ЦКС, параметров настроек программных и аппаратных модулей, процессов, режимов и других ресурсов ЦКС (например, пропускной способности и т.п.) регистрируется в конфигураторе ПАС ЦКС и затем адекватно отражается в изменениях МВУ. Для этого информация об изменениях в состоянии конфигуратора и в среде функционирования ЦКС поступает на вход анализатора текущего состояния ПАС и среды функционирования ЦКС. Анализатор отбирает информацию о тех параметрах среды и конфигуратора, которые влияют на изменения вероятностей проявления угроз (т.е., на защищенность информации в ЦКС). Эта информация используется синтезатором параметров МВУ с целью определения состояния модели угроз на последующий момент времени. Чтобы принять решение о необходимости изменений в МВУ, синтезатор также должен использовать соответствующим образом структурированную информацию о критериях значимости угроз и о всех вероятных угрозах для информационных ресурсов ЦКС на всем множестве состояний среды функционирования ЦКС и конфигуратора программно-аппаратных средств ЦКС.

В результате, если какие-либо параметры среды или конфигуратора (именно те параметры, которые приводят к образованию новых или устранению учитываемых каналов утечки или специальных воздействий на информацию) существенно изменяются (с позиций принятых в СУ критериев значимости угроз), то на выходе синтезатора появится информация, адаптирующая МВУ под новые условия среды функционирования ЦКС и новое состояние конфигуратора. Однако в случае изменений в МВУ, возникнет несоответствие в состояниях МВУ и конфигуратора ПАС ТЗИ, настроенного на прежнее состояние модели угроз. Поэтому с помощью анализатора текущего состояния МВУ и синтезатора параметров последующего состояния конфигуратора ПАС ТЗИ возникшее несоответствие устраняется. Процесс принятия решений синтезатором осуществляется на основе принятых в Украине критериев защищенности информационных ресурсов ЦКС, отраженных в НД [3], [4]. Кроме того, для принятия решений синтезатор должен обладать информацией о средствах и механизмах ТЗИ, допустимых к использованию на защищаемой ЦКС. Таким образом, под обновленный вариант МВУ выполняется адаптация КСМЗ с тем, чтобы в любой текущий момент времени обеспечивался заданный уровень защищенности информационных ресурсов ЦКС.

Перед созданием СУ КС ТЗИ необходимо убедиться, что процесс эксплуатации поддерживается соответствующими инструментальными средствами, подсистемой управления конфигурацией ПАС ЦКС и корректными процедурами инсталляции / деинсталляции как элементов, так и всей ЦКС в целом. Необходимо предоставить ведомость конфигурации поставленных ПАС, идентифицирующую комплект поставки защищаемой ЦКС и номер



Структура системы управления комплексом средств ТЗИ

версии поставленного программного обеспечения (ПО). В ведомости конфигурации следует учитывать все программные и аппаратные (технические) компоненты, из которых состоит защищаемая ЦКС. Кроме того, в случае если имеются изменения относительно поставленной конфигурации, предоставляют ведомость текущей конфигурации (или ведомость изменений конфигурации). Все аппаратные компоненты (вплоть до типовых элементов замены), техническая и организационно-распорядительная документация, включая справочники, программные модули, конструкторские чертежи и электрические принципиальные схемы ЦКС, однозначно идентифицируют. Применение этой идентификации обязательно.

Подсистема управления конфигурацией должна обеспечивать в реальном времени соответствие между текущей конфигурацией ПАС ЦКС и текущим состоянием организационно-распорядительной документации (и другой эксплуатационной документации, например, ведомости текущей конфигурации), сопровождающей процесс эксплуатации защищаемой ЦКС. Оборудование подсистемы управления конфигурацией должно находиться в состоянии наблюдать и протоколировать изменения (отличия) между различными версиями (типами) объектов, которые подвергаются конфигурационному контролю. Все объекты, которые возникают в процесс эксплуатации ЦКС, а также все изменения этих объектов подлежат конфигурационному контролю. Средства конфигурационного контроля должны иметь возможность поддерживать создание и обслуживание переменных связей между всеми контролируемыми объектами, а также возможность отображения вместе с параметрами изменяемого объекта всех других объектов, которых касается это изменение.

Организация, эксплуатирующая ЦКС, разрабатывает и утверждает МВУ ее информационным ресурсам, которая учитывает специфику конкретных условий ее применения (см., например, НД [2]). Модель вероятностных угроз должна содержать описание совокупности значимых угроз информационным ресурсам, способов и средств их проявления, а также указание уровней предельно допустимых потерь, связанных с возможными проявлениями этих угроз. В качестве нарушителей правил разграничения доступа рассматриваются субъекты, которые осуществляют преднамеренные или случайные воздействия на информационные ресурсы ЦКС, а также случайные события, в результате наступления которых возможны реализации угроз. Способы и средства осуществления угроз удобно отображать в терминах модели нарушителей, под которой понимается описание вероятных действий нарушителей, уровней их полномочий, ресурсных возможностей, используемых ими программных и технических средств.

Список литературы

1. НД ТЗИ 1.1-001-99. Техническая защита информации в программно-управляемых АТС общего пользования. Основные положения. – Введ. 01.07.1999.

2. НД ТЗИ 2.7-001-99. Техническая защита информации в программно-управляемых АТС общего пользования. Порядок выполнения работ. – Введ. 01.07.1999.

3. НД ТЗИ 2.3-001-99. Техническая защита информации в программно-управляемых АТС общего пользования. Методика защиты информации (базовая). – Введ. 01.07.1999.

4. НД ТЗИ 2.5-001-99. Техническая защита информации в программно-управляемых АТС общего пользования. Спецификации доверительных оценок корректности защиты. – Введ. 01.07.1999.

Стаття надійшла до редакції 27 вересня 1999 року.