УДК 65.012.8: 004.492

Г.Г. Гроздов
Служба безопасности Украины

Постановка задачи формирования эффективной комплексной системы защиты информации, основанной на использовании результатов теста на проникновение

Предложена общая модель построения распределенной атаки на АС. Для описания распределенной атаки использованы методы теории графов.
Ключевые слова: тест на проникновение, эффективная система защиты информации.

Введение

В настоящее время актуальна задача построения и оценки эффективности механизмов защиты информации в различных комплексных системах защиты информации (КСЗИ) автоматизированных систем (АС).

Можно выделить такие классы информации, защита которых должна обеспечиваться механизмами защиты информации (ЗИ), входящими в состав КСЗИ: информация, составляющая коммерческую и военную тайну. В АС указанных классов могут иметь приоритетное значение различные требования к механизмам ЗИ [2, 4].

В научно–технической литературе рассматриваются два аспекта эффективности системы ЗИ. С одной стороны, система защиты информации должна эффективно противодействовать угрозам [1, 2]. С другой стороны, она должна быть адекватной – расходы на безопасность не должны превышать стоимости самой информации и размера возможных потерь, вызванных успешной реализацией угроз [3].

В настоящее время наиболее агрессивным способом проверки эффективности КСЗИ автоматизированной системы (АС) от несанкционированного доступа является тест на проникновение (англ.–penetration test) [3].

Недостатки существующих тестов на проникновение, постановка задач исследования

Современные разработки в области защиты информации рассматривают основную задачу любой КСЗИ как противодействие распределенным атакам. Атакой на компьютерную систему называется действие или последовательность связанных между собой действий нарушителя, которые приводят к реализации угрозы путем использования уязвимостей этой компьютерной системы. Причем каждое из действий в отдельности опасным не является. Очевидно, что для повышения эффективности КСЗИ необходимо иметь формальное описание возможных действий нарушителей, а также способов их реализации.

Для успешной реализации атаки злоумышленник должен выполнить разведку объекта нападения с целью поиска уязвимостей, которые могут быть использованы в будущем. Само по себе наличие уязвимостей в автоматизированной системе не приводит к потерям, однако это может привести к успешным действиям злоумышленников. При разработке КСЗИ необходимо знать о наличии таких уязвимостей в компонентах АС. Необходимо разработать алгоритм поиска таких уязвимостей в компонентах АС.

Цели исследования можно сформулировать таким образом.

1. Разработать общую модель процесса построения распределенной атаки на АС, которая позволит учесть финансовые возможности противника и в конечном итоге получить способы реализации им распределенной атаки на защищаемую АС.
2. Разработать общую модель процесса формирования эффективной КСЗИ АС, способную противостоять распределенным атакам.
3. Исследовать возможные методы построения частных моделей, которые могут быть в последствие использованы.

Общая модель построения теста на проникновение АС

Как отмечалось выше, основная задача эффективной КСЗИ АС - это адекватное противодействие распределенным атакам. Распределенная атака состоит из четырех этапов, рассмотрим их подробнее.

На этапе *сбора информации* атакующая сторона выбирает цель нападения и собирает необходимую информацию о ней (в качестве такой информации выступают сведения о возможностях, которыми располагает защищающаяся сторона, данные об используемых средствах и методах защиты, и т.д.).

Затем происходит поиск *объекта атаки*, то есть наиболее уязвимого звена атакуемой системы, воздействие на которое приведет к достижению желаемого результата с

наименьшими затратами. Этап *реализации атаки* подразумевает выполнение атакующей стороной ряда действий, направленных на нанесение ущерба Системе. Этапом *завершения атаки* является "заметание следов" атакующей стороной. Основной целью этого этапа является снижение вероятности обнаружения атаки защищающейся стороной.

Сформулируем задачи, которые должны быть решены для построения теста на проникновение АС:

1. Разработать модель функционирования АС и модель использования ее ресурсов. Результатом должна быть технологическая схема функционирования АС ($\{TS\}$) и множество параметров использования ресурсов АС ($\{MR\}$).

2. На основании результатов предыдущего этапа построить модель уязвимостей АС. Указанный этап необходим для адекватной оценки уязвимостей АС, что позволит в последствии разработать модель распределенных атак на АС. Результатом этапа станет множество уязвимостей компонентов АС ($\{LT\}$). (К компонентам АС относятся информация, аппаратное и программное обеспечение, обслуживающий персонал и физическая среда).

3. Исходя из множества уязвимостей компонентов АС ($\{LT\}$), а также результатов первого этапа, сформировать модель распределенной атаки на АС. Результатом моделирования станет полный перечень возможных атак на АС ($\{LA\}$).

4. На основании технологической схемы АС ($\{TS\}$) построить модель противника, оценить его возможности. Результатом построения указанной модели должны стать сведения о категориях противника ($\{P\}$), его возможностях по реализации атак ($\{A\}$).

5. Разработать модель оценки потерь. В качестве исходных данных модели должны быть заданы перечень угроз информации ($\{U\}$), модель использования ресурсов Системы ($\{MR\}$), а также технологическая схема функционирования АС ($\{TS\}$). Указанная модель должна учитывать как возможные потери, вызванные успешными атаками, так и потери от применения средств защиты информации.

6. Разработать модель угроз информации АС. В качестве исходных данных для построения этой модели необходимы: множество уязвимостей компонентов АС ($\{LT\}$), полный перечень возможных атак на АС ($\{LA\}$), сведения о категориях противника ($\{P\}$), его возможностях по реализации атак ($\{A\}$). Результатом этого этапа моделирования должен стать список угроз информации ($\{U\}$).

7. Исходя из возможностей противника, на основании модели угроз и модели оценки потерь необходимо построить модель формирования распределенной атаки. Исходными данными рассматриваемой модели будут: множество угроз информации АС ($\{U\}$), вектор значений возможных потерь в случае успешной реализации угроз ($\{L\}$), полный перечень возможных атак на АС ($\{LA\}$), множества уязвимостей компонентов АС ($\{LT\}$), сведения о категориях противника ($\{P\}$), его возможностях по реализации атак ($\{A\}$), а также время, которым располагает атакующая сторона (T). Результатом этой модели должен стать вектор использования средств защиты информации (ω) в Системе.

Если для оценки эффективности КСЗИ АС используется модель теста на проникновения "белая коробка", будем полагать, что переменные $\{AS\}$, $\{MR\}$и $\{A\}$ заданы изначально.

При использовании модели тестирования "черная коробка" будем полагать, что изначально известны $\{AS\},\{A\}$.

Таким образом, общая модель формирования с учетом распределенных атак на АС примет такой вид (рис.1).

Модифицированный способ решения задачи формирования эффективной КСЗИ АС (защита от распределенной атаки)

В предлагаемой методике построения модели распределенной атаки на АС воспользуемся математическим аппаратом теории графов. Будем называть графом атаки такой граф, в котором приведены все возможные последовательности действий нарушителя для достижения своих целей. Каждую из указанных последовательностей назовем трассой атаки.

Исходя из вышеизложенного, модифицированный способ формирования эффективной КСЗИ АС будет выглядеть следующим образом:

1. Составить вектор *IR* для элементов формального описания информационных ресурсов, используемых АС на различных этапах обработки информации ($\{MR\}$).

2. Для каждого элемента вектора *IR* составить множество путей доступа к элементу *IR(i)*. Для этого использовать алгоритм поиска всех путей в графе. Результаты занести в таблицу вида $< IR(i) >< \{T\} >< \{NL\} >$, где:

IR(i) - элемент формального описания информационных ресурсов, используемых АС на различных этапах обработки информации;

{T} - множество возможных трасс доступа к нему. Под трассой доступа будем понимать необходимую последовательность действий, которую необходимо выполнить – успешное прохождение процедур аутентификации и авторизации на уровне различного ПО компонентов АС и т.п.;

{NL} - множество необходимых условий. Под условиями будем понимать необходимые настройки в ПО компонентов АС: ОС, СУБД, прикладного и специализированного ПО. К ним

относятся – учетные данные пользователей, полномочия по доступу к ресурсам, настройки подсистем безопасности – ОС, СУБД, прикладного и специализированного ПО.

3. Для каждой из полученных трасс рассмотреть варианты несанкционированного чтения, создания, создания необходимых условий для доступа к информации *IR(i)*.

4. Совокупность полученных вариантов даст множество трасс атак для *IR(i)*.

5. Повторить пункты 2-4 для всех элементов вектора *IR*.

6. Сформировать граф распределенной атаки на ресурсы АС. Для этого получить множество условий для реализации атак *{NL}* и множество действий нарушителя политики безопасности *{AP}*. На рис.2 приведены правила формирования указанного графа.

7. Используя методы теории графов, найти остов графа, полученного в пункте 6. В теории графов разрезом называется множество ребер, удаление которых делит граф на два или более изолированных подграфа [14]. Используя методы теории графов, получить множество разрезов графа *{RZ}*.

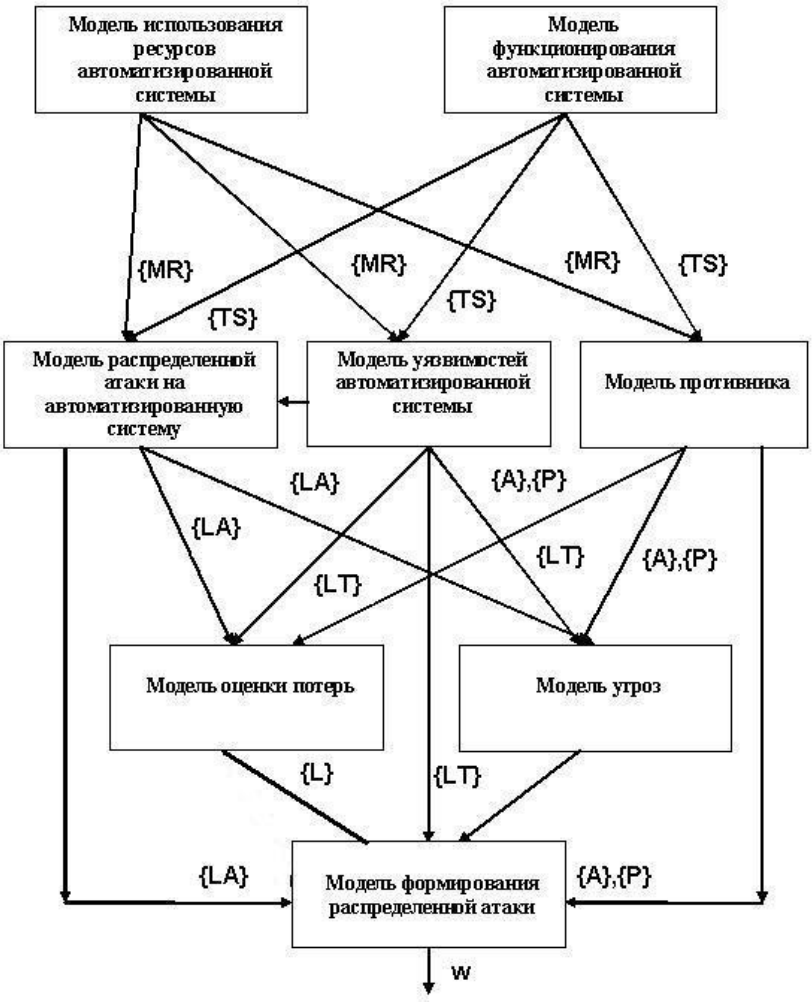

Рисунок 1 - Общая модель процесса формирования распределенной атаки на АС

8. Все найденные в пункте 7 разрезы графа распределенной атаки на АС занести в таблицу вида $< RZ(i) >< \{NL\} >< \{ \gamma_i \} >$, где:

{RZ(i)} - множество разрезов графа распределенной атаки;

{NL} - множество необходимых условий - вершин графа распределенной атаки на АС;

γ_i - множество механизмов защиты информации в составе КСЗИ АС, для обеспечения разреза RZ(i) графа распределенной атаки. Представляет собой бинарный вектор длиною М. Элемент указанного бинарного вектора γ_{ij} равен 1, если

механизм G_{ij} задействован в составе КСЗИ АС, в противном случае γ_{ij} равен нулю.

Для каждого из полученного в пункте 7 разрезов графа бинарных векторов γ необходимо вычислить размер остаточного риска (1), а также размер средств, выделяемых на обеспечение ЗИ в АС (2).

Предлагаемый способ позволяет найти решение, оптимальное или рациональное в среднем. При формировании КСЗИ АС, обрабатывающих информацию, которая составляет государственную, военную или коммерческую тайну могут быть использованы различные критерии:

– для обеспечения эффективной защиты может быть выбран вариант с наименьшим остаточным риском;

– для минимизации расходов на формирование КСЗИ АС может быть выбран вариант с наименьшим значением C_d, у которого значение остаточного риска является наименьшим из рассматриваемых.

Описанный выше способ детально изложен в [2].

Методика формирования эффективной комплексной системы защиты информации автоматизированной системы на основе методов теории игр

В качестве математического аппарата для построения новой модели будет использована математическая теория игр. Из теории игр известен способ, как обеспечить гарантированную границу своего проигрыша, хуже которого быть не должно [5].

В теории игр стратегия игрока в игре - это полный план действий при всевозможных ситуациях, способных возникнуть [6]. Стратегия определяет действие игрока в любой момент игры и для каждого возможного течения игры, способного привести к каждой ситуации.

При формировании КСЗИ АС, обрабатывающих информацию, которая составляет государственную, военную или коммерческую тайну могут быть использованы различные критерии.

Процесс формирования эффективной КСЗИ АС будет рассматриваться как бесконечная игра с противоположными интересами. Цели игроков, а также методы их достижения, приведены в таблице 2.

В таблице 2 использованы следующие обозначения, где 1 - свойства информации, нарушаемые распределенной атакой (Д – доступности, К – конфиденциальности, Ц – целостности).

Таблица 2

Использование методов теории графов для описания стратегий игроков при реализации распределенной атаки и защите АС

1	Защита от распределенной атаки	Построение теста на проникновение
К	Цели игрока: Не дать проложить трассу к ОЗ	Цели игрока: Проложить хотя бы одну трассу к ОЗ
	Метод решения: Построение пути минимальной стоимости	Метод решения: Построение пути минимальной стоимости
Д	Цели игрока: Не дать разорвать все трассы доступа к ОЗ	Цели игрока: Разорвать все трасс доступа к ОЗ
	Метод решения: Неполный разрез	Метод решения: Полный разрез графа
Ц	Цели игрока: Не дать атакующей стороне проложить хотя бы одну трассу доступа с правами на модификацию	Цели игрока: Проложить хотя бы одну трассу доступа с правами на модификацию
	Метод решения: Построение пути минимальной стоимости	Метод решения: Построение пути минимальной стоимости

Ходами в игре будут действия игроков по достижению цели.

Выводы из исследования и перспективы дальнейших разработок

Предлагаемая методика позволяет получить множество способов для реализации теста на проникновения АС. Однако существуют методические проблемы, которые необходимо разрешить в будущем:

1. Любая уязвимость компонента АС действительна определенный период времени. Указанную особенность необходимо учитывать при формировании множества $\{LT\}$.
2. Модель оценки потерь АС должна включать потери, связанные с использованием

механизмов защиты информации в составе АС. Это обстоятельство позволит повысить точность решения задачи построения тестов на проникновение.

3. Для построения адекватной КСЗИ АС необходимо реально оценить возможности вероятного противника.

Список использованной литературы

1. Гроздов Г.Г. Методика построения теста на проникновение в автоматизированную систему, основанная на математической теории игр / Г.Г. Гроздов // Наукові записки українського науково-дослідного інституту зв`язку. – 2010. – № 3.
2. Гроздов Г.Г. Модифицированный способ решения задачи формирования эффективной комплексной системы защиты информации автоматизированной системы: моногр. / Г.Г. Гроздов.– К.: ГУИКТ, 2009 – 32с.
3. Комаров А.А. Тесты на проникновение: методики и современные подходы / А.А. Комаров // Журнал "IT-спец". – 2009. – № 2. – С. 48-53.
4. Лукацкий А.В. Обнаружение атак / А.В. Лукацкий. – С.Пб.: BHV, 2001. – 611 с.
5. Майника Э. Алгоритмы оптимизации на сетях и графах / Э. Майника. – М. : Мир, 1981. – 328 с.
6. Мак-Кинси Д. Введение в теорию игр Д. Мак-Кинси. – К.: Издательство КВИРТУ, 1959. – 347 с.

Надійшла до редакції 20.02.2016

Г.Г. ГРЕЗДОВ
Служба безпеки України

ПОСТАНОВКА ЗАВДАННЯ ФОРМУВАННЯ ЕФЕКТИВНОЇ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ, ЯКА БАЗУЄТЬСЯ НА ВИКОРИСТАННІ РЕЗУЛЬТАТІВ ТЕСТУ НА ПРОНИКНЕННЯ

Запропонована загальна модель побудови розподіленої атаки на АС. Для опису розподіленої атаки на АС використовуються методи теорії графів.

Ключові слова: тест на проникнення, ефективна система захисту інформації.

G.G. GHREZDOV
Security Service of Ukraine

FORMULATION OF THE PROBLEM OF CONSTRUCTION OF AN EFFECTIVE COMPLEX SYSTEM FOR DATA PROTECTIONS IN AUTOMATED SYSTEMS BASED ON THE RESULTS OF PENETRATION TEST

A general model of a distributed attack on computer-aided systems is proposed. To describe a distributed attack the methods of the graph theory were used.

Keywords: penetration tests, effective system for data protection.