5. *Федоров В.М., Юрков П.Ю.* Сегментация сигналов на основе дискретного вейвлет-преобразования. Таганрог, Информационная безопасность / Материалы IX Международной научно-практической конференции. – Таганрог: Изд-во ТТИ ЮФУ, 2007. – 128-134 с.

УДК 681.397

Белый А.Ф.

КОМПЬЮТЕРНЫЕ ИГРЫ ДЛЯ ВЫБОРА МЕТОДОВ И СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

Современный уровень развития методов и средств защиты информации в автоматизированных системах (АС) характеризуется широкой номенклатурой средств, обеспечивающих требуемый класс защищенности. Широкое внедрение информационных и телекоммуникационных технологий в АС управления технологическими процессами, как правило, сопровождается появлением дополнительных уязвимостей и новых угроз нарушения информационной безопасности. Поэтому, актуальной проблемой является разработка методического и программного обеспечения для выбора и априорной оценки эффективности применения методов и средств защиты информации с учётом особенностей функционирования АС и специфики потенциальных действий нарушителя.

В настоящее время уровень развития компьютерных игр позволяет использовать их как основу для создания новых средств для выбора методов и средств защиты информации в АС. Компьютерные игры предоставляют дополнительные возможности для оценки эффективности средств защиты информации, выбора необходимых средств в условиях неопределенности знаний о модели нарушителя и процессах функционирования АС при воздействии компьютерных атак.

В перечне приоритетных проблем научных исследований в области информационной безопасности Российской Федерации предложены деловые и специализированные исследовательские игры по информационной безопасности.

Компьютерная игра для выбора методов и средств защиты информации в АС представляет собой комплекс программ, предназначенный для моделирования в реальном масштабе времени возможных действий нарушителя на уязвимости АС, адекватных мер защиты информации, процессов функционирования системы на заданном интервале времени и оценки эффективности выбранных вариантов игры.

Защищённой АС можно считать лишь ту систему, для которой осуществлён выбор оптимальных методов и средств защиты информации, соответствующих модели нарушителя и позволяющих устранить уязвимости. Под защищенной АС будем понимать систему, в которой реализован комплекс необходимых организационно-технических мероприятий по защите информации в соответствии с требованиями нормативных документов ФСТЭК России. В данном случае рассматриваются меры противодействия угрозам несанкционированного доступа (НСД), воздействия компьютерных вирусов и проявления недекларированных возможностей. Для испытаний АС и защиты от этих угроз применяются традиционные средства защиты информации (СЗИ) по ГОСТ 28195-89, ГОСТ 34.603-92, ГОСТ Р 51188-99, ГОСТ Р ИСО/МЭК 12119-2000, ГОСТ Р ИСО/МЭК 15026-2002, ГОСТ Р ИСО/МЭК 15408-2002.

Кроме того, для АС управления технологическими процессами важно сохранение работоспособности на заданном интервале времени в условиях воздействия компьютерных атак. Под отказоустойчивой АС будем понимать систему, в которой при воздействии компьютерных атак сохраняется полная или частичная рабо-

тоспособность на установленном интервале времени. Для обеспечения отказоустойчивости АС необходимо применять средства обнаружения атак (СОА) и избыточные модули восстановления работоспособности системы (рестарта операционной системы, систем управления базами данных, устранения ошибок в программах, администрирования вычислительных ресурсов и т.п.).

На практике применение сложных АС сопровождается множеством нештатных ситуаций и деструктивных воздействий, особенно, если в системе имеется подключение к глобальной информационной сети Интернет. Поэтому, актуальной является проблема разработки методических и технологических основ создания компьютерных игр для выбора методов и средств защиты информации в АС. Для принятия скоординированных решений по обеспечению защищённости и отказоустойчивости АС необходимо в компьютерных играх реализовать следующее:

- логическое соответствие алгоритмов компьютерных игр структурам программного, информационного и технического обеспечения АС;
- формализацию сценариев возможных действий нарушителя;
- описание в виде информационных моделей функций средств защиты информации и обеспечения отказоустойчивости;
- формализованное представление данных о работоспособности АС в условиях компьютерных атак;
- представить знания об опыте эксплуатации и результатах применения методов и средств защиты информации и обеспечения отказоустойчивости;
- описать возможные риски и ущерб от нарушения безопасности информации;
- разработать систему показателей оценки эффективности защиты информации и обеспечения отказоустойчивости.

Технологическая схема создания компьютерных игр для выбора методов и средств защиты информации в АС представлена на рис. 1.

В соответствии с технологической схемой программные средства компьютерных игр должны обеспечивать:

- формирование типовых сценариев действий нарушителя и применения СЗИ;
- формирование игровой обстановки для операторов компьютерной игры;
- сбор, хранение и подготовку исходных данных для компьютерных игр по результатам стендовых испытаний;
- имитационное моделирование АС в виде информационных объектов компьютерных игр;
- визуализацию действий сторон в процессе проведения компьютерных игр;
- оценку защищённости и отказоустойчивости АС по результатам проведения игр;
- ведение базы знаний о результатах применения методов и средств защиты, сценариях действий нарушителя.

Средства компьютерных игр позволяют накапливать знания в виде хранилищ данных в области информационной безопасности и проводить экспертам многокритериальный выбор возможных решений по защищённости и отказоустойчивости АС на основе полученной статистики. Как правило, компьютерные игры реализуются в виде аппаратно-программных комплексов управления принятием решений, объединенных вычислительной сетью и являющихся прототипом базовых компонентов АС.

Аппаратно-программные комплексы компьютерных игр должны обеспечивать априорную оценку возможных угроз воздействия компьютерных атак и других нарушений информационной безопасности, выявление уязвимостей АС, моделирование вариантов средств защиты информации и противодействия атакам,

отработку действий администраторов информационной безопасности и предварительную оценку ущерба от действий нарушителя.

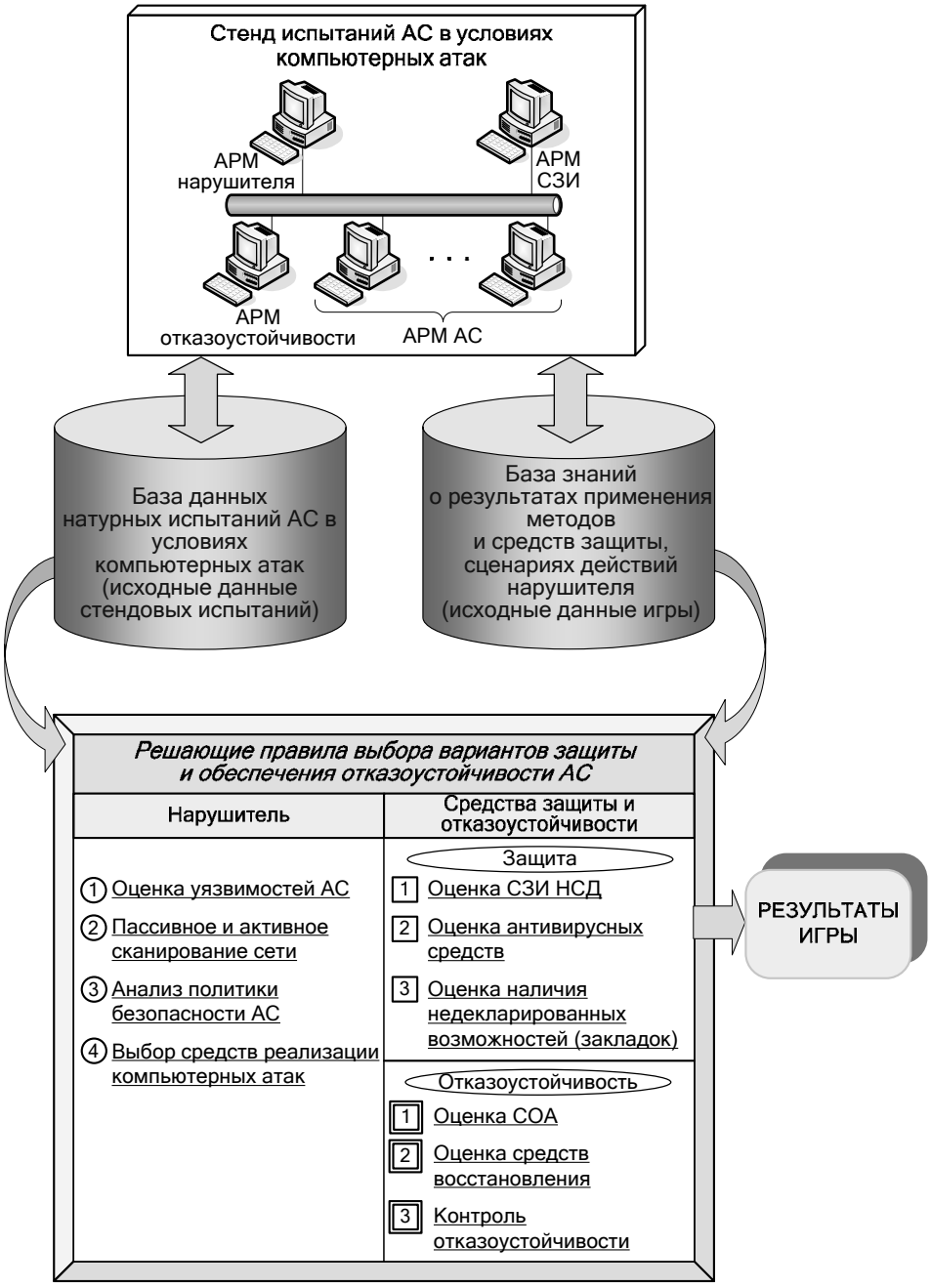

Рис. 1. Технологическая схема создания компьютерных игр для выбора методов и средств защиты информации в АС

Программно-алгоритмическое обеспечение компьютерных игр базируется на теории исследования операций и включает в свой состав совокупность методов математического, имитационного и полунатурного моделирования, а также является инструментом поиска и принятия решений в реальном масштабе времени. Методы экспертной оценки реализуются через роли игроков компьютерной игры.

Компьютерная игра служит для выработки рекомендаций по рациональным действиям и согласованному выбору средств защищенности АС при разработке компонентов системы и средств защиты информации в условиях наличия неопределенности действий нарушителя.

При проведении компьютерной игры на стенде воспроизводится имитационная и натурная модель функционирующих компонентов АС, подключается имитатор действий нарушителя и макеты средств защиты информации и производится оценка характеристик защищённости и отказоустойчивости АС путем воспроизведения в сценарии игры реальных динамических процессов и условий применения системы.

Правила проведения игры определяются параметрами, характеризующими варианты действий сторон (нарушитель и средства защиты и отказоустойчивости), информацию об АС, возможные результаты взаимосвязанной оценки защищенности и отказоустойчивости АС при различных соотношениях между параметрами средств нарушителя и средств защиты от подобных воздействий.

Эффективность принятия решений по комплексу вопросов защиты информации от несанкционированного доступа, антивирусной защите, выявлению компьютерных вирусов, обнаружению атак и сохранению работоспособности в условиях деструктивных воздействий нарушителя во многом определяется полнотой и достоверностью решений по выбору средств защищенности АС, их адекватностью угрозам и уязвимостям системы.

Требуемая защищенность и отказоустойчивость АС будет достигнута только в том случае, когда в условиях воздействий нарушителя выполнен установленный регламент сбора, обработки и передачи информации за заданный период времени.

Таким образом, актуальность самостоятельного и детального исследования проблемных вопросов создания компьютерных игр для выбора методов и средств защиты информации в АС обусловлена следующим:

- возможностью проведения априорных испытаний (тестирования) АС в условиях воздействий нарушителя и получения оценок защищённости и отказоустойчивости системы;
- наглядностью и оперативностью принятия многоальтернативных решений по защищенности АС;
- наличием возможностей проверки программной и информационной совместимости АС, средств защиты информации, антивирусных средств и средств обнаружения атак;
- динамикой оценки на основе использования игр возможных событий информационной безопасности и состояний работоспособности АС;
- разнообразием форм и способов детальной оценки сценариев действий нарушителя и средств защиты от них;
- наличием возможности существенно улучшить показатели защищенности и отказоустойчивости АС за счет многовариантного, детального анализа и оптимального выбора рациональных вариантов защиты информации;
- существенным расширением возможностей по автоматизированному накоплению статистики и использованию знаний о вариантах применения методов и средств защищённости и отказоустойчивости;

- возможностью оценки защищенности АС при подключении глобальных информационных сетей и беспроводных средств удаленного доступа.