А. А. Тарасов, Д. И. Коробкин

АЛГОРИТМ ОЦЕНКИ ДИНАМИЧЕСКОГО ПОКАЗАТЕЛЯ ЭФФЕКТИВНОСТИ ПРОГРАММНЫХ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ИХ РАЗРАБОТКЕ

В качестве объекта исследования воспользуемся широко распространенной ПСЗИ «Спектр-Z», которая соответствует требованиям руководящих документов.

Для оценки показателя эффективности ПСЗИ «Спектр-Z» «динамическая устойчивость» рассмотрим ситуацию предотвращения попытки несанкционированного доступа (НСД) к ПСЗИ с целью уничтожения информации в ее базе данных. Содержание алгоритма вычислительного эксперимента следующее.

С целью исследования ПСЗИ в распределенную вычислительную сеть АСУ специального назначения (СН) в обход подсистемы закрытия внедряется компьютерный вирус-закладка типа «троянский конь». Этим вирусом осуществляется контроль прерываний устройств ввода паролей при инициировании пользователями работы с подсистемами обеспечения санкционированного доступа, детального разграничения полномочий доступа, разграничения доступа к ресурсам ЭВМ и регистрации доступа.

Для предотвращения попытки исследования подсистем организации доступа к АСУ СН на первом уровне защиты ПСЗИ «Спектр-Z» с помощью подсистемы закрытия реализуются операции закрытия доступа к ресурсам ПЭВМ через системную дискету, а также на втором уровне защиты ПСЗИ при помощи подсистем обеспечения санкционированного доступа, детального разграничения полномочий доступа, разграничения доступа к ресурсам ЭВМ и регистрации доступа осуществляются операции идентификации и аутентификации.

В случае обнаружения этими подсистемами некорректных состояний ПСЗИ подсистема поддержания целостности рабочей среды ПЭВМ производит обнаружение несанкционированных изменений в рабочей среде ПЭВМ, искажений в программах и ключевой информации АСУ СН, поиск с помощью антивирусных средств вредоносных программ и их подавление.

Если цели злоумышленника на первом этапе достигнуты и в его распоряжении находятся идентификационные пароли ПСЗИ, то при помощи разработанных программ контроля основных подсистем ПСЗИ осуществляется проникновение в АСУ СН с целью исследования механизма шифрования программ и данных АСУ СН подсистемой преобразования информации ПСЗИ.

Для предотвращения попытки исследования основных подсистем ПСЗИ на втором уровне ее защиты ПСЗИ при помощи подсистемы обеспечения целостности рабочей среды осуществляется обнаружение вирусных программ злоумышленника и их подавление.

Если цели злоумышленника на втором этапе достигнуты и в его распоряжении находятся как идентификационные пароли ПСЗИ, так и шифры программ преобразования информации, то при помощи разработанных программ манипулирования информацией в АСУ СН осуществляется вскрытие ПСЗИ и проникновение в АСУ СН с целью определения (вызова) интересующих злоумышленника файлов и уничтожения (стирания) информации в них.

Если программы злоумышленника обнаруживаются подсистемой обеспечения целостности рабочей среды, то они уничтожаются.

В качестве злоумышленника выбирается один или несколько специалистов наивысшей квалификации в области информационной безопасности. Составляется план проведения эксперимента. В нем определяются очередность и материально-техническое обеспечение проведения экспериментов по определению уязвимых мест в ПСЗИ (например, максимальное время выполнения

ПСЗИ защитных функций). При этом могут моделироваться действия злоумышленников, соответствующие различным моделям нарушителей: от неквалифицированного злоумышленника, не имеющего официального статуса в исследуемой АСУ СН, до высококвалифицированного сотрудника службы безопасности [1].

Служба безопасности до момента преодоления защиты «злоумышленниками» должна ввести в ПСЗИ новые механизмы защиты (модифицировать), чтобы избежать «взлома» ПСЗИ.

Такой подход к оценке эффективности позволяет получать объективные данные о возможностях существующих ПСЗИ, но требует высокой квалификации исполнителей и больших материальных и временных затрат. Для проведения экспериментов необходимо иметь самое современное оборудование (средства инженерно-технической разведки, аппаратно-программные и испытательные комплексы (стенды) и т. п.) [1].

Способом оценки устойчивости программных средств и комплексов ЗИ, характеристики которых часто невозможно получить с помощью измерений, является моделирование (аналитическое, имитационное) процессов их функционирования с целью определения их вероятностно-временных характеристик. Эти характеристики позволяют представить основной показатель эффективности в вероятностной форме.

Предлагаемая методика моделирования основана на использовании механизма реализации защитных функций, что соответствует основным требованиям и положениям нормативных документов ФСТЭК России [2], где наличие соответствующих функций является условием отнесения ПСЗИ к определенному классу защищенности.

Для анализа работы программных средств (СрЗИ) их представляют в виде функциональной модели, с помощью которой функционирование ПСЗИ рассматривается как последовательное выполнение задач. Каждая из них связана с реализацией набора определенных защитных функций, что позволяет представить исследуемый процесс в виде последовательной смены состояний ПСЗИ, соответствующих выполнению конкретных защитных функций.

Такая структурно-функциональная модель представляется полумарковским поглощающим процессом с конечным числом состояний. Закон распределения времени пребывания ПСЗИ в каком-либо состоянии полагается нормальным. В соответствии с теорией конечных полумарковских процессов функционирование ПСЗИ можно описать системой уравнений для производящих функций, что позволяет выразить показатель устойчивости с помощью аналитических моделей.

При этом в качестве функциональной модели ПСЗИ используем ее представление в виде графа, вершинам которого соответствуют состояния (задачи), а ребрам — переходы между состояниями. При этом вершина 1 соответствует начальному состоянию, а вершина n — конечному состоянию. Начальное состояние соответствует моменту времени обращения к ПСЗИ, конечное — моменту времени окончания реализации защитных функций по данному обращению. Таким образом, τ_ρ — это промежуток времени от момента входа ПСЗИ в начальное состояние (соответствующее вершине 1) до момента входа ПСЗИ в конечное состояние (соответствующее вершине n).

Предложенные математическая модель и методика анализа устойчивости функционирования ПСЗИ характеризуются отсутствием ограничения на структуру графа состояний и позволяют получить аналитические выражения для оценки показателя устойчивости.

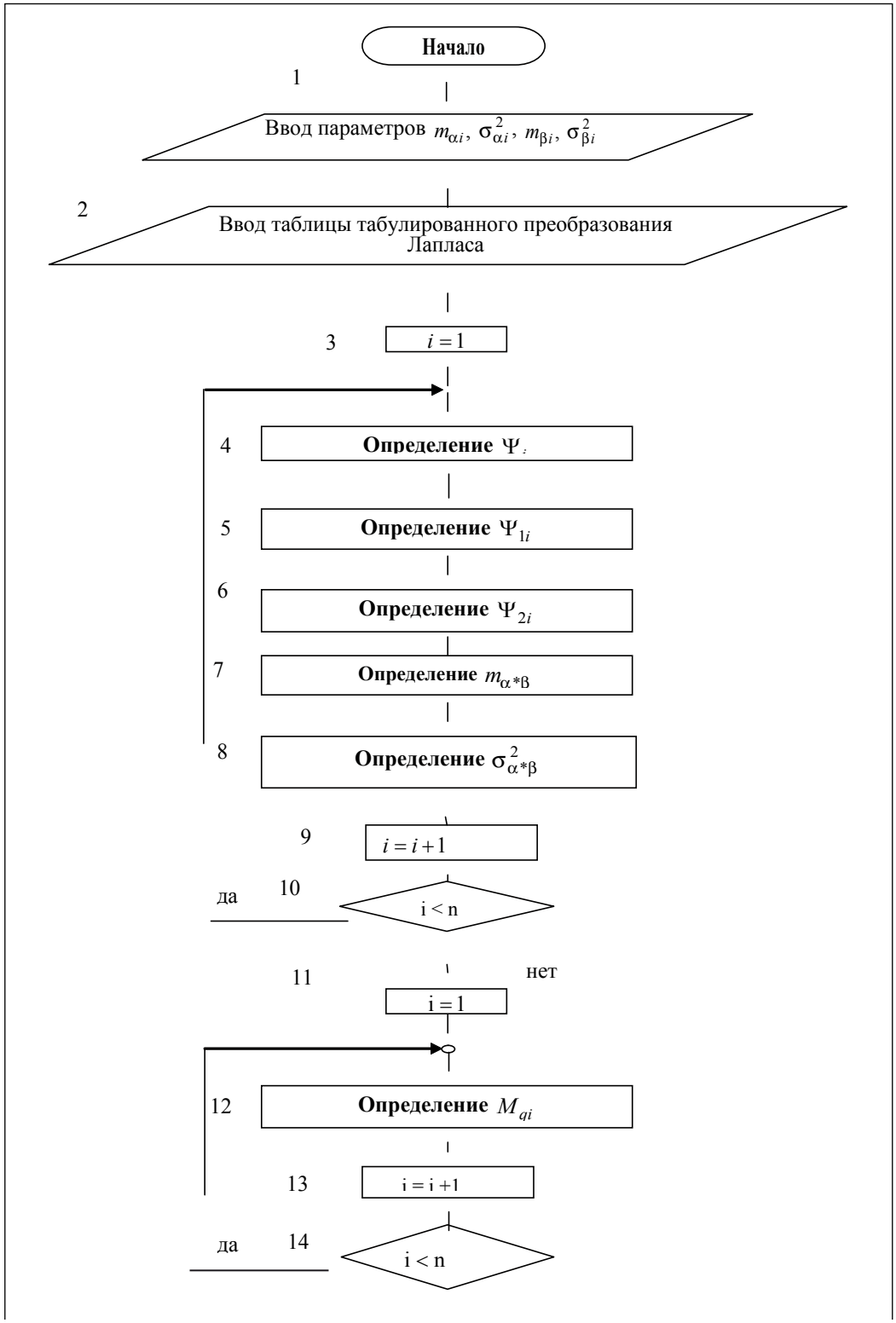
На рис. 1 представлена структурная схема алгоритма моделирования оценки «динамической устойчивости» ПСЗИ от НСД. Работа алгоритма осуществляется следующим образом.

Исходные данные (блок 1): $m_{\alpha i}$, $\sigma^2_{\alpha i}$ — среднее значение (математическое ожидание) и дисперсия нормального распределения, аппроксимирующего плотность распределения вероятностей (ПРВ) времени решения задачи стороной α (атакующая сторона); $m_{\beta i}$, $\sigma^2_{\beta i}$ — среднее значение (математическое ожидание) и дисперсия нормального распределения, аппроксимирующего ПРВ

времени решения задачи стороной β (ПСЗИ); $i = \overline{1,n}$ — идентификатор времени пребывания атакующей стороны или ПСЗИ в состоянии i.

$F(L)$ — табулированное преобразование Лапласа (блок 2) $L = \dfrac{m_\alpha - m_\beta}{\sqrt{\sigma_\alpha^2 + \sigma_\beta^2}}$.

Устанавливается значение 1 счетчика i состояний функционирования ПСЗИ (блок 3).



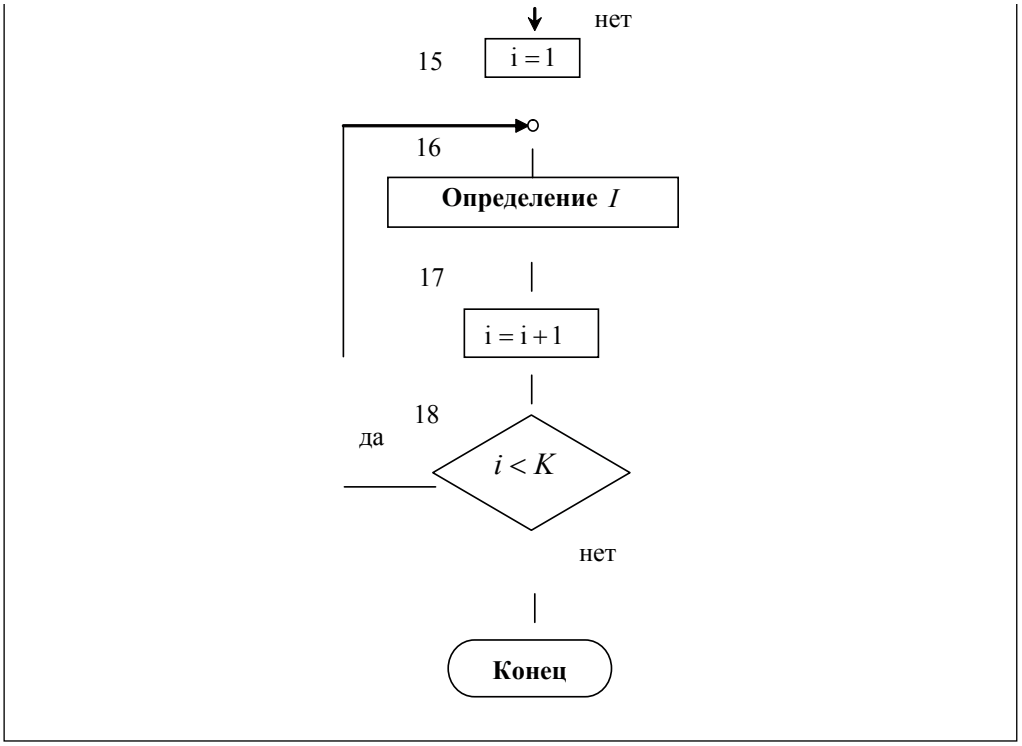


Рис. 1. Алгоритм оценки количественного показателя ПСЗИ «Спектр-Z»

Осуществляется переход ПСЗИ (злоумышленника) из состояния i в состояние $i+1$ (блок 9).

Проверяется условие выхода из цикла (блок 10).

Устанавливается значение 1 счетчика i (блок 11).

Определяются значения M_{qi} — коэффициенты нормировки соответствующих ПРВ (блок 12), здесь qi — индексы, раскрывающие последовательность эквивалентных подстановок, в результате которых получена данная ПРВ и коэффициент нормировки:

$q1 = S1 * N1,$

$q2 = (N1 * S1) + (S2 * N2),$

$q3 = (N1 * S1) + (N2 * S2) + (S3 * N3),$

$q4 = (N1 * S1) + (N2 * S2) + (N3 * S3) + (S4 * N4),$

$q5 = (N1 * S1) + (N2 * S2) + (N3 * S3) + (N4 * S4) + (S5 * N5),$

$q6 = (N1 * S1) + (N2 * S2) + (N3 * S3) + (N4 * S4) + (N5 * S5) + (S6 * N6),$

$q7 = (N1 * S1) + (N2 * S2) + (N3 * S3) + (N4 * S4) + (N5 * S5) + (N6 * S6) + (S7 * N7).$

Увеличивается значение счетчика i на 1 (блок 13).

Проверяется условие выхода из цикла (блок 14).

Устанавливается значение 1 счетчика i (блок 15).

Определяется значение показателя устойчивости ПСЗИ от НСД

$$I = P(\tau_S \le \tau_N) = \int_0^\infty [M_{q1}\omega_{q1}(\tau) + M_{q2}\omega_{q2}(\tau) + M_{q3}\omega_{q3}(\tau) + M_{q4}\omega_{q4}(\tau) + M_{q5}\omega_{q5}(\tau) + M_{q6}\omega_{q6}(\tau) + M_{q7}\omega_{q7}(\tau)]d\tau$$

(блок 16) и выводится текущее значение интеграла на экран (строим график).

Увеличивается значение счетчика i на 1 (блок 17).

Проверяется условие выхода из цикла (блок 18).

Рассмотренный алгоритм оценки показателя эффективности ПСЗИ «динамическая устойчивость» является основой для разработки программно-технического комплекса для оценки этого параметра.

СПИСОК ЛИТЕРАТУРЫ:

1. *Застрожнов И. И., Коробкин Д. И., Окрачков А. А., Рогозин Е. А.* Математическая модель оценки устойчивости при проектировании систем защиты информации // Вестник ВГТУ. Сер. Радиоэлектроника и системы связи. 2008. Том 5. № 6. 2008.
2. Гостехкомиссия России. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. М.: Воениздат, 1992.