4. Щеглов А.Ю. Проблемы и принципы проектирования систем защиты информации от НСД [Текст] / А.Ю. Щеглов. – Сборник "Экономика и производство". – М.: 2001. – № 3. – С. 34 – 46.

5. Павлов И.Н. Проектирование систем защиты информации. Фор-мальный подход [Текст] / И.Н. Павлов. – "Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні". – Київ.: 2005. – Вып. 11. – С. 54 – 59.

6. Павлов І.М. Формальное описание процесса проектирования комплексных систем защиты информации в информационно-телекоммуникационных системах [Текст] / І.М. Павлов, Г.Д. Радзівілов. – Вісник ДУІКТ. – Київ.: 2010. – Т.8. – №1. – С.84 – 93.

7. Павлов І.М. Методологія технічного проектування систем захисту інформації / Павлов І.М. – Захист інформації. – Київ: 2011. № 3 (52). – С. 21 – 29.

8. Павлов І.М. Формалізація проектних показників якості захисту інформації комплексної системи захисту інформації / Павлов І.М., Бірюков В.О. – Захист інформації. – Київ: 2011. – № 2(51). – С. 15 – 21.

9. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі [Текст] / НД ТЗІ 3.7 – 003 – 05. – Київ.: 2005. – 35 с.

Рецензент: Петров А.С.
Надійшла 5.10.2011

УДК 004.621.3:681.322.01

Скоробогатько Е.А.
(ГУИКТ)

ЦЕЛИ И ЗАДАЧИ ЗАЩИТЫ ИНФОРМАЦИИ В ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

Введение

В последнее время быстрое развитие технологий передачи и обработки информации сделало ее одним из ценнейших ресурсов. На сегодняшний день информация приобрела уникальную ценность и является одним из критически важных ресурсов — это новые идеи, производственные, коммерческие секреты и т.д. Информация используется для принятия важных стратегических решений и поэтому ее достоверность и актуальность очень важны. Разглашение или утечка информации могут повлечь различные негативные последствия. Уничтожение одного или нескольких информационных ресурсов способно надолго парализовать деятельность целой организации. Поэтому, совершенно очевидно, что вопросы обеспечения безопасности информации сегодня являются ключевыми проблемами.

Защита каждого объекта информатизации, а также подходы к ее реализации строго индивидуальны. Обеспечение информационной безопасности предполагает проведение целого комплекса организационных и технических мероприятий по обнаружению, отражению, ликвидацию воздействий различных видов возможных угроз. Кроме того, защита должна быть обеспечена по всему спектру гипотетических угроз. Даже одно слабое звено в системе безопасности, возникающее в результате какого-либо изъяна в ее организации, не позволит прочим звеньям в нужный момент противостоять возникшим угрозам. Поэтому для построения надежной защиты необходимо выявить все возможные угрозы безопасности информации, оценить их опасность, вероятность их реализации и по этим данным определиться с необходимыми мерами и средствами защиты, а также оценить их эффективность.

Основная часть

Анализ угроз безопасности информации в телекоммуникационных сетях (ТКС) позволяет сформировать главную цель $Ц_1$ защиты информации – обеспечить безопасность информации в ТКС (рис.1), т.е. предотвращение ущерба системе и интересам пользователей

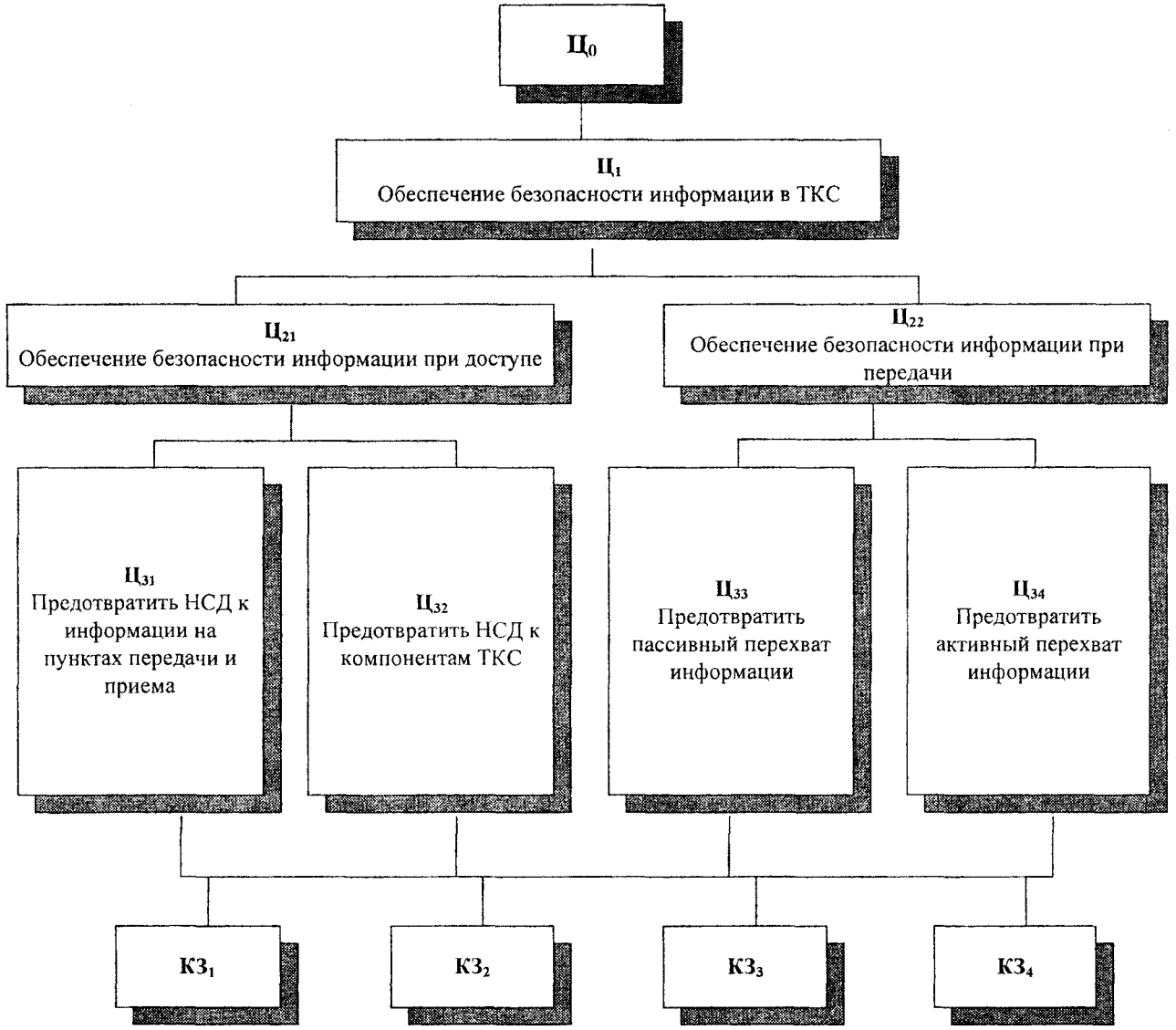

Рис. 1. Дерево целей и задач защиты информации в ТКС

за счет несанкционированных действий (НСД), разглашение, утечки, искажения и уничтожения, информации, нарушение работы технических средств связи и средств обеспечения функционирования сети, включая и вспомогательные средства, а так же ущерба персоналу и пользователей. Цель $Ц_1$ подчинена цели функционирования ТКС $Ц_0$.

Используя методы системного анализа [1,2] можно произвести декомпозицию цели $Ц_1$ на подцели. Такая декомпозиция позволяет сформулировать основные задачи (комплексы задач КЗ), которые необходимо решать для обеспечения безопасности данных в сети, а также определить свойства процесса функционирования ТКС и систем обеспечения безопасности информации. Представленное на рис. 1 дерево целей и задач отражает результат декомпозиции цели $Ц_1$.

Основные цели системы безопасности можно сформулировать как:

- защита информации в сетях и на объектах передачи и приема ее;
- сохранение и эффективное использование ее:
- защита прав пользователей сети.

Задачами системы безопасности являются[3]:

- своевременное выявление и устранение угроз безопасности информации и ресурсам; причин и условий, способствующих нанесению ущерба интереса пользователей;
- отнесение информации к категории ограниченного доступа и ресурсов – к различным уровням защищенности и подлежащим защите;
- создание механизмов и условий оперативного реагирования на угрозу безопасности и НСД;
- эффективное предотвращение попыток атак на ресурсы ТКС;
- создание условий для максимального возможного предотвращения и локализации НСД, ослабление негативного влияния последствий нарушения безопасности.

Объектами, подлежащие защите от потенциальных внутренних и внешних угроз и противоправных посягательств в ТКС являются (рис. 2):

- персонал, работающий в ТКС, а также имеющие доступ к информации;
- материальные и другие ресурсы (здания, сооружения, техническое оборудование и другие источники информации);
- информационные ресурсы с ограниченным доступом, составляющие тайну;
- средства и системы информации и охраны информации.

Рис. 2. Объекты, подлежащие защите в ТКС

Основными задачами обеспечение безопасности информации в ТКС являются [3]:

- организация и составление разрешительной системы допуска исполнителей к работе со сведениями ограниченного доступа;
- осуществление закрытой специальной связи;
- организация и координация работ по защите информации, передаваемой по ТКС;
- обеспечение безопасности в процессе обеспечение конфиденциальной связи;
- осуществление контроля за сохранностью конфиденциальной информации, обрабатываемой и передаваемой ТКС;

Задачи, решаемые для обеспечения безопасности информации в ТКС, являются безусловно, взаимосвязанными. Поэтому, исходя из полученных подцелей $ЦЗ_1$ – $ЦЗ_4$ (рис 1) и содержание каждой из этих задач, все задачи можно объединить в отдельные комплексы задач (КЗ) $КЗ_1$ – $КЗ_4$, которые связаны с разработкой и применением средств и механизмов защиты информации, а также методов, моделей и алгоритмов в рамках основных научных направлений теории обеспечения безопасности информации [3].

Безопасность ТКС достигается проведением единой политики в области защитных мероприятий, системой мер правового, законодательного, организационного и инженерно-технического характера, адекватным угрозам и обеспечения заданного уровня защищенности.

Для создания и поддержания необходимого уровня защищенности объектов ТКС необходимо неукоснительное следование основным принципам обеспечения безопасности информации. Этими принципами являются: законность, достаточность, взаимная ответственность персонала.

Выводы

Таким образом цели представляют собой ожидаемые результаты функционирования системы защиты информации, а задачи то, что надо сделать для того, чтобы система могла обеспечить достижение поставленных целей. Возможность решения задач зависит от ресурса, выделяемого на защиту информации. Ресурс включает в себя людей, решающих задачи защиты информации, финансовые, технические и другие средства, расходуемые на защиту информации. Входами системы защиты информации являются угрозы информации, а выходами — меры, которые надо применить для предотвращения угроз или снизив их до допустимого уровня.

При постарении системы защиты ключевым исходным моментом является формирование всех задач защиты, так как надлежащим распределением ресурсов в осуществление каждой из задач можно оказывать воздействие на уровень защищенности информации, создавая таким образом объективные предпосылки для разработки оптимальной системы защиты.

Список литературы

1. Вунш Г. – Теория систем / Вунш Г. – м. : Сов.радио, 1978.–228с.

2. Згуровський М.З. – Основи системного аналізу / Згуровський М.З., Панкратова Н.Д. – К. : Видавнича група BHV, 2007. – 544 с.

3. Ленков С.В. – Методы и средства защиты информации в 2-х томах / Ленков С.В., Перегудов Д.А., Х

Рецензент:Кунях Н.Н.
Надійшла 31.05.2011