В. С. Симанков, Е. С. Тарасов
Россия, г. Краснодар, КубГТУ

МЕТОДИЧЕСКИЙ ПОДХОД К АНАЛИЗУ И ВЫРАБОТКЕ ПРИЕМОВ ПРОТИВОДЕЙСТВИЯ ИСПОЛЬЗОВАНИЮ НЕТРАДИЦИОННЫХ ИНФОРМАЦИОННЫХ КАНАЛОВ

Применение несертифицированного аппаратного и программного обеспечения в автоматизированных системах влечет за собой необходимость учета факторов, связанных с наличием в этом оборудовании недокументированных возможностей, влияющих на безопасность обрабатываемой информации.

Если рассматривать производителя средств, используемых для обработки конфиденциальной информации, как противника, то его возможности по несанкционированным действиям в вычислительной системе неограниченны.

Традиционные средства защиты бессильны против закладок, выполненных на уровне архитектуры. Когда речь идет о защите коммерческой информации, угроза совместных действий производителей выглядит малоправдоподобной, но в случае сведений, составляющих государственную тайну, приходится предполагать, что противник (например, спецслужбы стран-производителей оборудования) может (и будет) использовать все возможности, заложенные в архитектуру вычислительных систем.

Для нейтрализации данных угроз безопасности конфиденциальной информации проводится комплекс мероприятий по государственной сертификации импортного ПО и специальные проверки аппаратного обеспечения.

Развитие техники и технологий привело к возможности осуществления несанкционированного доступа к конфиденциальной информации, обрабатываемой в АС, по *нетрадиционным информационным каналам* (НИК), невидимым (скрытым) для современных средств защиты, с использованием, в частности, аппаратно-программных закладок (АПЗ), внедренных в систему.

Нетрадиционный информационный канал - это несанкционированный способ скрытой передачи нелегитимной информации по действующим («традиционным») каналам связи, нарушающий системную политику безопасности [10].

В связи с этим возникла проблема анализа нетрадиционных (скрытых) каналов всюду, где возникают ограничения на информационные потоки.

Любой такой анализ предполагает решение четырех взаимосвязанных задач:

- выявление скрытых каналов;
- оценка пропускной способности и опасности, которую несет их - функционирование;
- выделение сигнала или получение какой-либо информации, передаваемой по скрытым каналам;
- противодействие реализации скрытого канала вплоть до его уничтожения.

Если противник знает схему контроля в системе защиты, то при выполнении определенных условий возможно построение невидимого для нее скрытого канала управления программно-аппаратным агентом в компьютерной среде [1].

Аналогично – при условии знания противником системы защиты доказывается возможность построения скрытого канала при общении программно-аппаратных агентов в открытой среде между собой [2]; т. е. при помощи аппаратно-программных закладок, реализованных в оборудовании при поддержке производителя, возможно обеспечить двунаправленную передачу данных между злоумышленниками.

Доказательство невозможности обнаружения и устранения потайных каналов

имеется также в работах А. А. Грушо и Е. Е. Тимониной [4].

Рис. 1. Методы и средства анализа безопасности ИС

Со скрытыми каналами можно бороться двумя способами: пытаться блокировать их полностью или уменьшать пропускную способность. Представляется очевидным, что если не формализовать структуру данных, передаваемых программами по легальным каналам, последние всегда можно использовать для скрытой пе-

редачи информации [9]. Модели скрытых каналов используются для разработки методов их выявления или для обоснования невозможности такового.

Создание комплексных СЗИ в данных условиях (высокой степени неопределенности функционирования) должно сопровождаться использованием согласованного семейства моделей, адаптивно конструирующихся одна из другой и, таким образом, непрерывно совершенствующихся на основе оптимального выбора исходных данных; при непосредственном синтезе системы защиты исходными должны явиться положения о выборе математически продуктивного критерия оптимальности в соответствии с архитектурой системы защиты и технологией обработки информации на объекте и четкой математической формулировки задачи, учитывающей все имеющиеся сведения и позволяющей решить ее в соответствии с принятым критерием [3].

Использование комплекса моделей также необходимо для решения задач:

- описания структуры и поведения системы, прогнозирования значений ее параметров;
- формирования подмножеств контролируемых параметров и диапазонов значений зон их контроля на основе заданных требований к устойчивости функционирования системы;
- контроля и диагностирования нарушений работоспособности системы;
- самоорганизации и саморазвития семейств моделей для описания структуры, поведения, прогнозирования, контроля и диагностирования с учетом обеспечения необходимой устойчивости системы в условиях влияния факторов среды.

Результатом исследований должны быть созданные на основе известных и специально разработанных методов и средств модели для описания структуры и поведения СЗИ, а также контроля, диагностирования и прогнозирования ее состояний (системы выявления АПЗ сетевого уровня, выявление на системном уровне, функционирующие на основе заданной совокупности критериев, полученных в результате вероятностного, логического, синтаксического или семантического анализа).

Методы и средства, используемые для анализа и оценки безопасности ИС, можно разделить на две категории: контрольно-испытательные и логико-аналитические (рис.1) – по различиям в точке зрения на предмет исследования [7, 8].

Контрольно-испытательные методы анализа рассматривают его через призму фиксации факта нарушения безопасного состояния системы, а логико - аналитические – посредством доказательства наличия отношения эквивалентности между моделью исследуемой программы и моделью объекта (АПЗ). В такой классификации тип используемых для анализа средств не принимается во внимание - в этом ее преимущество по сравнению, например, с разделением на статический и динамический анализ.

Комплексная система исследования безопасности должна включать как контрольно-испытательные, так и логико-аналитические методы анализа, используя преимущества каждого их них.

С методической точки зрения логико - аналитические методы выглядят более предпочтительными, так как позволяют оценить надежность полученных результатов и проследить последовательность (путем обратных рассуждений) их получения.

Однако эти методы еще мало развиты и, несомненно, более трудоемки, чем контрольно-испытательные, те, в которых критерием безопасности программы служит факт регистрации в ходе тестирования программы нарушения требований по безопасности, предъявляемых к системе (рис. 2).

Контрольно-испытательные методы делятся на контролирующие процесс функционирования ИС и те, в которых отслеживаются возможные изменения, вызванные деятельностью АПЗ. Эти методы не требуют формального анализа, позволяют использовать имеющиеся технические и программные средства и быстро ведут к созданию готовых методик.

Рис. 2. Схема анализа безопасности
с помощью контрольно-испытательных методов

Они начинаются с определения набора контролируемых параметров системы; этот набор будет зависеть от используемого аппаратного и программного обеспечения (от операционной системы) и исследуемого объекта. Затем составляется программа испытаний и проверки требований безопасности, предъявляемых к данной системе в предполагаемой среде эксплуатации на запротоколированных действиях и изменениях в операционной среде, использующая стохастические методы и экстраполяцию результатов. Очевидно, что наибольшую трудность здесь представляет определение набора критичных с точки зрения безопасности параметров, которые сильно зависят от специфики исследуемой системы и определяются путем экспертных оценок; кроме того, в условиях ограниченных объемов испытаний, заключение о выполнении или невыполнении требований безопасно-

сти, как правило, будет носить вероятностный характер.

При проведении анализа безопасности с помощью логико-аналитических методов (рис. 3) строится модель исследуемой системы и формально доказывается эквивалентность ее модели объекта (АПЗ). Методы используют формальные модели, основанные на совокупности признаков, свойственных той или иной группе известных объектов.

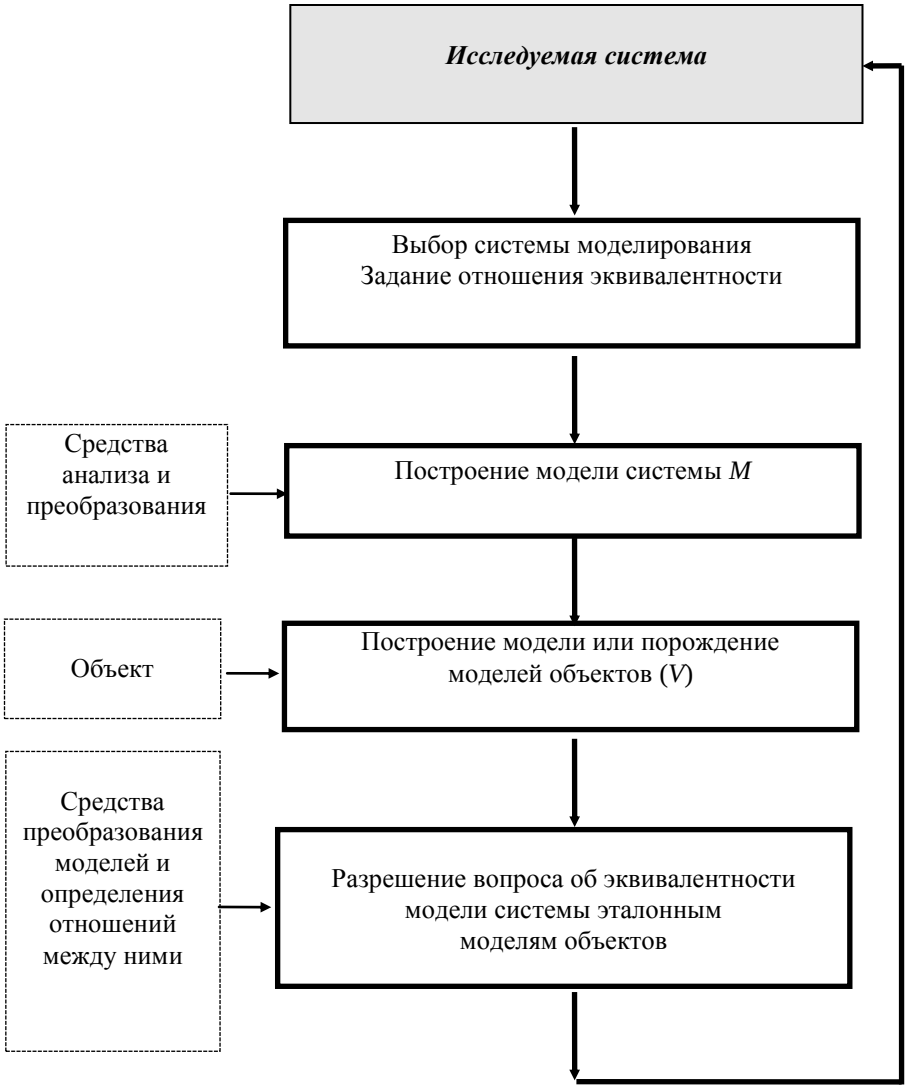

Рис. 3. Схема анализа безопасности с помощью логико-аналитических методов

Для проведения логико-аналитического анализа безопасности необходимо, во-первых, выбрать способ представления и получения моделей системы и объектов. После этого необходимо построить модель исследуемой системы и попытаться доказать принадлежность ее части к отношению эквивалентности, задающему

множество объектов.

Необходимо, чтобы модели объекта и системы были заданы одним и тем же способом. Проблемой здесь является создание формальных моделей систем и объектов, или хотя бы определенных их классов. Механизм задания отношения между системой и объектами определяется способом представления модели. Наиболее перспективным здесь видится использование семантических графов и объектно-ориентированных моделей [5].

Для моделирования поведения системы могут быть применены методы интеллектуального анализа. При достаточном количестве данных о поведении объекта возможно автоматическое порождение гипотез о взаимосвязи (в том числе и неявной) между различными параметрами и компонентами, корреляционных зависимостях и оценка вероятности каждой гипотезы; некоторые системы, используя аппарат нечеткой логики, могут оценивать данные не только с количественной, но и с качественной стороны.

В целом полный процесс анализа состоит из лексического верификационного, синтаксического верификационного и семантического анализа. Каждый из них представляет собой законченное исследование, выводы которого могут иметь как самостоятельное значение, так и коррелироваться с результатами полного процесса анализа [6].

Лексический верификационный анализ предполагает поиск, распознавание и классификацию различных лексем объекта исследования. Синтаксический верификационный анализ предполагает поиск, распознавание и классификацию синтаксических структур объектов, а также построение структурно - алгоритмической модели самой системы.

Семантический анализ предполагает исследование системы, изучение смысла составляющих ее компонентов в аспекте единой операционной среды. В отличие от предыдущих видов, основанных на статическом исследовании, семантический анализ нацелен на изучение динамики системы, ее взаимодействия с окружающей средой. На основании полученных результатов можно сделать заключение о степени безопасности ИС.

Неэффективность традиционных математических методов (статистики и теории вероятностей, классических методов оптимизации) и сложность процесса принятия решений приводят к тому, что при оценке и выборе альтернатив необходимо использовать и обрабатывать качественную экспертную информацию. Перспективным направлением разработки методов принятия решений в данной ситуации является лингвистический подход на базе теории нечетких множеств.

Решение задач анализа и синтеза СЗИ усложняется рядом их особенностей, основными из которых являются: сложная опосредствованная взаимосвязь показателей качества СЗИ с показателями качества информационной системы; необходимость учета большого числа показателей (требований) СЗИ при оценке и выборе их рационального варианта; преимущественно качественный характер показателей, учитываемых при анализе и синтезе СЗИ; существенная взаимосвязь и взаимозависимость этих показателей, имеющих противоречивый характер; трудность получения исходных данных, необходимых для решения задач анализа и синтеза СЗИ, в особенности на ранних этапах их проектирования.

Изучение проблематики скрытых каналов показывает, как важно правильно поставить задачу, рассматривая ее не изолированно, а в реальном окружении с неуклонным повышением системности подхода – в том смысле, что проблема защиты заключается не только в создании соответствующих механизмов, а представляет собой регулярный процесс, осуществляемый на всех этапах жизненного цикла системы при комплексном использовании всех имеющихся возможностей.

Проведенный анализ и представленные методики позволяют подойти к решению исследуемой проблемы с системной точки зрения, демонстрируя, как при этом все средства, методы и мероприятия, используемые для защиты, рационально объединяются в единый целостный механизм.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Грушо А. А.* Скрытые каналы и безопасность информации в компьютерных системах // Дискретная математика, Т. 10. Вп. 1. 1998.

2. *Грушо А. А.* О существовании скрытых каналов // Дискретная математика. Т.11. Вып. 1. 1999.

3. *Грушо А. А., Тимонина Е. Е.* Теоретические основы защиты информации. М.: Изд-во. -«Яхтсмен», 1996.

4. *Тимонина Е.Е.* Механизмы контроля скрытых каналов // Информационные технологии в науке, образовании, телекоммуникации, бизнесе: Труды международной конференции. Украина, Крым, 2002.

5. *Казарин О. В.* Безопасность программного обеспечения компьютерных систем. М., 2003.

6. *Домарев В. В.* Безопасность информационных технологий. Системный подход. Киев: ДиаСофт. 2001.

7. *Зегжда Д. П.,Шмаков Э. М.* Проблема анализа безопасности программного обеспечения// Безопасность информационных технологий. 1995. №2.

8. *Зегжда Д. П.* Проблемы безопасности программного обеспечения. - СПб.: Изд-во. СПбГТУ, 1995.

9. *Lampson B. W.* A Note of the Confinement Problem. – Communications of ACM, 1973.

10.*Tsai C. R., Gligor V. D., Chandersekaran C. S*. A Formal Method for the Identification of Covert Storage Channels in Source Code. - IEEE Transactions on Software Engineering, 1990.

А. П. Жук, Р. Ю. Савелов
Россия, г. Ставрополь, Ставропольский государственный университет

АРХИТЕКТУРА МЕЖСЕТЕВОГО ЭКРАНА ДЛЯ КОРПОРАТИВНЫХ СЕТЕЙ

В настоящее время ввиду бурного развития бизнеса наиболее большое распространение получили корпоративные сети, которые также называют сетями масштаба предприятия. Пользователями корпоративной сети являются только сотрудники предприятия [1].

Корпоративные сети имеют ряд концептуальных преимуществ, таких как высокая отказоустойчивость, способность выполнения параллельных вычислений, возможность гибкого распределения работ по всей системе, оперативный доступ к обширной корпоративной информации, взаимодействие с потенциальными клиентами посредством общедоступных сетей и Internet и другие.

Но вместе с этим в корпоративных сетях появляются и риски, связанные с опасностями взаимодействия с открытой и неконтролируемой внешней средой. Такая среда представляет собой большую угрозу безопасности корпоративным сетям, так как возрастает количество удалённых пользователей, которые могут получить несанкционированный доступ к ресурсам сети предприятия.

Для устранения проблем, связанных с безопасностью, известно много различных решений, самым распространенным из которых является применение межсетевых экранов. Их использование - это первый шаг, который должно сделать любое предприятие, подключающее свою корпоративную сеть к Internet [2].