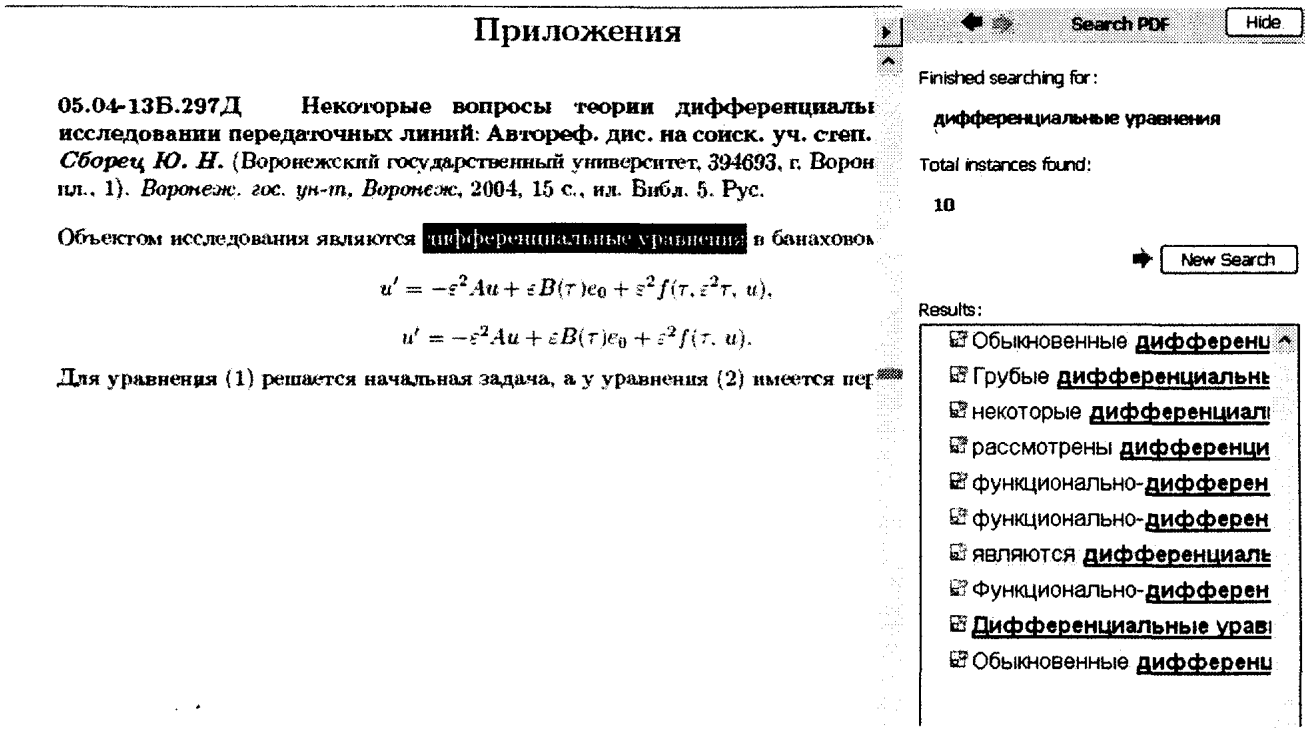


Рис. 15. Результаты поиска по термину "дифференциальные уравнения"

## СПИСОК ЛИТЕРАТУРЫ

1. Шамаев В. Г., Жаров А. В. Проблемы создания ретроспективных реферативных баз данных ВИНИТИ по физико-математическим наукам.— Рук. деп. в ВИНИТИ 24.05.2005.— № 737–В2005.

2. Шамаев В. Г., Жаров А. В., Батурина О. Н., Горшков А. Б., Максимов И. Н., Старцева О. Б. Описание технологии подготовки ретроспективных реферативных баз данных ВИНИТИ по физико-математическим наукам.— Рук. деп. в ВИНИТИ 24.05.2005.— № 739–В2005.

3. Представление элементов данных во внутрисистемном формате ВИНИТИ. Нормативно-техническое предписание НТП ВИНИТИ 10–2004.— М.: ВИНИТИ, 2004.— 104 с.

*Материал поступил в редакцию 23.12.05.*

УДК 004.732.056:001.8

Н. Н. Гусева

# Методологические основы анализа алгоритмического аппарата оценки формирования оптимальной комплексной системы обеспечения безопасности распределенной локальной компьютерной сети

*Рассматриваются вопросы методологии анализа алгоритмического аппарата оценки формирования оптимальной комплексной системы обеспечения безопасности распределенной локальной компьютерной сети (КСОБ РЛКС). Предлагается новый универсальный метод оценки эффективности формирования оптимальной КСОБ с использованием новых техники и технологий защиты информации в РЛКС.*

Комплексная система обеспечения безопасности распределенной локальной компьютерной сети (КСОБ РЛКС) рассматривается как человеко-машинная система, функционирование которой направлено на повышение эффективности выполнения операций всей локальной компьютерной сети. Эффективность КСОБ — это комплексное операционное свойство целенаправленного процесса функционирования системы, характеризующее её способность достигать поставленную цель. Под целью понимается желаемый результат функционирования в течение определенного времени.

Средством для достижения заданной цели являются операции — упорядоченная совокупность взаимосвязанных действий.

Система — это взаимосвязь эргатических и неэргатических элементов (аппаратных, программных, информационных средств, обслуживающего персонала, пользователей), непосредственно участвующих в процессе выполнения операции [1].

Объектом исследования теории эффективности является операция, т. е. процесс функционирования в нашем случае комплексной системы обеспечения безопасности.

Предмет исследования — закономерности оптимальной организации процесса функционирования системы обеспечения безопасности.

Обеспечение безопасности информационных сетей приобретает большое значение, поскольку характер информации представляет собой коммерческую тайну. Создавая корпоративную сеть, необходимо предусматривать стратегию обеспечения безопасности, позволяющую защитить компьютерную информационную сеть от внутренних и внешних несанкционированных посетителей [2]. Под внешним воздействием на безопасность КСОБ понимается комплекс действий, вызываемый программными злоупотреблениями. Поэтому необходимо определить тип локальной компьютерной сети как объекта защиты.

При оценке эффективности КСОБ необходимо выявить и количественно измерить влияние неправомерных воздействий на КСОБ. Эта задача является одной из важнейших в проблеме информационной безопасности. При ее решении следует: определить структуру и содержание всех причин нарушения целостности информации; выявить способы несанкционированного размножения информации; определить задачи анализа и оценки угроз информации; выявить систему показателей уязвимости информации; определить полное множество угроз информации; установить систему дестабилизирующих факторов, влияющих на уязвимость информации. Дестабилизирующими факторами являются такие, вследствие которых на определенном этапе могут быть нежелательные воздействия на информацию.

При создании КСОБ РЛКС, использующей каналы Интернет, необходимо соблюдать функциональные требования и учитывать два основных принципа [3]:

- использование при установлении соединения клиент-сервер закрытого протокола, обеспечивающего защищенное взаимодействие абонентов по виртуальному каналу связи;
- доступность открытых протоколов (команд Интернет) для взаимодействия по защищенному виртуальному каналу после установления соединения.

Поскольку КСОБ представляет собой сложную человеко-машинную систему (СЧМ), то ее проект необходимо разрабатывать как часть проекта локальной компьютерной сети, а не отдельный проект.

При оценке её эффективности целесообразно использовать принцип декомпозиции, т. е. разбить КСОБ на подсистемы и оценивать отдельно каждую из них, после чего провести интегральную оценку всей системы. Получение прибыли с участием КСОБ РЛКС достигается в основном за счет:

а) предотвращения ущерба, т. е. увеличения "сохраненной стоимости";

б) увеличения объемов производства продукции с помощью надежной КСОБ, которая способствует повышению эффективности функционирования локальной компьютерной сети;

в) снижения себестоимости выпускаемой продукции с помощью надежной системы обеспечения безопасности.

При этом главное внимание уделяется целевой и экономической эффективности. Первая из них отражает степень соответствия КСОБ своему назначению, вторая — экономическую эффективность — экономическую целесообразность создания и внедрения КСОБ.

Начало совершенствования существующей КСОБ осуществляется за счет внедрения новой техники (новые программно-аппаратные средства) и технологий (НТТ), которые подразделяются на три группы:

- НТТ первой группы непосредственно обеспечивают повышение эффективности функционирования КСОБ (программно-аппаратные средства и способы использования традиционных и нетрадиционных средств защиты);
- НТТ второй группы повышают эффективность управленческой деятельности организации по линии обеспечения безопасности информации, т. е. они используются в управлении КСОБ (ПК, пакеты программ);
- НТТ третьей группы направлены на повышение эффективности деятельности человека-оператора, функционирующего в КСОБ, т. е. на увеличение эффективности деятельности человека в системе эргономического обеспечения КСОБ.

Деление новой техники и технологий на три группы объясняется принципиальным их различием по целевому назначению, наличием специфики при формировании методологических основ оценки эффективности использования НТТ.

Оценка эффективности функционирования КСОБ РЛКС должна осуществляться с помощью системы показателей, включающих интегральные и частные, абсолютные и относительные показатели.

В результате внедрения новой техники и технологий, кроме целевого эффекта КСОБ, можно получить как прямой, так и косвенный экономический эффект. При оценке полного экономического эффекта за счет КСОБ необходимо учитывать оба этих вида эффекта.

Система показателей оценки эффективности внедрения КСОБ и алгоритмы определения их значений должны обеспечивать проведение как априорной, так и апостериорной оценок КСОБ.

Оценка эффективности КСОБ должна включать оценку эффективности эргономического обеспечения (ЭО) локальной компьютерной сети [1]. Априорная и апостериорная оценки эффективности эргономического обеспечения базируются на следующих методологических предпосылках.

- Целевой и экономический эффекты, получаемые за счет системы эргономического обеспечения разработки и эксплуатации (СЭОРЭ) КСОБ, самостоятельны. Каждый из них можно оценить количественно с помощью показателей целевой и экономической эффективности.

- Комплексность оценки заключается в том, что она проводится: на всех стадиях создания и эксплуатации КСОБ, с учетом единовременных и текущих затрат на формирование и функционирование СЭОРЭ; с учетом всего комплекса показателей трудовой деятельности операторов человеко-машинной системы КСОБ.
- Оценка экономической эффективности СЭОРЭ может осуществляться в двух вариантах: по источникам прямой экономии, создаваемым при функционировании СЭОРЭ; по источникам прямой и косвенной экономии, создаваемым за счет СЭОРЭ.

Косвенная экономия рассчитывается путем определения стоимостного эквивалента для прироста целевого эффекта, получаемого за счет СЭОРЭ.

Одним из главных факторов, влияющих на результативность и качество работы по оценке эффективности СЭОРЭ КСОБ, является достоверность исходных данных, необходимых для оценки [2]. Полнота и достоверность данных зависят от того, на какой стадии жизненного цикла СЧМ КСОБ проводится оценка её эргономического обеспечения [1].

Интегральные (для всесторонней оценки по всем источникам экономии) и частные (по одному или нескольким источникам экономии), абсолютные и относительные показатели эффективности характеризуют достигнутый уровень функционирования КСОБ локальной компьютерной сети. Они имеют размерность.

Целевая эффективность является основным критерием при выборе проектируемого варианта КСОБ. При разработке и внедрении КСОБ проект должен подкрепляться проведением экспертизы и экономическими расчетами в соответствии с инвестициями, поскольку они связаны с риском и влияют на результаты финансовой деятельности в сторону уменьшения потерь от действия дестабилизирующих факторов. Потери КСОБ могут быть техническими, организационными, технологическими, экономическими. Все они вытекают друг из друга. Потери на одном уровне влекут за собой потери на следующих [3].

При определении величины потерь, следует иметь в виду ресурсы, на которые возможны атаки злоумышленников, или которые могут быть утеряны полностью или частично. При этом следует учитывать вероятность восстанавливаемости ресурса в исходное состояние.

Для исследования потерь КСОБ ЛКС следует выделить совокупные потенциальные потери без использования КСОБ — они определяются ценностью активов локальной компьютерной сети и возможные реальные потери при использовании КСОБ — этот тип потерь является расчетным [4].

При проектировании КСОБ должна учитываться величина выигрыша нарушителя, и основная задача — сведение этой величины к минимуму.

При исследовании потенциальных угроз необходимо также изучить ресурсы КСОБ и найти комплекс решений к каждому ресурсу [3].

Инвестиции в КСОБ представляются в виде целевой функции увеличения прибыли и уменьшения затрат и потерь.

Проект должен быть подвергнут анализу экономической целесообразности и инвестиционной привлекательности. Надежность — это относительная величина, которая определяется как вероятность безотказной работы КСОБ в течение определенного временного интервала и при соответствующих условиях функционирования. При оценке надежности КСОБ локальной компьютерной сети следует учитывать все показатели, связанные с изменением среды функционирования КСОБ.

Показатели экономической эффективности КСОБ отражают целесообразность вложения средств в обеспечение безопасности информации в распределенной локальной компьютерной сети, которая определяется величиной уменьшения потенциальных потерь, коэффициентом окупаемости и др.

Расчет количественных показателей неразрывно связан с риском и затратами на уменьшение риска.

Анализ риска служит основой для инвестиций в КСОБ и способствует повышению осведомленности персонала, подготовке и принятию решений по выбору средств контроля, определению затрат на организацию защиты. Чем меньше затрат на организацию защиты, тем выше риск потери информации [5].

При создании КСОБ выделяют следующие виды риска:

- технический, который присутствует повсеместно и распространяется на весь спектр аппаратных и программных средств защиты;
- проектно-эксплуатационный. Техническая сложность проектируемой КСОБ должна обеспечивать завершенность и целостность системы. Она может потребовать повышения квалификации обслуживающего персонала или, как крайний случай, его замены;
- системный. Система спроектирована с учетом требований окружающей среды, обеспечивает сохранность информации и ресурсов от несанкционированного доступа;
- функциональный. После завершения проектирования КСОБ может оказаться, что функциональное наполнение не соответствует заданным требованиям, тогда возникает необходимость в дополнительных исследованиях и разработках по его совершенствованию.
- финансовый. Этот вид риска допустим только в случае уникальности защищаемой информации. Снижение этого риска возможно за счет управления другими видами риска, сокращения их до минимально допустимых.

На сегодняшний день существуют два типа риска: глобальный (долгосрочный) и локальный (краткосрочный) [4]. На основе анализа можно сделать вывод, что долгосрочный риск решается на уровне КСОБ локальной компьютерной сети, а краткосрочный — локально, с помощью используемых методов и средств защиты.

Использование показателя "дрейф" при расчете надёжности технических систем показывает изменение характеристик элементов КСОБ (старение, деградация и др.). Оптимизация дрейфа надежности технических систем ставится в зависимость от воздействий окружающей среды (температура, влажность и др.). Дрейф КСОБ — это ограничение пределов надежности.

Включение в структуру КСОБ избыточных элементов защиты необходимо с целью повышения