УДК 681.3:519.1

ПРОБЛЕМА ОПТИМИЗАЦИИ ПРОЦЕССОВ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ СФЕРЫ КРИТИЧЕСКИХ ПРИЛОЖЕНИЙ

С.В. Скрыль, В.С. Зарубин, А.Я. Фомин

Обосновывается актуальность проблемы оптимизации процессов защиты информации в информационно-телекоммуникационных системах сферы критических приложений. Приводится перечень задач по ее решению

Ключевые слова: информационно-телекоммуникационные системы сферы критических приложений, средства защиты информации встраиваемого типа, угрозы нарушения доступности и целостности информации

Анализ перспектив совершенствования информационных технологий свидетельствуют о наличии устойчивой тенденции интегрирования средств обработки информации и средств ее обмена в рамках нового класса систем – информационно-телекоммуникационных (ИТКС). Подобные системы реализуют на сегодняшний день, значительную часть объема информационных услуг в различных сферах жизнедеятельности современного общества, в том числе и в сфере, известной как сфера критических приложений. Это в свою очередь, выдвигает высокие требования к обеспечению работоспособности этих систем в условиях воздействия негативных факторов на процессы их функционирования.

Одним из наиболее серьезных факторов снижения эффективности функционирования ИТКС сферы критических приложений являются угрозы нарушения доступности и целостности информации. Как системообразующие информационно-телекоммуникационные инфраструктуры данной сферы обеспечивают выполнение функций управления объектами и процессами, нарушение работоспособности которых может привести к существенному ущербу. Воздействие угроз нарушения доступности и целостности информации на управляющие информационные процессы, реализуемые ИТКС сферы критических приложений, крайне критичными к своим временным параметрам, приводит к серьезным последствиям, связанным с огромными временными издержками по восстановлению корректности этих процессов. С учетом постоянно возрастающих требований к оперативности обработки информации в таких системах актуальность проблемы обеспечения их информационной безопасности ставится в настоящее время крайне остро /1/.

Выработка адекватных угрозам нарушения целостности и доступности информации и особенностям функционирования ИТКС сферы критических приложений мер противодействия угрозам, привела к разработке соответствующих средств защиты, которые в литературе известны как встраиваемые /2/. Главной особенностью таких средств является то, что они реализуют функции защиты информации практически одновременно с функциями информационного процесса за счет чередования выполнения этих функций. Это позволяет значительно сократить время реакции на воздействия угроз и обеспечить своевременное восстановление информационного процесса.

Вместе с тем одновременная реализация функций защиты информации с функциями ее обработки сопряжена с необходимостью одновременного использования временного ресурса ИТКС.

Существующая же практика использования подобных средств защиты информации в ИТКС в целом и в ИТКС сферы критических приложений в частности дает основание утверждать о несогласованном, бессистемном и, как следствие, неэффективном использовании

Скрыль Сергей Васильевич - МГТУ имени Н.Э. Баумана, д-р техн. наук, профессор кафедры ИУ-10, тел. (495) 632-22-47

Зарубин Владимир Сергеевич – Воронежский институт МВД России, начальник кафедры технических систем безопасности и связи, канд. техн. наук, доцент, тел. 89102473470

Фомин Анатолий Яковлевич - ВГТУ, соискатель, e-mail: mnac@comch.ru

ими временного ресурса этих систем. Это ставит довольно сложную как в научном, так и в практическом плане задачу - еще на этапе проектирования ИТКС рассматриваемого класса решить задачу эффективного использования встраиваемых средств защиты информации.

Как показывает анализ состояния вопроса, одним из наиболее перспективных путей решения данной задачи является разработка методик, моделей и алгоритмов оптимального использования временных ресурсов ИТКС средствами защиты информации встраиваемого типа в соответствии с особенностями механизма обеспечения защиты.

Реализация этого подхода возможна на основе решения ряда частных оптимизационных задач, связанных с выявлением и оптимальным распределением этих ресурсов в интересах реализации встраиваемых средств защиты информации с учетом характеристик соответствующих механизмов защиты.

Несмотря на то, что совершенствование методологии обеспечения информационной безопасности стало актуальной проблемой, специальные исследования применительно к задачам распределения ресурсов в интересах использования средств защиты компьютерной информации встраиваемого типа носят ограниченный характер. В этой связи следует отметить ряд работ, относящихся к вопросам распределения ресурсов в компьютерных системах специального назначения в интересах комплексного использования средств защиты информации придаваемого и встраиваемого типа. К ним относится /3/ и ряд других. Несмотря на существенные различия в разработанном методическом аппарате эти работы объединяет один общий недостаток – применяемые модели исследуемых процессов позволяют лишь частично решать задачу распределения ресурсов: охватывая только вопросы распределения временной избыточности. Что же касается использования этой избыточности при ее реализации конкретными средствами защиты информации, то разработанный аппарат не обеспечивает выбор более или менее определенного варианта таких средств, а предоставляет лишь область решений для такого выбора в терминах нечетких множеств. Естественно, что корректность решения задачи в этих условиях не может быть высокой.

Это дает основание утверждать, что проблема оптимизации процессов защиты информации в ИТКС сферы критических приложений является актуальной, а связанные с этим направлением вопросы совершенствования методологии нуждаются в проработке как в методическом, так и в прикладном плане.

В связи с этим становится крайне актуальной проблема разработки и исследования алгоритмов оптимального использования временного ресурса ИТКС сферы критических приложений средствами защиты информации встраиваемого типа для противодействия угрозам нарушения доступности и целостности информации этих систем в интересах повышения эффективности защиты информации.

Решение данной проблемы связано с решением ряда научных задач, основными из которых являются:

1. Формулировка методических положений относительно возможности повышения эффективности защиты информации в ИТКС сферы критических приложений средствами защиты информации встраиваемого типа в условиях оптимального использования временного ресурса этих систем.

2. Разработка методической базы оптимизации процессов защиты информации в системах данного класса, включающей:

- методику выявления оптимального объема временного ресурса этих систем в интересах использования средствами защиты информации встраиваемого типа;

- методику оптимального распределения этого объема между процедурами обработки информации в интересах реализации различных механизмов ее защиты.

3. Обоснование аппарата математического моделирования для оценки показателей эффективности обработки информации в ИТКС и эффективности защиты информации в этих системах от воздействия угроз нарушения ее доступности и целостности.

4. Разработка схемы вычислительных экспериментов по формированию вариантов использования средств защиты информации встраиваемого типа для противодействия угрозам нарушения целостности и доступности информации в ИТКС сферы критических при-

ложений в условиях оптимального использования временного ресурса этих систем.

Решение первой из перечисленных задач сопряжено с необходимостью формулировки основных принципов решения проблемы оптимизации процессов защиты информации в ИТКС сферы критических приложений.

Методической основой при решении данной задачи в соответствии с методологическими положениями системного анализа /4/ является принцип согласованности целей при реализации процедур информационного процесса и процедур защиты информации предполагающий, что процедуры защиты от воздействия угроз нарушения доступности и целостности информации могут быть эффективно реализованы за счет использования дополнительного (резервного) ресурса вычислительной среды ИТКС.

Принцип оцениваемости временного ресурса ИТКС определяет необходимое и достаточное условия для постановки и решения задачи оптимизации процессов защиты информации в ИБС ОСС в условиях использования средств защиты встраиваемого типа.

Принцип однородности показателей эффективности обработки информации в ИТКС и эффективности защиты информации от воздействия угроз нарушения ее доступности и целостности предполагает, что при обосновании этих показателей в основу взят один и тот же физический параметр. Очевидно, что наиболее целесообразной формой описания функциональных возможностей ИТКС сферы критических приложений являются временные параметры. Эти параметры напрямую связаны с объемом соответствующего программного обеспечения как целевого, реализующего процедуры обработки информации, так и дополнительного, реализующего процедуры обеспечения защиты информации от воздействия угроз нарушения ее доступности и целостности.

В соответствии с принципом математической интерпретации совместного функционирования средств обработки информации и средств ее защиты от воздействия угроз нарушения ее доступности и целостности существует соответствующее формализованное представление этих процедур в рамках единого процесса.

Сформулированные принципы позволяют сформулировать проблему оптимизации процессов защиты информации в ИТКС сферы критических приложений, которая формально ставится как проблема максимизации показателя эффективности защиты информации в этих системах на множестве вариантов распределения оптимальным образом выявленного временного резерва ИТКС.

Решение второй из перечисленных задач сопряжено с необходимостью формулировки и доказательства ряда теоретических положений относительно аналитических зависимостей показателей эффективности процессов защиты информации в ИТКС и процессов ее обработки в этих системах от величины их временного резерва.

Это позволяет разработать методический аппарат, обеспечивающий определение оптимума временного ресурса ИТКС, который может быть выделен как временной резерв для реализации встроенных механизмов защиты информации. Это в свою очередь является предпосылкой для дальнейшего оптимального распределения этого резерва между процедурами обработки информации в ИТКС в интересах реализации встраиваемых механизмов защиты информации.

Методической основой при решении третьей из перечисленных задач решения проблемы оптимизации процессов защиты информации в ИТКС сферы критических приложений является комплекс математических моделей, включающий модель процессов возникновения угроз нарушения доступности и целостности информации в этих системах, модель противодействия такого рода угрозам информационной безопасности, а также модель информационных процессов в ИТКС данного класса в условиях обеспечения защиты информации средствами защиты встраиваемого типа.

При моделировании воздействий угроз нарушения целостности и доступности информации в ИТКС сферы критических приложений достаточно воспользоваться результатами обоснования такого рода воздействий, как потока событий, обладающего свойствами стационарности, ординарности и отсутствия последействия /5/.

При моделировании процессов противодействия угрозам нарушения доступности и целостности информации в ИТКС, а также моделировании информационных процессов в этих системах в условиях обеспечения защиты информации средствами защиты встраиваемого типа возможно использование разработанных аналитических моделей для оценки вероятностных показателей в приложениях теории информационной безопасности /6, 7/.

При решении четвертой из перечисленных задач возникает необходимость преодоления ряда проблем, связанных с планированием вычислительных экспериментов при использовании математических моделей защищенности информационных процессов /8/.

Решение проблемы оптимизации процессов защиты информации применительно к такому классу ИТКС, как информационно-биллинговые системы операторов сотовой связи показывает, что применение разработанных, в соответствии с изложенным подходом, методов противодействия угрозам нарушения доступности и целостности информации в этих системах позволяет повысить показатель эффективности противодействия на 30%, а показатель эффективности информационных процессов – на 20%.

Литература

1. Информационная безопасность телекоммуникационных систем (технические вопросы): учеб пособие для системы высшего профессионального образования России / С.В. Скрыль [и др.]. – М.: Радио и связь, 2004. – 388 с.

2. Информационная безопасность открытых систем: учебник для вузов. В 2-х томах. Т. 1. Угрозы, уязвимости, атаки и подходы к защите / А.И. Толстой [и др.]. – М.: Горячая линия-Телеком, 2006. – 536 с.

3. Хохлов Н.С. Моделирование и оптимизация противодействия разрушению информации в системах управления и связи органов внутренних дел при электронных воздействиях: монография / Н.С. Хохлов под. ред. С.В. Скрыля. – Воронеж: Воронежский институт МВД России, 2005. – 181 с.

4. Шелупанов А.А. Основы системного анализа в защите информации: учеб. пособие для студентов высших учебных заведений / А.А. Шелупанов, С.В. Скрыль. - М.: Машиностроение, 2008. – 138 с.

5. О некоторых допущениях в математической интерпретации угроз нарушения целостности и доступности информации в компьютерных системах / В.С. Зарубин [и др.]. // Информация и безопасность: науч. техн. журнал – Воронеж: ВГТУ, 2009. Вып. 4. – С. 625 – 626.

6. О возможности применения вероятностных показателей в приложениях теории информационной безопасности / А.Г. Остапенко, С.В. Скрыль [и др.] // Радиотехника (журнал в журнале), 2002, №11. С. 97-100.

7. Аналитические модели обеспечения защищенности информационных процессов / С.В. Скрыль [и др.]. // Информация и безопасность: науч. техн. журнал – Воронеж: ВГТУ, 2008. Вып. 4. – С. 593 – 596.

8. Проблемы планирования вычислительных экспериментов при использовании математических моделей защищенности информационных процессов / К.С. Скрыль [и др.]. // Информация и безопасность: науч. техн. журнал – Воронеж: ВГТУ, 2009. Вып. 1. – С. 143 – 144.

Московский государственный технический университет имени Н.Э. Баумана
The Moscow state technical university of a name of N.E. Bauman
Воронежский институт МВД России
Voronezh Institute of Russian Ministry of Interior

PROBLEM OF OPTIMIZATION OF PROCESSES OF PROTECTION OF THE INFORMATION IN TELECOMMUNICATION SYSTEMS OF SPHERE CRITICAL APPENDICES

S.V. Skryl, V.S. Zarubin, A.Y. Fomin

The urgency of a problem of optimization of processes of protection of the information in telecommunication systems of sphere of critical appendices is proved. The list of problems under its decision is resulted

Key words: telecommunication systems of sphere of critical appendices, means of protection of the information of built in type, threat of infringement of availability and integrity of the information