Bozhenyuk Alexander Vitalievich
E-mail: avb002@yandex.ru.

Rozenberg Igor Naymovich
Public corporation “Research and development institute of railway engineers”.
E-mail: I.kudreyko@gismps.ru.
27/1, Nizhegorodskaya street, Moscow, 109029, Russia.
Phone: 84959677701.

Yastrebinskaya Dina Nikolaevna
Scientific and Technical Center "*INTECH*" of Federal State-Owned Educational Establishment of Higher Vocational Education “Southern Federal University”.
E-mail: dny.tsure@gmail.com.
Oktyabrskaya Square, 4, Taganrog, 347922, Russia.
Phone: +79289048814.

УДК 681.5.08

Ф.А. Самсонов, И.И. Костюченко, М.В. Петров, В.Н. Наконечный

МЕТОД ФАКТОРНОГО ПАРАМЕТРИЧЕСКОГО МОДЕЛИРОВАНИЯ ФУНКЦИОНАЛЬНОЙ УСТОЙЧИВОСТИ ИНФОРМАЦИОННО-РАСЧЕТНЫХ СИСТЕМ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Статья посвящена применению метода факторного параметрического моделирования к решению актуальной научной задачи оценки безопасности современных информационно-расчётных систем и сетей, а также расчёту дифференциального и интегрального значений риска реализации потенциальных угроз различной природы в таких системах.

Информационно-расчётная система; безопасность; возможностная мера; уязвимость; угроза; воздействие; ослабление; восприимчивость; ущерб.

F.A. Samsonov, I.I. Kostuchenko, M.V. Petrov, V.N. Naconechnyi

METHOD OF FACTORIAL PARAMETRICAL MODELING OF THE LOSS TO SYSTEMS FUNCTIONAL STABILITY SPECIAL INFORMATION-ACCOUNTING SYSTEMS

The Article is dedicated to using the method of factorial parametric modeling to decision of the actual scientific problem of the estimation to safety modern information-accounting systems and networks and estimations differential and integral risk to realization of the potential threats of the different nature in such system

Information-accounting system; safety; possibility measure; criticality; threat; influence; weakening; receptivity; damage.

Важнейшей составляющей национальной безопасности любого современного постиндустриального информационного общества является её информационная безопасность. Поскольку информационное, программное обеспечение, технологии обработки, передачи, сохранения данных заняли ключевую позицию в тех областях современного общества, которые принято относить к критично важным для обороноспособности и экономической стабильности государства: систем автоматизированного управления и контроля состояния радиационных, химических, биологических опасных объектов; систем сбора, обработки и передачи данных в информационных, информационно-расчётных и управляющих системах органов государственной власти, штабов соединений родов войск ВС РФ, а также автоматизированных систем боевого управления войсками и оружием [1,7].

В соответствии с принятой в Российской Федерации Концепции национальной безопасности, Военной доктрины и Доктрины информационной безопасности одной из основных задач национальной безопасности РФ, помимо обеспечения информационной безопасности критически важных государственных информационных структур, является ведение активного противоборства угрозам их функционирования. Одним из наиболее важных направлений в обеспечении безопасности существующих информационно-расчётных систем является разработка единой методики оценки безопасности систем и принятие комплекса стандартных показателей безопасности для всех видов воздействующих факторов применительно к физически разнородным объектам и воздействующим факторам [6].

В настоящее время признано [3,4,5], что исследование безопасности и риска систем «человек – машина – среда» может быть адекватно проведено в рамках системы «потенциально опасный объект – средства и меры защиты – опасные и вредные факторы – человек».

Реализация потенциальной угрозы в ИРС приводит к нарушению функциональной устойчивости системы в виду как проектных просчётов состава и структуры ИРС, так и в виду наличия уязвимостей в системе организационных, технических (аппаратного и программного уровня) мероприятий контроля и обеспечения безопасности.

Возможность количественной оценки опасности от реализации потенциальной угрозы определяется как риск происшествия, связанного с информационно-расчётной системой и является основой для расчёта значения ущерба от такого происшествия.

В качестве объектов угрозы, в соответствии с [3,7], могут рассматриваться как физические элементы ИРС, так и информация или информационные ресурсы [2].

Наличие объекта угрозы и потенциальной угрозы в информационно-расчётной системе не означает, что она обязательно нанесёт ущерб системе, поскольку для этого требуется использование уязвимости в системе средств и мероприятий защиты. Безопасность ИРС связана с защитой объектов угрозы ИРС от потенциальных угроз, классифицируемых в зависимости от возможности доступа к объектам угроз, при этом во внимание принимаются все разновидности угроз, но в первую очередь те, которые связаны со случайными или умышленными действиями оператора (пользователя). Таким образом, современные информационно-расчётные системы и вычислительные сети военного назначения являются по своей природе сложными эргатическими системами, функционирующими в условиях воздействий факторов рабочей среды с целями, определёнными их функциональным предназначением [3-4,5]. Структурная сложность и разнородность воздействующих на элементы системы факторов (в том числе действий пользователей системы) обусловлено целесообразностью проведения декомпозиции сложной системы на подсистемы. Декомпозиция рассматриваемой ИРС на составляющие и переход от общего рассмотрения сложноформализуемых и практически несопоставимых (в силу своей природы (в первую очередь – поведенческой неопределённости оператора) характеристик элементов к виду системы {угроза – мероприятия и средства защиты – уязвимость}, в которой возможно перечисление и формальное описание характеристик видов воздействующих факторов, условий функционирования системы и характеристик восприимчивости элементов системы к соответствующим видам воздействий. Рассматриваемый подход даёт потенциальную возможность представить описание процессов, происходящих в ходе эксплуатации ИРС в различных условиях обстановки, в виде формальной модели и определить методы её исследования и определения безопасности как качественной характеристики функциональной устойчивости и защищённости [3].

Проведенный сравнительный анализ подходов к расчету вероятности реализации угроз [4,5] – утрате функциональной устойчивости ИРС – и оценке вклада предпосылок в реализации угрозы в настоящее время производится пассивно, т.е. только по результатам реализации происшествия, что применительно к системам с высоким прогнозируемым значением риска (прежде всего к информационным системам, обеспечивающим актуальной информацией расчётно-аналитические центры и штабы группировок) или невозможно, или явно не удовлетворяет требованиям предупредительно-профилактической стратегии обеспечения безопасности. Кроме того, на практике часто остаются неизвестными: комплекс факторов, который способствовал реализации конкретного происшествия, текущее состояние потенциальных уязвимостей системы, а также образование объектом системы вторичных факторов угроз [5,6].

Отмеченные выше недостатки устраняются путем применения активных подходов в анализе и оценке безопасности сложных систем, к которым относится, в частности, метод факторного параметрического моделирования как самостоятельное направление теории возможностей, позволяющее получать точность значения риска порядка 10^{-4} в условиях неполноты или противоречивости исходных данных [2].

Исходными данными для решения задачи моделирования происшествий и оценки безопасности ИРС с помощью факторного параметрического метода являются:

- структурно-логическое описание ИРС и описание условий рабочей среды, в которых она функционирует: $Q_S = \{q^s_1, ..., q^s n\}$; $Q_a = \{q^a_1, ..., q^a_n\}$;
- техническое описание порядка эксплуатации и регламента доступа к структурным элементам ИРС в виде нормативно-распорядительных документов (инструкций, наставлений и т.п.): $I = \{i_1, ..., i_n\}$;
- множество факторов, рассматривающихся по отношению к ИРС в качестве угроз: $X=\{x_1,\ldots, x_n\}$;
- множество описаний ситуаций, в которых возможна реализация угроз: $S^F = \{s^F_1, \ldots, s^F_n\}$;
- множество описаний структурных элементов ИРС, рассматривающихся в качестве потенциальных уязвимостей ИРС: $D^F=\{d^F_1, ..., d^F_n\}$;
- множество описаний задач обеспечения функциональной устойчивости ИРС: $Z^F = \{z^F_1, ..., z^F_n\}$;
- множество мероприятий и средств противодействия угрозам ИРС: $H^F = \{h^F_1, ..., h^F_n\}$;
- множество описаний устройств, входящих в состав структурных элементов ИРС, в виде технических характеристик их восприимчивости к видам физических воздействий рабочей среды: $R = \{R_1, ..., R_\tau\}$;
- множество описаний факторов рабочей среды (условий боевой обстановки), в которой происходит функционирование элементов ИРС, в виде значений физических и информационных воздействий: $V = \{V_1, ..., V_\tau\}$;
- множество параметров ослабления / усиления воздействий факторов рабочей среды на элементы ИРС: $F = \{F_1, ..., F_\tau\}$;
- уровень точности оценки риска реализации угрозы (происшествия): $\xi_{\text{расч}} \le \xi_{\text{треб}}$;
- бюджет на организацию и обеспечение противодействия угрозам ИРС: $C_{\text{доп}}$.

Общий алгоритм методики, представленный на рис. 1, предполагает поэтапное выполнение следующих основных действий:

1. Инфологическое описание модели «оператор – рабочая среда – ресурс» (О–РС–Р): методами экспертного оценивания производится формирование переч-

ня приоритетных целей функционирования, ресурсов, внешних и внутренних угроз, воздействующих на ресурсы ИРС, мероприятий и средств защиты, оказывающих влияние на воздействие факторов рабочей среды.

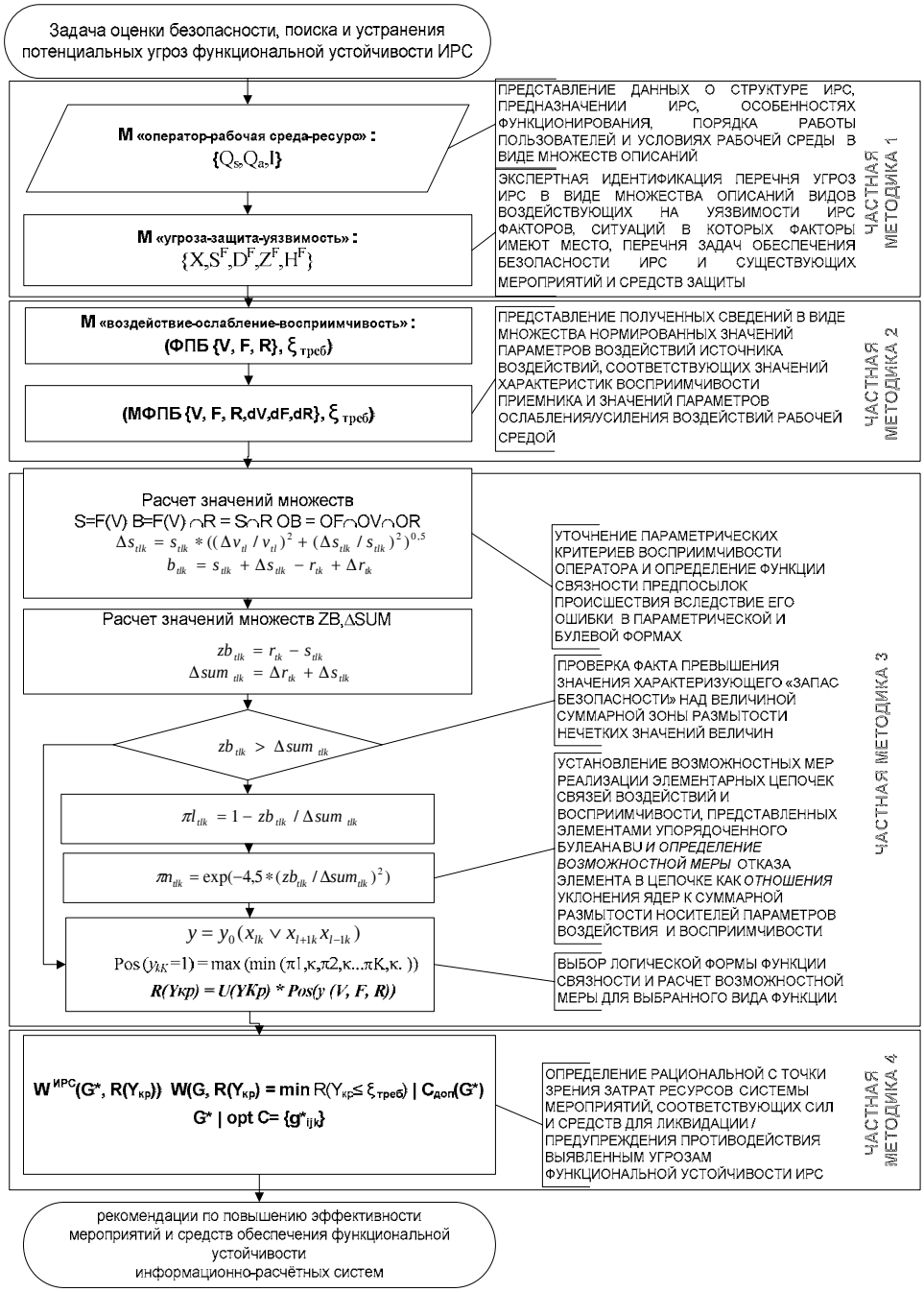

Рис. 1. Общая структура методики факторного параметрического моделирования утраты функциональной устойчивости ИРС

2. Идентификация угроз в ИРС: на основе анализа множеств Q_s, Q_a, G, описывающих модель «О–РС–Р» аналитической группой с применением экспертной системы, содержащей в базе данных описание типовых кризисных ситуаций в ИРС, приведших к утрате функциональной устойчивости, производится выявление и идентификация потенциальных угроз, поиск чувствительных к выявленным угрозам уязвимостей и их ранжирования в соответствии с важностью для устойчивого функционирования ИРС.

3. Построение факторного параметрического базиса (нумерация источников и приемников воздействий, в соответствии с рангом вида фактора рабочей среды; формирование упорядоченного булеана, элементы которого есть последовательности номеров источников и приемников видов воздействий), преобразование вида исходных данных описаний характеристик воздействий и восприимчивости к нечеткому виду (x – значение ядра величины, Δx – зона размытости величины на уровне α-среза).

4. Определение интегральных и дифференциальных мер риска реализации угроз функциональной устойчивости ИРС.

5. Определение рациональной системы методов (пригодной при фиксированном значении затрат на силы и средства обеспечения безопасности – $C_{доп}$ и оптимальном по критерию «эффективность ИРС» – при свободном показателе затрат) защиты ресурсов ИРС в целях недопущения утраты её функциональной устойчивости.

Концепция информационной технологии моделирования происшествий и динамической оценки безопасности информационно-расчётных систем базируется на идее распределённых сервисов реализующих «клиент-серверную» архитектуру, включающую в свой состав следующие основные элементы:

1. Рабочие места пользователей ресурсов ИВС, оснащённые системой датчиков и резидентных программ, контролирующих в режиме реального времени, изменение количественных и качественных характеристик ПОО ИВС.
2. Локальный модуль динамической оценки безопасности системы по данным текущего мониторинга «Возмер-Мониторинг», предназначенный для сбора, обработки данных от резидентных программных модулей и системы датчиков, размещённых в рабочей среде ИВС.
3. Протоколы и каналы передачи пакетов формализованных данных и неформализованных сообщений от клиентских мест (пользовательских терминалов ИВС) к центру обработки запросов (серверу).
4. Базу данных и базу правил (известных формализованных сценариев и факторно-параметрических описаний видов воздействий на ПОО ИВС) в составе экспертной системы.
5. Пакет специального программного обеспечения M.A.R.T.1.1 автоматизированной обработки экспертных оценок, моделирования происшествий в ИВС и автоматизированной генерации рекомендаций должностным лицам по предотвращению происшествия [8].

Модель функционирования системы описывается следующим образом:

- в соответствии с этапами предварительного структурного анализа ИВС экспертами по безопасности формируется факторно-параметрическая модель происшествий на ПОО ИВС. Пакет специального программного обеспечения «Возмер» использует в полученной модели информацию от системы датчиков параметров рабочей среды (температурно-влажностного режима, вибраций и т.д.), резидентных модулей (действия пользователей и прикладных программ);

- системных служб (износ жесткого диска, количество ошибок записи в оперативную память, температура графического ядра видеоподсистемы и т.д.) и в режиме реального времени осуществляет расчёт и мониторинг изменения качественного состояния защищённости системы в целом и отдельных её элементов, используя методы расчёта интегрального и дифференциального значений риска.

При возникновении нештатной ситуации (ситуации, не описанной экспертами в первичной факторно-параметрической модели ИВС) и/или добавлении новых элементов в ИВС формируется запрос в виде формализованного пакета с текущими значениями параметров ИВС и неформализованный пакет описаний (в том числе фото, видео, словесных и т.д.) происшествия или добавляемого в структуру ИВС объекта. Пакет описаний направляется по каналам передачи данных через подсистему приема и первичной обработки данных с клиентского места в службу моделирования безопасности (на сервер обработки запросов). Полученный пакет исходных для моделирования данных, подвергается экспресс-анализу специалистом службы информационно-технической поддержки.

В случаях применения экспертной системы производится: сопоставление факторно-параметрической модели с аналогичными в базе данных; поиск наиболее адекватной факторно-параметрической модели и достоверного сценария развития ситуации, затем производится моделирование вариантов реализации угроз с определением дифференциальных и интегральных значений возможностных мер утраты функциональной устойчивости ИРС. На основе выбранной из базы знаний модели оцениваемой ИРС определяется значение риска происшествия и формируется перечень рекомендаций на основе типовых решений, выбранных автоматизированной интеллектуальной системой поддержки принятия решения «ИРС-Эксперт».

Анализ современных подходов к решению задачи моделирования безопасности сложных и уникальных эргатических систем и оценки риска реализации потенциальной угрозы в таких системах позволил установить возможность решения данной задачи методом факторно-параметрического анализа.

Применение факторно-параметрического метода для оценки интегрального и дифференциальных рисков реализации угрозы функциональной устойчивости ИРС позволило получить количественные значения возможностной меры риска выхода из строя элементов системы даже в условиях неполноты и противоречивости информации, как о характеристиках факторов угроз, так и о степени уязвимости самой ИРС.

Экспериментальная проверка достоверности полученных результатов изложенная в [9] подтвердила возможность использования методики для определения рационального состава мероприятий и средств защиты функциональной устойчивости ИРС в условиях прогнозируемых и реализующихся в рабочей среде угроз и выработать комплекс рекомендаций должностным лицам организаций (подразделений) по вариантам противодействий угрозам безопасности ИРС в различных условиях обстановки.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. ГОСТ Р ИСО/МЭК 15408-1–1999. Методы и средства обеспечения безопасности.
2. *Есипов Ю.В, Самсонов Ф.А., Черемисин А.И.* Мониторинг и оценка риска систем. – М.: Издательство ЛКИ, 2008. – 136 с.
3. *Махутов Н.А.* Научные проблемы безопасности техногенной сферы // Проблемы машиностроения и надежности машин. – 1999. – № 1. – С. 109-116.
4. *Орловский С.А.* Проблемы принятия решений при нечеткой исходной информации. – М.: Наука, 1981. – 231 с.
5. *Острейковский В.А.* Теория систем. – М.: Высшая Школа, 1997. – 240 с.
6. *Рябинин И.А.* Надежность и безопасность структурно - сложных систем. – СПб.: Политехника, 2000. – 248 с.

7. Федеральный закон РФ от 10 января 2003 г. N 24-ФЗ "Об информации, информатизации и защите информации".
8. *Самсонов Ф.А., Есипов Ю.В.* Методика и программный продукт «Возмер 2.3» для расчета дифференциальных и интегральных показателей риска // Моделирование и анализ безопасности и риска в сложных системах: Труды международной научной школы МА БР – 2008. – СПб.: Изд-во СПбГУАП, 2008. – С. 350-353.
9. *Самсонов Ф.А.* Экспериментальная проверка пригодности факторной параметрической модели для оценки безопасности распределённых ИРС и локальных ВС // Сборник материалов межвузовской военно-научной конференции № 7 «Проблемы управления поддержанием боевой готовности соединений и частей в условиях повседневной и боевой деятельности». – Ростов-на-Дону: РВИ РВ. – 2008, Инв. №12/532 ДСП. – С. 107-113.

Самсонов Филипп Анатольевич
Ростовский военный институт ракетных войск.
E-mail: phas@aaanet.ru.
344037, г. Ростов-на-Дону, пр. Нагибина, 24/50.
Тел.: +79281852411.

Костюченко Иван Иванович
E-mail: kostuchen@rambler.ru.
Тел.: +79081938152.

Петров Михаил Валентинович
E-mail: phas@aaanet.ru.
Тел.: +79054512183.

Наконечный Виталлий Николаевич
E-mail: kostuchen@rambler.ru.
Тел.: +79281763251.

Samsonov Filipp Anatolyevich
Rostov Military Institute of Rocket Troops
E-mail: phas@aaanet.ru.
24/50, M. Nagibina pr., Rostov-on-Don, 344037, Russia.
Phone: +79281852411.

Kostuchenko Ivan Ivanovich
E-mail: kostuchen@rambler.ru.
Phone: +79081938152.

Petrov Mikhail Valentinovich
E-mail: phas@aaanet.ru.
Phone: +79054512183.

Naconechnyi Vitallyi Nicolaevich
E-mail kostuchen@rambler.ru.
Phone: +79281763251.

УДК 539.3

О.А. Губеладзе, С.В. Федоренко, А.В. Цыбенко

ЭКСПРЕСС ОЦЕНКА СИЛЫ СОПРОТИВЛЕНИЯ ПРЕГРАДЫ ПРИ ВЗАИМОДЕЙСТВИИ С ТРАНСПОРТНО-УПАКОВОЧНЫМ КОМПЛЕКТОМ ПРИ ПАДЕНИИ

Рассматривается задача определения силы сопротивления грунта как сплошной среды, изменяющей плотность при действии сжимающих нагрузок, возникающих при соударении с ним транспортно-упаковочного комплекта (контейнера с приборами). Найденное