УДК 681.3

И.Г. Дровникова[1], Е.А. Рогозин[2], Д.И. Коробкин[3], А.А. Змеев[4]
([1]Воронежский институт МВД России; [2]Воронежский институт МВД России,
[3]ВУНЦ ВВС "ВВА", [4]Военная академия ВКО им. Г.К. Жукова; e-mail: idrovnikova@mail.ru)

ЭВОЛЮЦИОННЫЕ МЕТОДЫ ОБОСНОВАНИЯ ТРЕБОВАНИЙ К СИСТЕМАМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Приводятся возможные направления применения эволюционных методов при обосновании требований к системам обеспечения техносферной безопасности и возможные перспективы доработки нормативных документов, регламентирующих вопросы обеспечения безопасности информации.

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

I.G. Drovnikova, E.A. Rogozin, D.I. Korobkin, A.A. Zmeev

EVOLUTIONARY METHODS TO SUBSTANTIATION REQUIREMENTS TO SAFETY SYSTEMS OF INFORMATION IN AUTOMATED SYSTEMS

The possible areas of application of evolutionary methods in justifying system requirements technospheric security and possible prospects for revision of regulatory documents that regulate the issues of information security is given.

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

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

Одной из важнейших задач теории безопасности информации является обоснование требований ***к средствам защиты информации автоматизированных систем (СЗИ АС)***. Важность данной задачи обусловлена высокой степенью влияния уровня защищённости информации на эффективность функционирования АС и как следствие на эффективность выполнения технологических процессов, в которых задействована АС. Важность данной задачи обусловлена тем, что результатом её решения является определение оптимальной части ресурсов вычислительной системы, которые допустимо выделить на эксплуатацию (функционирование) СЗИ, при условии обеспечения заданного уровня эффективности АС.

На сегодняшний день методической основой обоснования требований к подсистеме ***информационной безопасности (ИБ АС)*** при проектировании являются руководящие документы Федеральной службы технического и экспортного контроля России (ФСТЭК) [1-3]. Задание требований состоит в соотнесении его с одним из классов защищенности. Аналогичный подход используется во вновь вводимом в России международном стандарте "Общие критерии оценки безопасности информационных технологий" ISO/IEC 15408: 1999.

"Информационная технология – Методы и средства защиты информации – Критерии оценки безопасности информационных технологий" ***"Общие критерии" (ОК)***. Место класса в ОК занял ***профиль защиты (ПЗ)*** [4].

Профиль защиты представляет собой фактически перечень защитных функций, обязательных к реализации в данном классе. Нормативная документация задает фактически перечень функций, которые должны выполнять СЗИ, чтобы соответствовать определенному классу защищенности.

Таким образом, в РД ФСТЭК России требований и методик к нормированию и оценки эффективности подсистемы ИБ АС не содержится. В "Общих критериях" (ОК) вводится понятие ***стойкости функции безопасности (Strength of Function (SOF))***. Согласно ОК, может быть заявлен уровень или специальная метрика стойкости для каждой функции. Анализ стойкости функций выполняют для принятия решения, отвечают ли такие функции сделанным заявлениям. Например, анализ стойкости механизма пароля может, показав достаточность области задания пароля, продемонстрировать, что функция, использующая этот механизм, отвечает заявленной стойкости.

Предлагается использовать три уровня стойкости функций безопасности: SOF-basic (уровень стойкости функции безопасности ОО, на котором, как показывает анализ, функция предоставляет адекватную защиту от случайного нарушения безопасности ОО нарушителями с низким потенциалом нападения), SOF-medium (уровень стойкости функции безопасности ОО, на котором функция предоставляет адекватную защиту от прямого или умышленного нарушения безопасности ОО нарушителями с умеренным потенциалом нападения), SOF-high (уровень стойкости функции безопасности ОО, на котором функция предоставляет адекватную защиту от тщательно спланированного и организованного нарушения безопасности ОО нарушителями с высоким потенциалом нападения). Однако физического описания метрики (показателя) стойкости функции безопасности и, соответственно, методик его нормирования и оценки ОК не содержат.

Применение в составе системы обеспечения ИБ в АС, разнородных по выполняемым функциям и эффективности защиты информации от НСД, программных средств защиты приводит к необходимости системного рассмотрения требований к БИ. При этом значимость свойств отдельных элементов СЗИ снижается, а на первый план выдвигаются общесистемные задачи – определение оптимальной структуры и режимов функционирования системы, организация взаимодействия между её элементами, учёт влияния внешней среды. При целенаправленном объединении элементов в систему последняя приобретает специфические свойства, изначально не присущие ни одной из её составных частей. При системном подходе учитываются свойства СЗИ, которые определяют взаимодействие элементов и оказывают влияние на АС в целом, а также на достижение поставленной цели безопасности [5, 6].

В соответствии с указанными проблемами в теории защиты информации, целью исследований является разработка методики обоснования количественных требований к уровню БИ, основанной на оценке эффективности ЗИ и оптимизации. При этом модель, предназначенная для оценки эффективности ЗИ, моделирующая обобщенный алгоритм реализации полного множества угроз НСД к информации в условиях реализации различных мер по защите информации, используется в качестве целевой функции задачи оптимизации.

При разработке модели защиты целесообразно использовать методы марковских процессов, которые позволяют получить наиболее адекватные модели случайных процессов с приемлемыми для практических расчётов вычислительными затратами [7, 8].

Основная идея построения вероятностной модели динамического конфликта "угроз БИ – СЗИ" заключается в переходе от независимого описания функционирования противоборствующих сторон безусловными вероятностно-временными характеристиками к описанию их взаимодействия конфликтно-обусловленными вероятностно временными характеристиками, отражающими выигрыш одной из сторон в случае опережающего выполнения ею своей задачи [9]. При этом математическое выражение марковской модели защиты имеет многопиковый вид, что приводит к проблемам преждевременной сходимости. Большое количество оптимизируемых переменных приводит к значительным вычислительным затратам.

В этой связи для решения задачи нормирования предлагается использовать ***методы эволюционного моделирования***. В основе метода лежат генетические алгоритмы, являющиеся адаптивными алгоритмами оптимизации, использующими как аналог механизма генетического наследования, так и аналог естественного отбора [10].

Генетические алгоритмы, по сравнению с градиентными методами оптимизации, обладают рядом преимуществ:

- не требуют никакой информации о поведении функции (например, дифференцируемости и непрерывности);
- разрывы, существующие на поверхности ответа, незначительно влияют на полную эффективность оптимизации;
- относительно стойки к попаданию в локальные оптимумы.

Обоснование требований к БИ с использованием марковской модели защиты с применением эволюционного метода сводится к построению генетического кода, представляющего структуру марковской модели защиты, подобно тому, как ДНК (дезоксирибонуклеиновая кислота) представляет фенотипические свойства организма. При этом "хромосома" (генетический код) эволюционной модели, используемой при обосновании требований к БИ, составляется в виде цепочек единиц и нулей, каждая из которых кодирует наличие или отсутствие одного из свойств модели защиты. Поиск оптимальных решений заключается в поиске цепочек из всего их многообразия, обеспечивающих максимум функции приспособливаемости.

Литература

1. ***Гостехкомиссия РФ.*** Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. М.: Воениздат, 1992.

2. ***Гостехкомиссия РФ.*** Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники. М.: Воениздат, 1992.

3. ***Гостехкомиссия РФ.*** Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. М.: Воениздат, 1992.

4. ***ГОСТ*** Р ИСО/МЭК 15408-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.

5. ***Хвостов В.А. и др.*** Методы и средства повышения защищенности автоматизированных систем: монография. Воронеж: Воронежский институт МВД России, 2013. 108 с.

6. ***Макаров О.Ю., Хвостов В.А., Хвостова Н.В.*** Методика нормирования требований к информационной безопасности автоматизированных систем // Вестник Воронежского государственного технического университета. 2010. Т. 6. № 11. С. 47-51.

7. ***Кисляк А.А., Макаров О.Ю., Рогозин Е.А., Хвостов В.А.*** Об одном способе формализации понятия стойкости функции безопасности ГОСТ ИСО/МЭК 15408 // Вестник Воронежского государственного технического университета. 2009. Т. 5. № 2. С. 94-98.

8. ***Кисляк А.А., Макаров О.Ю., Рогозин Е.А., Хвостов В.А.*** Методика оценки эффективности межсетевых экранов // Вестник Воронежского государственного технического университета. 2009. Т.5. № 5. С. 131-135.

9. ***Макаров О.Ю., Рогозин Е.А., Хвостов В.А. и др.*** Метод оценивания устойчивости программных систем защиты информации от несанкционированного доступа на основе динамической модели конфликта // Вестник Воронеж. гос. техн. ун-та. Сер. Радиоэлектроника и системы связи. 2001. Вып. 4.1. С. 12-19.

10. ***Макаров О.Ю., Рогозин Е.А., Хвостов В.А. и др.*** Обоснование норм безопасности информации автоматизированных систем с использованием методов эволюционного моделирования // Вестник Воронеж. гос. техн. ун-та. Сер. Радиоэлектроника и системы связи. 2002. Вып. 4.2. С. 32-39.