УДК 681.3

И.Г. Дровникова[1], И.Н. Селютин[2], Д.И. Коробкин[3], М.В. Питолин[4]
([1]Воронежский институт МВД России; Воронежский институт правительственной связи (филиал) Академии ФСО России, [3]ВУНЦ ВВС "ВВА", [4]Воронежский институт МВД России; e-mail: idrovnikova@mail.ru)

О ТРЕБОВАНИЯХ К ПОКАЗАТЕЛЯМ КАЧЕСТВА ФУНКЦИОНИРОВАНИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Предложен метод обоснования требований к показателям качества программных средств защиты информации от несанкционированного доступа, основанный на использовании теоретико-игровой модели.

Ключевые слова: генетический алгоритм, эволюционная модель, безопасность информации, несанкционированный доступ.

I.G. Drovnikova, I.N. Selutin, D.I. Korobkin, M.V. Pitolin

ABOUT REQUIREMENTS TO QUALITY CHARACTERISTICS FUNCTIONING OF MEANS INFORMATION PROTECTION OF THE AUTOMATED SYSTEMS

We propose a method to substantiate claims about the quality characteristics, programmatic information security systems from unauthorized access, based on the use of game-theoretic model.

Key words: genetic algorithm, evolutionary model, safety of the information, not authorised access.

Статья поступила в редакцию Интернет-журнала 17 февраля 2015 г.

В настоящее время практически нет такой сферы деятельности, где бы ни использовалась ***вычислительная техника (ВТ)*** и ***автоматизированные системы управления (АСУ)***.

Процесс широкого внедрения ВТ и АСУ в структуры управления также затронул и системы управления ядерным оружием, высшими органами государственной власти, кредитно-финансовых учреждений.

Такие области применения ВТ и новых информационных технологий принято называть ***критическими***, что обусловлено исключительной важностью вопросов, решаемых данными системами и размером ущерба или других последствий, которые могут наступить из-за нарушения их работоспособности, отказов и сбоев в работе.

В связи с этим в системах критических приложений на первый план выходят задачи обеспечения надёжности их функционирования, и в частности, информационной безопасности (защиты информации).

Как показал опыт эксплуатации АСУ критических приложений, наибольший вклад в нарушение информационной безопасности этих систем вносят факты ***несанкционированного доступа (НСД)*** к информации [1, 2].

Под НСД, согласно существующей нормативной документации [3], понимается доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых вычислительной техникой или автоматизированными системами. Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения вычислительной техники или автоматизированных систем.

На состояние информационной безопасности отечественных АСУ оказывает влияние их построение на основе международных стандартов реализующих модель взаимодействия открытых систем. В связи с этим архитектура и основные технические решения изначально рассчитаны на возможность легкого изменения конфигурации, добавления новых аппаратных и программных компонент. Также в настоящее время практически все аппаратное обеспечение (ВТ, средства телекоммуникаций) отечественных АСУ строится на импортной элементной базе, так как уровень развития отечественной элементной базы не удовлетворяет современным требованиям ни по массогабаритным показателям, ни по быстродействию. Практически все системное и общесистемное программное обеспечение, используемое при создании АСУ, является импортным.

Сложившееся противоречие между современными тенденциями развития отечественных АСУ и необходимостью защиты информации от НСД в настоящее время преимущественно решается с использованием ***программных средств защиты информации (ПСЗИ)*** [1, 2, 4].

Разработка внедрение и эксплуатация этих систем осуществляется в соответствии с Руководящими Документами Гостехкомисии РФ [4-6], определяющими функциональные требования по ЗИ от НСД. Также разработан и вводится в действие ряд стандартов, определяющих необходимость создания ПСЗИ при разработке АСУ [7].

Однако рассмотренная нормативная документация по защите информации предъявляет требования к ПСЗИ достаточно узко, и ограничивается функциональными требованиями. Остальные характеристики выбираются исходя из личного опыта разработчика в связи с тем, что в нормативной документации, посвященной качеству ПС [8], системы показателей, характеризующих качество ПСЗИ, нет.

Таким образом складывается ситуация отсутствия формального взаимодействия и взаимопонимания разработчиков ПСЗИ с заказчиком или потенциальным пользователем данной системы уже на начальном этапе проектирования – уточнения требований к механизмам реализации требуемых функций программы и утверждения требований к её качеству. Что, в свою очередь, приводит к возникновению ошибок, обусловленных неопределенностью или некорректностью технических заданий и спецификаций требований. Тем самым не обеспечиваться поступательный ход процесса разработки ПСЗИ без возвратов для уточнения или переделки компонентов или даже всего комплекса программ. Обширной практикой доказано, что обнаружение и устранение ошибок в комплексах программ на начальных этапах проектирования в десятки и сотни раз быстрее и дешевле, чем в процессе завершения разработки и испытаний [9].

Целью данной статьи является разработка методических основ обоснования требований к характеристикам качества ПСЗИ при их проектировании на основе анализа особенностей функционирования в составе АСУ критических приложений.

Основой для формирования системы показателей, по которым возможно обоснование требований к ПСЗИ, является анализ её свойств и особенностей, характеризующих качество её функционирования в составе программного обеспечения АСУ критических приложений. При этом под качеством функционирования, понимается множество свойств, обуславливающих пригодность ПСЗИ выполнять свои функции.

В соответствии с существующей отечественной и международной нормативной документацией в области качества ПС можно выделить 6 групп характеристик, которые целесообразно использовать при анализе и обосновании требований к ПСЗИ как к сложным ПС [8]:

- функциональность;
- надёжность;
- эффективность;
- удобство использования;
- сопровождаемость;
- мобильность.

Под ***функциональностью ПСЗИ*** понимается совокупность свойств программного средства, определяемая наличием и конкретными особенностями набора функций, способных удовлетворять заданные или подразумеваемые потребности.

Под ***надёжностью ПСЗИ*** понимается совокупность свойств, характеризующая способность программного средства сохранять заданный уровень пригодности в заданных условиях в течение заданного интервала времени.

При этом считается, что программное средство не подвержено износу или старению. Ограничения его уровня пригодности являются следствием дефектов, внесенных в содержание программного средства в процессе постановки и решения задачи его создания или модификации. Количество и характер отказов программного средства, являющихся следствием этих дефектов, зависят от способа применения программного средства и от выбираемых вариантов его функционирования.

Надёжность программных средств, являющихся частью конкретной системы обработки информации, может входить в состав признаков её качества наряду с её надёжностью как технической системы.

Под ***удобством использования ПСЗИ*** понимается совокупность свойств программного средства, характеризующая усилия, необходимые для его использования, и индивидуальную оценку результатов его использования заданным или подразумеваемым кругом пользователей программного средства.

Под ***эффективностью ПСЗИ*** понимается совокупность свойств программного средства, характеризующая те аспекты его уровня пригодности, которые связаны с вероятностно-временными характеристиками выполнения функциональных задач и используемых при этом ресурсов АСУ, необходимых при заданных условиях функционирования.

При этом ресурсы могут включать другие программные средства, технические средства, материалы (бумагу, гибкие магнитные диски и др.), услуги различных категорий персонала.

Под ***сопровождаемостью ПСЗИ*** понимается совокупность свойств программного средства, характеризующая усилия, которые необходимы для его модификации. Модификация может осуществляться для устранения дефектов, усовершенствования программного средства или его адаптации к изменениям в условиях функционирования, а также в составе и особенностях требуемых функций.

Под ***мобильностью ПСЗИ*** понимается совокупность свойств программного средства, характеризующая его приспособленность для переноса из одной среды функционирования в другие.

Обоснование требований к ПСЗИ, как к сложным ПС, в общем случае формальными методами – достаточно нетривиальная задача из-за сложности взаимосвязи элементов АСУ, большого числа возможных угроз и, как правило, отсутствия достаточной информации об их статистических характеристиках.

Поэтому при обосновании требований к ПСЗИ предполагается ограничится рассмотрением случая, когда:

- определено разбиение множества угроз НСД на обобщённые угрозы (то есть подмножества, состоящие из угроз НСД, сходных по оказываемому на АСУ воздействиям и типовым сценариям возникновения НСД);
- определено множество классов защищённости, в соответствии с которыми может быть сертифицирована АСУ;
- для каждой пары "класс защищённости – обобщённая угроза" могут быть получены оценки ущербов в случае возникновения НСД.

Для решения задачи обоснования требовании к характеристикам качества ПСЗИ предлагается использовать конечную теоретико-игровую модель. При этом предполагается рассмотреть антагонистическую игру двух сторон: 1 – ПСЗИ, осуществляющие защиту информации в АСУ, и 2 – нарушитель (источник НСД).

Возможные стратегии первой стороны состоят в осуществлении, предписанных различными классами защищенности функций с различным функциональным уровнем (различными значениями показателей качества ПСЗИ, характеризующими её как сложную ПС). Возможные стратегии второй стороны – осуществление одного из определённого множества НСД с различными характеристиками.

Незначительно снижающим точность модели, но существенно упрощающим расчёты будет предположение о том, что действия каждой из сторон или являются однократными или могут быть сведены к некоторому однократному воздействию. Данное предположение позволит использовать одношаговую игровую антагонистическую модель.

Таким образом, имеется множество функций ПСЗИ $F = \{F_1, F_2, ..., F_n\}$, каждый элемент которого $F_i \subset F$ характеризуется соответствующим функциональным состоянием $\{f_1, f_2, ..., f_n\}$, описывающим возможные требования к этой функции как сложной ПС, основное содержание которых описано ранее.

Обозначим класс защищённости, которому соответствует АСУ, – *C*, тогда множество стратегий первой стороны (ПСЗИ) будет описываться следующим кортежем:

$$C_i = \langle C, f_{i1}, f_{i2}, ... f_{in} \rangle,$$

где f_{ij} – *j*-й показатель качества ПСЗИ, реализованный при классе защищённости *C* при *i*-й стратегии.

Таким образом, каждая *i*-я стратегия первой стороны – это ПСЗИ, обеспечивающие класс защищённости C с характеристиками качества f_{ij}.

Примером показателей качества f_{ij} для характеристик надёжности $f_{1i} = \{0{,}1; 0{,}2; ...; 0{,}9\}$ значения коэффициента готовности $K_г$ при выполнении защитной функции, показателей эффективности $f_{2i} = \{1, 2, ..., K\}$ значения среднего времени выполнения функции (точного времени выполнения функции при наличии профиля программы) $\bar{\tau}_i(\tau_i)$, характеризующего временную эффективность и т.п.

Аналогичным образом можно построить множество стратегий второй стороны (нарушителя – источника НСД).

Каждая стратегия второй стороны описывается кортежем:

$$U_k = \langle name, u_{k1}, u_{k2}, ..., u_{km} \rangle,$$

где *name* – условное наименование обобщённой угрозы НСД;

u_{kl} – показатели, характеризующие процесс возникновения НСД.

Используя множества стратегий C_i и U_k можно задать антагонистическую игру:

$$\Gamma = \langle C, U, H \rangle,$$

где H – матрица выигрыша вида:

$$H = \begin{bmatrix} -h_1 - h_{11} & -h_1 - h_{12} & . & -h_1 - h_{1m} \\ -h_2 - h_{21} & -h_2 - h_{22} & . & -h_2 - h_{2m} \\ . & . & . & . \\ -h_n - h_{n1} & . & . & -h_n - h_{mn} \end{bmatrix};$$

h_i – затраты на реализацию стратегии i первой стороны (затраты на реализацию ПСЗИ с функциональным уровнем f_i);

h_{ik} – значения ущербов, возникающих при возникновении *k*-го НСД при *i*-й стратегии первой стороны (ПСЗИ с функциональным уровнем f_i).

Знак "–" взят для обоих составляющих выигрыша первой стороны, так как для неё затраты на защиту информации и ущербы от возникновений НСД являются отрицательными величинами.

Обоснование требований к ПСЗИ предполагается осуществить на основе полученного решения игры $\Gamma = \langle C, U, H \rangle$, минимизирующей как затраты на проведение защитных мероприятий, так и ущербов от возникновений НСД, то есть требованиями к характеристикам качества ПСЗИ будут значения f_j, составляющие решение игры. Таким образом, решение игры в чистых стратегиях ясно укажет требования к характеристикам качества ПСЗИ, при которых значения затрат на защиту информации и ожидаемые потери от возникновения НСД минимальны.

Блок-схема алгоритма обоснования требований к ПСЗИ можно представить в виде, показанном на рис. 1.

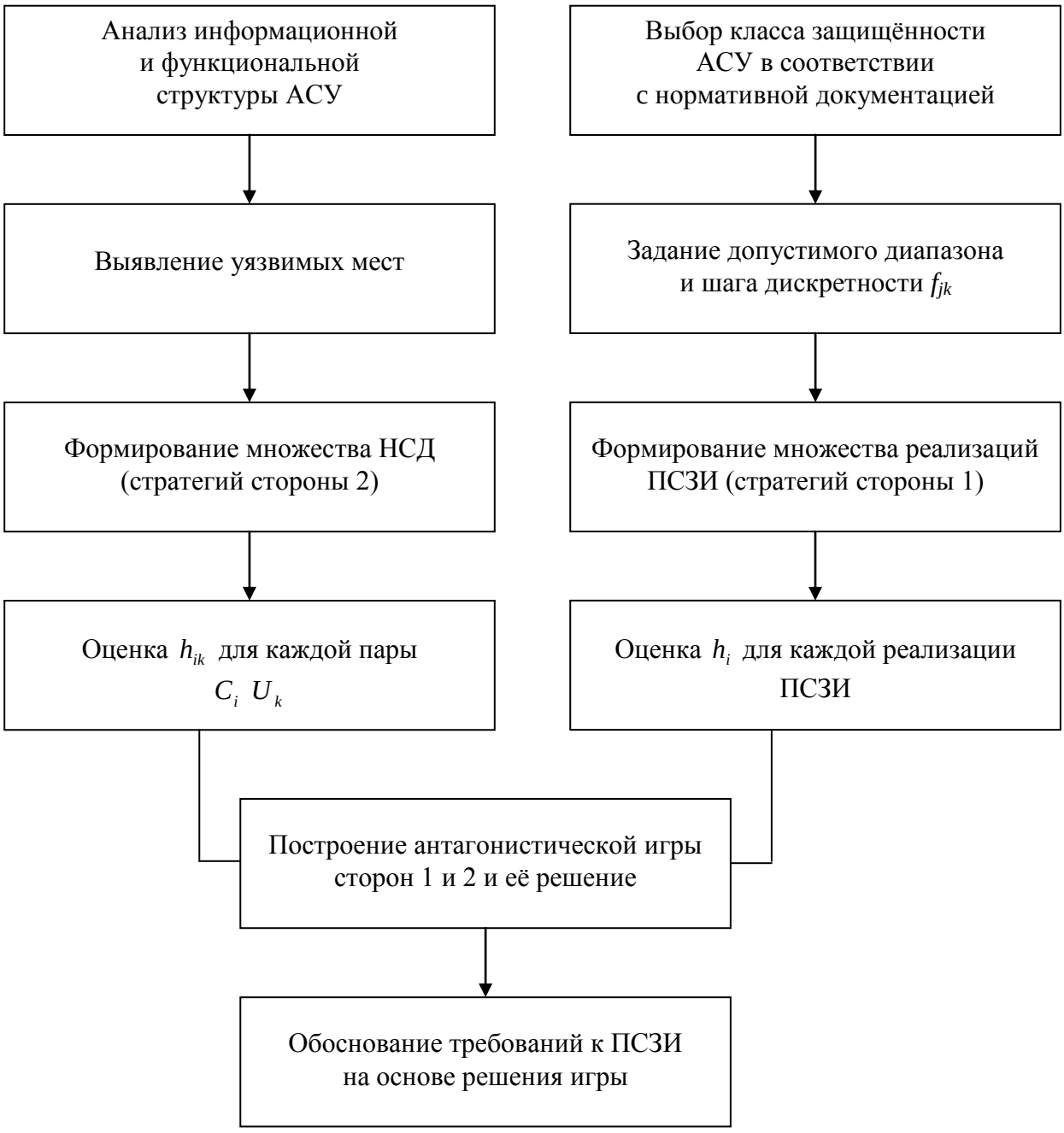

Рис. 1. Блок-схема алгоритма обоснования требований к ПСЗИ

Определение значений величины h_{ik} математических ожиданий ущербов от k-х НСД при i-х возможных реализациях ПСЗИ могут быть получены в ходе анализа рисков (как правило, для оценки внутренней стоимости информации может применяться метод экспертных оценок) с участием непосредственных владельцев информации.

При этом необходимо в интересах обоснования требований к вероятностно временным характеристикам ПСЗИ рассмотреть динамические характеристики возникающих НСД, то есть полученные в ходе оценки рисков элементы матрицы выигрышей первой стороны h_{ik} необходимо умножить на вероятность k-го возникновения НСД за некоторое максимально допустимое время, обусловленное характеристиками ПСЗИ, присущими i-й реализации (P_{ik}).

В связи с тем, что как среднее время возникновения НСД, так и временные характеристики ПСЗИ в общем случае – случайные величины, то для определения вероятности P_{ik} целесообразно использовать метод динамического конфликта, который, в сочетании с теорией случайных процессов, позволяет получить аналитическую модель взаимодействия конфликтующих сторон. При построении данной модели необходимо использовать метод полумарковских процессов, который позволяет получить наиболее адекватные модели с произвольными законами распределения переходных характеристик.

Таким образом, предлагаемый новый метод обоснования требований к характеристикам качества ПСЗИ позволяет построить формализованную процедуру, позволяющую на основе анализа функциональной схемы АСУ критических приложений и её основных информационных потоков получить численные значения показателей, характеризующих её как сложную ПС.

Литература

1. ***Герасименко В.А.*** Защита информации в автоматизированных системах обработки данных: в 2-х кн.: кн. 1. М.: Энергоатомиздат, 1994. 400 с.
2. ***Мельников В.В.*** Защита информации в компьютерных системах. М.: Финансы и статистика; Электронинформ, 1997. 368 с.
3. ***Гостехкомиссия*** России. Руководящий документ. Зашита от несанкционированного доступа к информации. Термины и определения. М.: Воениздат, 1992.
4. ***Гостехкомиссия*** России. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. М.: Воениздат, 1992.
5. ***Гостехкомиссия*** России. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. М.: Воениздат, 1992.
6. ***Гостехкомиссия*** России. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации. М.: Воениздат, 1992.
7. ***ГОСТ*** Р 50739-95. Средства вычислительной техники. Защита информации от несанкционированного доступа.
8. ***ГОСТ*** 28195-89. Оценка качества программных средств. Общие положения.
9. ***Липаев В.В.*** Качество программного обеспечения. М.: Финансы и статистика, 1983. 263 с.