Бочкарева Ю.Г., В.К. Клянчин, Г.Н.Чижухин
Пензенский филиал ФГУП НТЦ "Атлас", Пензенский государственный университет

СИСТЕМНЫЙ ПОДХОД К БЕЗОПАСНОСТИ ТЕХНОЛОГИИ ВЕРИФИЦИРОВАННОГО АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ ПРОГРАММ

Коротко о технологии верифицированного автоматизированного проектирования программ (ВАПП). Программное обеспечение (software) сегодня является необходимым и обязательным дополнением к техническим средствам (hardware), которые давно имеют и совершенствуют уже несколько десятилетий системы автоматизации их проектирования (САПР). Однако системы автоматизации *программирования* (проектирования software) по-прежнему находится в зачаточной стадии, хотя создание таких систем не только ускорил бы процессы программирования, но и позволил обеспечить большую безопасность создаваемого software.

Для верифицированного автоматизированного проектирования программ (ВАПП) предложена технология [1,2], основанная на использовании тензорной алгебраической системы (ТАС) [3] и Венского метода проектирования программ (VDM) [4]. Начало ее реализации представлено в работах, направленных:

- на создание специального глоссария [5], как конгломерата ТАС и VDM;
- на доказательство с использованием ТАС правильности перехода (верификации) с одного уровня представления программы на другой [6];
- на создание тензорной спецификации программы и на методику ее автоматического преобразования в программу на языке высокого уровня [7].

Однако, несмотря на эти, уже решенные при реализации ВАПП принципиальные вопросы, сегодня по-прежнему нет автоматизированного преобразования словесного описания (СО) алгоритма в его более четкий вид - «канонизированное» формализованное СО (ФСО), основанное на понятии «соответствие», а также дальнейшего автоматического преобразования ФСО в инверсную граф-схему алгоритма (ИГСА), необходимую для автоматического синтеза регулярного выражения алгоритма (РВА).

Кроме того, отсутствует системный анализ безопасности технологии ВАПП, который должен, на наш взгляд, состоять из следующих составных частей:

- системного анализа безопасности самой технологии программирования;
- системного анализа безопасности верификации программирования;
- системного анализа безопасности автоматизации программирования;
- комплексного системного анализа безопасности всей технологии ВАПП.

Общая постановка системного анализа информационной безопасности. Сначала рассмотрим системный анализ любой АСОИ (автоматизированная система обработки информации) как объекта информатизации с точки зрения информационной безопасности [8].

Для подобного анализа [9] необходимо представить, что такая АСОИ должна содержать в себе некоторую *подсистему информационной безопасности* (ПИБ), состоящую из *компонентов*, каждый из которых есть множество относительно однородных *элементов*, объединенных некоторыми функциями для обеспечения выполнения общих целей ее функционирования. Причем подсистема здесь не сводится к сумме компонентов, хотя в случае объединения их в подсистему они выступают и, соответственно, воспринимаются как единое целое. Для ПИБ АСОИ, на наш взгляд, имеют место следующие компоненты:

- стратегии (способы) *защиты* информации, стратегии (методы) прогнозирования *нападения* на рассматриваемый объект,

- стратегии (механизмы) принятия решения, основывающиеся на анализе возможных результатов суммарного действия двух предыдущих стратегий и представляющие собой *политику безопасности* (набор норм, правил и практических приемов, регулирующих такое

управление и распределение ценной информации [10],которое обеспечивает ее безопасность).

Элемент. ПИБ - это условно неделимая, самостоятельно функционирующая ее часть, которая, например, для первой компоненты представляет собой одну стратегию защиты. Таких стратегий, как известно [11], может быть несколько. Из элементов ПИБ состоят все ее компоненты и элементы объединяются общей функциональной средой.

Функциональная среда - это характерная для ПИБ совокупность законов, алгоритмов и параметров, согласно которым осуществляется взаимодействие (обмен, взаимоотношение) между ее компонентами и функционирование (стабильность или деградация) ПИБ в целом.

И, наконец, *структура* ПИБ подразумевает совокупность связей, обеспечивающих этот информационный обмен между компонентами, определяющий функционирование ПИБ в целом, и способы взаимодействия ее с внешней средой.

Рассмотрим подробней компоненты и элементы ПИБ, из которых они состоят. Например, организация защиты информации в самом общем виде может быть сформулирована как задача поиска оптимального компромисса между *потребностями в защите* и *необходимыми ресурсами* для этих целей [12]. Потребности обусловлены важностью и объемами защищаемой информации, условиями ее хранения, обработки и использования. Ресурсы могут быть ограничены заданным пределом либо определяются условием обязательного достижения требуемого уровня защиты. В первом случае защита организуется так, чтобы при выделенных ресурсах обеспечивался максимальный уровень защиты, а во втором ~ уровень защиты обеспечивает минимальное расходование ресурсов. Нетрудно видеть, что сформулированные случаи есть не что иное, как прямая и обратная постановки оптимизационных задач. Они достаточно детально изучены с помощью методов современной теории систем, информатики и прикладной математики. Однако "имеющиеся неопределенные ситуации, а также, прежде всего, в данном случае невозможность получения функциональных зависимостей между объемом затрачиваемых для защиты ресурсов и достигаемым уровнем защиты не позволяют строго решить эти задачи известными методами.

Поэтому в целях создания условий для ориентации в этих неопределенных ситуациях и вводятся понятия *стратегий* [11,12]. Под *стратегиями* (защиты, прогнозирования нападения, принятия решения) понимается как системный взгляд на сложившуюся ситуацию защиты от нападения, который распространяется и на системный подход к принятию наиболее рационального решения в этой ситуации. В целом стратегии и представляют собой *системный анализ рассматриваемой ПИБ.* Количество стратегий должно быть небольшим (чтобы просто ориентироваться в самих стратегиях), но в то же время должно полно и достаточно адекватно отображать всю гамму потенциально возможных ситуаций.

В этом смысле хороший урок (по части количества стратегий защит) преподает нам природа, в которой всего четыре стратегии защиты: 1) *оборонительная* или пассивная (надевание «брони»), например, черепаха - на себя или охранная территория -на окружающую среду; 2) *наступательная* или активная защита, выражающаяся в нападении и уничтожении нападающего (в том числе и с помощью вирусов); 3) *пространственно-временная* или защита с помощью изменения месторасположения в пространстве (например, бегство в пространстве от нападающего или перемещение в другую область адресного пространства ЗУ) или во времени (размножение - создание собственных копий); 4) *содержательная* или защита с помощью внесения изменений в объект защиты или окружающей его среды (хамелеон меняет свой цвет, а дымовая завеса на флоте изменяет окружающую среду). Все такие стратегии защиты необходимо применять и в АСОИ.

Защищающемуся техническому объекту недостаточно владеть даже всеми четырьмя стратегиями защиты. Он должен уметь еще и прогнозировать развитие событий. Поэтому вводится понятие *абсолютной системы защиты* **[13],** в которой как раз и работает вторая стратегия - *стратегия прогнозирования*, способная в любой момент спрогнозировать нападение (т.е. наступление угрожающего события), причем за время, достаточное для

приведения в действие любой из адекватных стратегий защиты. *Любая защищающаяся ПИВ* (отдельно взятый человек, государство, банк и т.п.) *должна на основе системного анализа информации о текущих событиях внутри и вне системы определить (идентифицировать) прогнозируемое событие и принять решение **о** стратегии защиты на основе имеющейся политики безопасности* — третьей стратегии - стратегии принятия решений

Системный анализ безопасности самой технологии программирования. Рассматривая технологию программирования, как ПИБ, необходимо представлять ее как такую технологию, которая не только должна производить заданный продукт - программу, но и обеспечивать при этом безопасность дальнейшего существования этого продукта. Тогда компоненты такой ПИБ можно представить в следующем виде:

- стратегия прогнозирования нападения на технологию программирования должна **состоять** из таких элементов ПИБ. которые представляют собой прогноз различного рода воздействия угроз нормальному созданию и функционированию программы, например, прогноз воздействия недокументированных возможностей, различных закладок и вирусов, размещаемых в программе в процессе производства, и прогноз возможных программных нападений на нее из сетей в процессе эксплуатации и т.п.;

- стратегия защиты, определяющаяся различными организационными мерами, обеспечивающими нейтрализацию воздействия угроз *за счет включения* в технологию для написания программы *не только* обычного *алгоритмического* аппарата (языка программирования), в том числе и обеспечивающего кодирование программы, *но также и* одного (или несколько), более строгих математических, а именно, *алгебраических аппаратов,* дающих возможность осуществлять контроль за правильностью функционирования (контроль целостности) алгоритмического аппарата, как при производстве программы, так и при ее дальнейшей эксплуатации;

- стратегия принятия решений - политика безопасности, определяющая в случае принятия отмеченных организационных мер, как правильное применение алгебраического(их) аппарата(ов), так и контроль за его(их) применением.

Системный анализ безопасности верификации программирования. Обеспечение уверенности в том, что созданная программа реализует именно заданный алгоритм, а не какой-то другой, т.е. верификация программирования, была и остается одним из ключевых направлений развития современной методологии программирования.

Это особенно важно при создании *безопасного* ПО, так как оно означает, что в нем реализуются только те функции, которые заявлены в задании на проектировании и не содержится никаких недокументированных возможностей и прочих деструктивных воздействий, не зависимо от того каким образом они в нем появились. Традиционные способы обеспечения такой уверенности путем тестирования программ не могут полностью решить эти задачи и обеспечить требуемый на сегодня уровень безопасности.

Верификацию программирования также можно рассмотреть как компоненту ПИБ, состоящую из трех стратегий:

- стратегия прогнозирования нападения на верификацию программирования должна состоять из таких элементов ПИБ, которые представляют собой прежде всего прогноз воздействия угроз типа правильности проведения верификации, например, ошибок верификации;

- стратегия защиты, определяющаяся различными организационными мерами, обеспечивающими нейтрализацию воздействия угроз *за счет включения* в процесс верификации строгого математического, а именно, *алгебраического аппарата,* основанного на изоморфизме тензорных алгебраических систем, дающего возможность осуществлять контроль за правильностью функционирования процесса верификации при производстве программы;

- стратегия принятия решений - политика безопасности, определяющая правильность применения алгебраического аппарата, основанного изоморфизме **ТАС.**

При этом стратегию защиты надо определять как *такую часть технологии программирования,* которая производит *безопасную* программу, *за счет проведения*

верификации ее в процессе производства. В результате ее действия будет обеспечиваться невозможность появления таких элементов нападения на ПИБ, которые представляют собой различного рода угрозы нормальной верификации программы, прежде всего, ошибки в ее проведении.

Таким образом, верификация в технологии ВАПП основана на привлечении аппарата тензорси (тензоров системотехники), объединенных в тензорную алгебраическую систему (ТАС), позволяющую осуществить алгебраический контроль за **корректностью** программы (соблюдением на каждом шаге проектирования программы условий выполнения изоморфизма тензорных алгебраических систем). Правильность применения этого аппарата (контроль за верификацией) составляет сущность третьей стратегии, применяемой в данной ПИБ, — политики безопасности, обеспечивающей со стороны верификации, как уже стратегии защиты, параметры и нормы этого контроля.

Системный анализа безопасности автоматизации программирования. Автоматизацию проектирования программ также необходимо рассматривать как еще одну компоненту ПИБ и тоже как стратегию защиты. При этом под ней надо определить *такую часть технологии программирования*, которая также производит *безопасную* программу, но уже за счет *обеспечения не участия* человека в процессе ее производства. В результате действия этой стратегии обеспечивается невозможность размещения в программе при ее производстве элементов нападения на ПИБ, представляющих собой различные угрозы нормальному функционированию программы, определяемые, прежде всего, недокументированными возможностями, закладками и т.п.

Автоматизация проектирования программ в технологии ВАПП основана на привлечении алгебраического аппарата тензорси и макропроцессорного подхода, опирающегося на использование уже верифицированных макробиблиотек. Правильность применения этих аппаратов и осуществление контроля за их применением дополняет политику безопасности для той же самой ПИБ со стороны автоматизации программирования, как стратегии защиты.

Комплексный системный анализ безопасности всей технологии ВАПП. Комплексность системного анализа безопасности рассматриваемой технологии заключается в объединении всех компонент ПИБ для различных ее частей в единую компоненту.

Так комплексная стратегия защиты всей ВАПП как компоненты ПИБ есть:

- *включение в нее для написания программы не только алгоритмического, **но** также и алгебраических аппаратов;*
- *включение в нее такой части технологии программирования*, которая производит *безопасную* программу *за счет проведения верификации в процессе производства;*
- *включение в нее такой части технологии программирования,* которая производит *безопасную* программу, *за счет не участия* человека в процессе ее производства *(за счет автоматизации производства программ).*

Комплексная стратегия прогнозирования нападения на ВАПП есть: - обеспечение прогнозов для различного рода воздействий угроз нормальному созданию и функционированию программы, как размещаемых в программе в процессе производства, так и прогноз возможных программных нападений на созданную программу из сетей в процессе эксплуатации и т.п.;

- обеспечение прогнозов нападения на верификацию программирования, прежде всего типа неправильности проведения верификации, т.е. ошибок в ее верификации;
- обеспечение прогнозов нападения на автоматизацию программирования, прежде всего, типа ошибок в работе автоматических подсистем.

Комплексная стратегия принятия решения - *политика безопасности*, определяющая в случае принятия организационных мер, как правильность применения алгебраического(их) аппарата(ов), так и контроль за его(их) применением, как в процессе производства программы, так и в процессе ее эксплуатации.

Список литературы

1. Чижухин Г.Н. Технология верифицированного автоматизированного проектирования

программных средств защиты информации.//Известия ТРТУ. Тематический выпуск. Материалы V МНПК «Информационная безопасность». Таганрог: Изд-во ТРТУ, 2003. №4(33),С.78-81

2. Чижухин Г.Н. Технология верифицированного автоматизированного проектирования для создания безопасного soft.// Интеграл, 2004, №1(15),- с.36-38

3. Чижухин Г.Н. Тензорная алгебраическая система.//Труды V МНТК«Новые информационные технологии и системы", Пенза, Изд-во ИГУ, - С. 195-202.

4. Петренко А.К. Венский метод разработки программ // Программирование - №6 - 1991, С, 3-23

5. Фатеев А.Г., Чижухин Г.Н. Глоссарий основных обозначений языка СПЕЦТАС. Части 1,2 // Труды НТК "Безопасность информационных технологий", ПНИЭИ, Пенза, 2002.С.43-48

6. Фатеев А.Г., Чижухин Г.Н. Методика пошаговой детализации спецификации программы с одновременной ее верификацией // Труды НТК "Безопасность информационных технологий". ПНИЭИ, Пенза, 2002.С.40-43 "

7. Фатеев А.Г., Чижухин Г.Н. Математические модели средств спецификаций программ на основе тензорного языка системотехники // Труды НТК'Ъезопасность информационных технологий", ПНИЭИ, Пенза, 2002.С.49-52.

8. Бочкарева Ю.Г., Смогунов В.В., Фунтиков В.А., Чижухин Г.Н. Подход к системному анализу информационной безопасности.//Успехи современного естествознания -№10, 2004 г., С.66-67

9. Хомяков Д.М, Хомяков П.М.. Основы системного анализа. - М.: Изд-во механико-математического факультета МГУ им. М.В.Ломоносова, 1996, 108 с.

10. Грушо А.А., Тимонина Е.Е.. Теоретические основы защиты информации. - М.: Изд-во агентства «Яхтсмен», 1996, 192 с.

11. Чижухин Г.Н.. Основы защиты информации в вычислительных системах и сетях ЭВМ: Учеб. пособие.-.Пенза: Изд-во Пенз. гос. ун-та , 2001, 164 с.

12. ГерасименкоВ.А., Малюк А.А. Основы защиты информации: Учебник для вузов - М.: Изд-во ООО «Инкомбук», 1977, 537с.

13. Расторгуев СП.. Абсолютная система защиты.// Системы безопасности связи и телекоммуникаций-№3, 1996, С.86-89.