УДК 004.621:654.1 **Пискун И.В., Хорошко В.А. (ГУИКТ)**

ПРИНЦИПЫ УПРАВЛЕНИЯ ТЕХНИЧЕСКОЙ ЗАЩИТОЙ ИНФОРМАЦИИ В СИСТЕМАХ СВЯЗИ

Рассматриваются проблемы создания систем управления комплексами средств технической защиты информации с целью поддержания заданного уровня защищенности информационных ресурсов систем связи.

Введение

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]. Процесс создания систем ТЗИ, обеспечивающих заданный уровень защищенности ЦКС, регламентирован нормативной базой Украины [2], а для этапа технической эксплуатации соответствующие нормативные документы (НД) отсутствуют. Однако в реальных условиях эксплуатации среда функционирования ЦКС с позиций ТЗИ подвергается существенным текущим изменениям (например, выполнятся текущая реконфигурация программно-аппаратных средств системы, изменяется состав 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 стадии эксплуатации t_i , i = 1,…, n в результате известных организационно-технических мероприятий [2] защищенность ЦКС и будет соответствовать требуемому нормативному уровню (например, 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.

Основная часть

Опыт применения систем защиты показывает, что эффективной может быть лишь комплексная система защиты информации и объекта, сочетающая следующие меры:

1.**Законодательные.** Использование законодательных актов, регламентирующих права и обязанности физических и юридических лиц, а также государства в области ЗИ.

2. Морально-этические. Создание и поддержание на объекте такой моральной атмосферы, в которой нарушение регламентированных правил поведения оценивалось бы большинством сотрудников как негативное.

3. Физические. Создание физических препятствий для доступа посторонних лиц и охраняемой информации.

4. Административные. Организация соответствующего режима секретности, пропускного и внутреннего режима.

5. Технические. Применение электронных и других устройств для защиты информации.

6. Криптографические. Шифрования и кодирования для сокрытия обрабатываемой и передаваемой информации от несанкционированного доступа.

7. **Программные.** Применение программных средств разграничения доступа.

Обоснованный выбор требуемого уровня защиты информации является системообразующей задачей, после как занижения, так и завышения уровня неизменно ведет к потерям ее. При этом роль данного вопроса резко возросла в связи с тем, что, во-первых, теперь в число защищаемых помимо военных, государственных и ведомственных, включены

также секреты промышленные, коммерческие и даже личностные, а во-вторых, сама информация все больше становится товаром.

Сегодня методы и средства несанкционированного получения систем связи пробрели такую популярность, что нередко само понятие "защита информации" применяется исключительно в смысле защиты информации от утечки через компьютерные сети. Некоторые специалисты по ТЗИ склонны выделить утечку информации через информационные сети в отдельный канал, равноценный другим техническим каналам утечки информации. Однако, в отличие от таких технических каналов, как радиоканал или акустический канал, утечка информации из систем связи является следствием не побочных, нежелательных процессов, вызванных конструктивными особенностями аппаратных средств и неучтенных разработчиками, а основных, штатных процессов, выполняющих в ЦКС.

Конечно, в определенном смысле утечка информации из ЦКС также возникает вследствие несовершенства программно-аппаратных решений, реализованных в системе связи. Но, тем не менее, пользуясь подобными изъянами в архитектуре ЦКС, злоумышленник все же использует ее ресурсы и процессы по прямому назначению.

В качестве методологической основы используемого здесь подхода к построению СУ КС ТЗИ в ЦКС принятые единые (унифицированные) для Европейского Союза "Критерии оценки безопасности систем информационной техники" (ITSEC, версия 1.2), отраженные в HD ТЗИ [1] - [5] применительно к ЦКС.

Согласно принятой в вышеназваных 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 и информационных ресурсов.

Суть предлагаемого способа построения СУ КС ТЗИ заключается в реализации процессов адаптации, которые поддерживают в реальном масштабе времени взаимное соответствие конкретных выборок совокупностей параметров и их значений вышеназванных трех логически связанных объектов на стадии запрещаемой 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 (пропускной способности 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 поступит 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, возникает несоответствие в состояниях МВУ и конфигуратора ПАС ТЗИ, настроенного на прежнее состояние модели угроз.

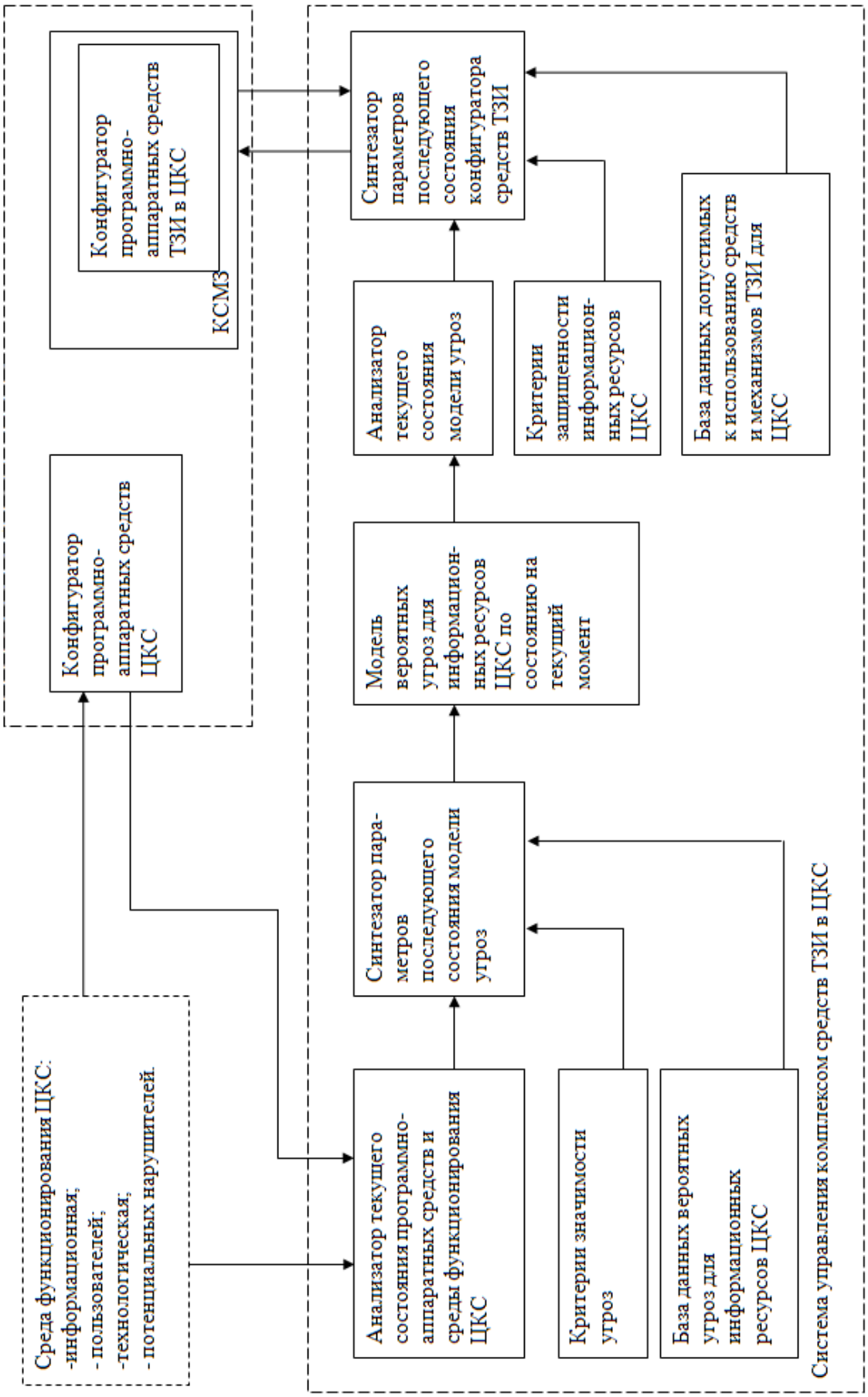
Поэтому с помощью анализатора текущего состояния МВУ и синтезатора параметров последующего состояния конфигуратора ПАС ТЗИ возникшие несоответствие устраняется. Процесс принятия решений синтезатором осуществляется на основе принятых в Украине критериев защищенности информационных ресурсов ЦКС, отраженных в НО [3], [4] и [5]. Кроме того, для принятия решений синтезатор, должен обладать информацией средствах и механизмах ТЗИ, допустимых к использованию не 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 конфигурации ПАС ЦКС и корректными процедурами инсталляции (деинсталляции как элементов, так и всей ЦКС в целом. Необходимо предоставить ведомость конфигурации поставленных ПАС, идентифицирующего комплект поставки защищаемой ЦКС и номер 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 масштабе времени соответствие между текущей конфигурацией ПАС ЦКС и текущим состоянием организационно-распорядительной документации (и другой эксплуатационной документации), сопровождающей процесс эксплуатации защищаемой ЦКС. Оборудование подсистемы управления конфигурацией должно находиться в состоянии наблюдать и проконтролировать изменения (отличия) между различными версиями (типами) объектов, которые подвергается 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 объема всех других объектов, которых касается это изменение.


Структура системы управления комплексом средств ТЗИ
Система управления комплексом средств ТЗИ в ЦКС
Среда функционирования ЦКС:
-информационная;
- пользователей;
-технологическая;
- потенциальных нарушителей.
Анализатор текущего состояния программно-аппаратных средств и среды функционирования ЦКС
Критерии значимости угроз
База данных вероятных угроз для информационных ресурсов ЦКС
Синтезатор пара-метров последующего состояния модели угроз
Модель вероятных угроз для информацион-ных ресурсов ЦКС по состоянию на текущий момент
Анализатор текущего состояния модели угроз
Критерии защищенности информацион-ных ресурсов ЦКС
База данных допустимых к использованию средств и механизмов ТЗИ для ЦКС
Синтезатор параметров последующего состояния конфигуратора средств ТЗИ
Конфигуратор программно-аппаратных средств ЦКС
КСМЗ
Конфигуратор программно-аппаратных средств ТЗИ в ЦКС

Выводы

Организация, эксплуатирующих ЦКС, разрабатывает и утверждает МВУ ее информационным ресурсам, которая учитывает специфику конкретных условий ее применения [2]. Модель вероятных 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.

Література

1. НД ТЗІ 1.1- 001- 99. Технічний захист інформації на програм но-керованих АТС загального користування. Основні положення.

2. НД ТЗІ 2.7. - 001- 99. Технічний захист інформації на програмно-керованих АТС загального користування. Порядок проведення робіт.

3. НД ТЗІ 3.7. - 002 - 99. Технічний захист інформації на програмно-керованих АТС загального користування. Методика оцінки захищеності інформації (базова).

4. НД ТЗІ 2.5 - 002 - 99. Технічний захист інформації на програмно-керованих АТС загального користування. Специфікація гарантій захисту.

5. НД ТЗІ 2.5 - 002 - 99. Технічний захист інформації на програмно-керованих АТС загального користування. Специфікація довірчих оцінок корисності реалізації захисту.

Надійшла: 05.03.11

Рецензент: д.т.н., проф. Корченко О.Г.