УДК 65.012.8: 004.492

Г.Г. Грездов
Служба безопасности Украины

Методика построения защиты от распределенной атаки, основанная на теории графов

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.

В настоящее время наиболее агрессивным способом проверки эффективности комплексных систем защиты информации (КСЗИ) автоматизированной системы (АС) от несанкционированного доступа является тест на проникновение (англ.–penetration test) [1]. Во время таких мероприятий в ход идут все возможные способы преодоления механизмов защиты, которые могут применить нарушители политики безопасности [13]. Результаты тестов на проникновение анализируются, что позволяет повысить эффективность системы защиты информации, а также устранить найденные уязвимости. В странах Евросоюза и США проведение тестов на проникновение – одна из важнейших процедур повышения информационной безопасности предприятия в целом.

В некоторых странах модель теста на проникновение регламентирована органом, отвечающим за лицензирование и аттестацию в области защиты информации. Так, в ФРГ модель проверки объекта автоматизации [16] входит во многие технологические стандарты по безопасности.

Традиционными тестами на проникновение являются так называемая "черная коробка" и "белая коробка". Разница между ними состоит в том, что в первом случае аудиторы ставят в известность весь штат компании о проводимых мероприятиях, а во втором – нет. Такая разница в тестах накладывает отпечаток на последующие действия аудиторов. Отметим, что названные выше приемы трудно назвать методиками. Это подходы, которые выбираются самим заказчиком, а методы их реализации вырабатывает сам аудитор. Это дает возможность расширять конкуренцию в сфере аудита защиты информации, а также позволяет аудиторам создавать уникальные методики.

"Белая коробка" – это способ выявления брешей изнутри. Моделью нарушителя при этом будет внутренний пользователь, имеющий подключение к ресурсам АС, но не обладающий при этом дополнительными привилегиями.

Недостатки существующих тестов на проникновение, постановка задач исследования

Несмотря на свои достоинства, современные тесты на проникновение имеют ряд недостатков. К ним следует отнести такие обстоятельства.

1. Первое открытое средство анализа защищенности информационных систем SATAN появилось в 1995 году. В настоящее время применение подобных средств в ходе теста на проникновение является дурным тоном. Например, стандарт безопасности, используемый в платежно-карточной сфере (PCI OSS) говорит о недостаточности и ошибочности такого подхода вследствие уникальности каждой конкретной системы. Кроме того, многие сканеры безопасности могут оказаться беспомощными к глубокому анализу, так как администраторы могли настроить системы обнаружения атак на противодействие такому сканированию [17, 18].

2. Большинство стандартов для тестов на проникновение имеют узкую направленность: одни тесты предназначены для анализа отдельного вида программных систем (например, веб-серверов), другие предназначены для выявления предпосылок ограниченного числа атак. Отсутствуют универсальные методики, позволяющие учесть недостатки любой уникальной системы [17, 18].

Цели исследования можно сформулировать таким образом.

1. 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.

2. 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.

3. 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.

Общая модель построения модели распределенной атаки на АС

Как отмечалось выше, основная задача современной КСЗИ АС - это противодействие распределенным атакам. Как отмечается в [14], 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 модели распределенной атаки на 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.

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

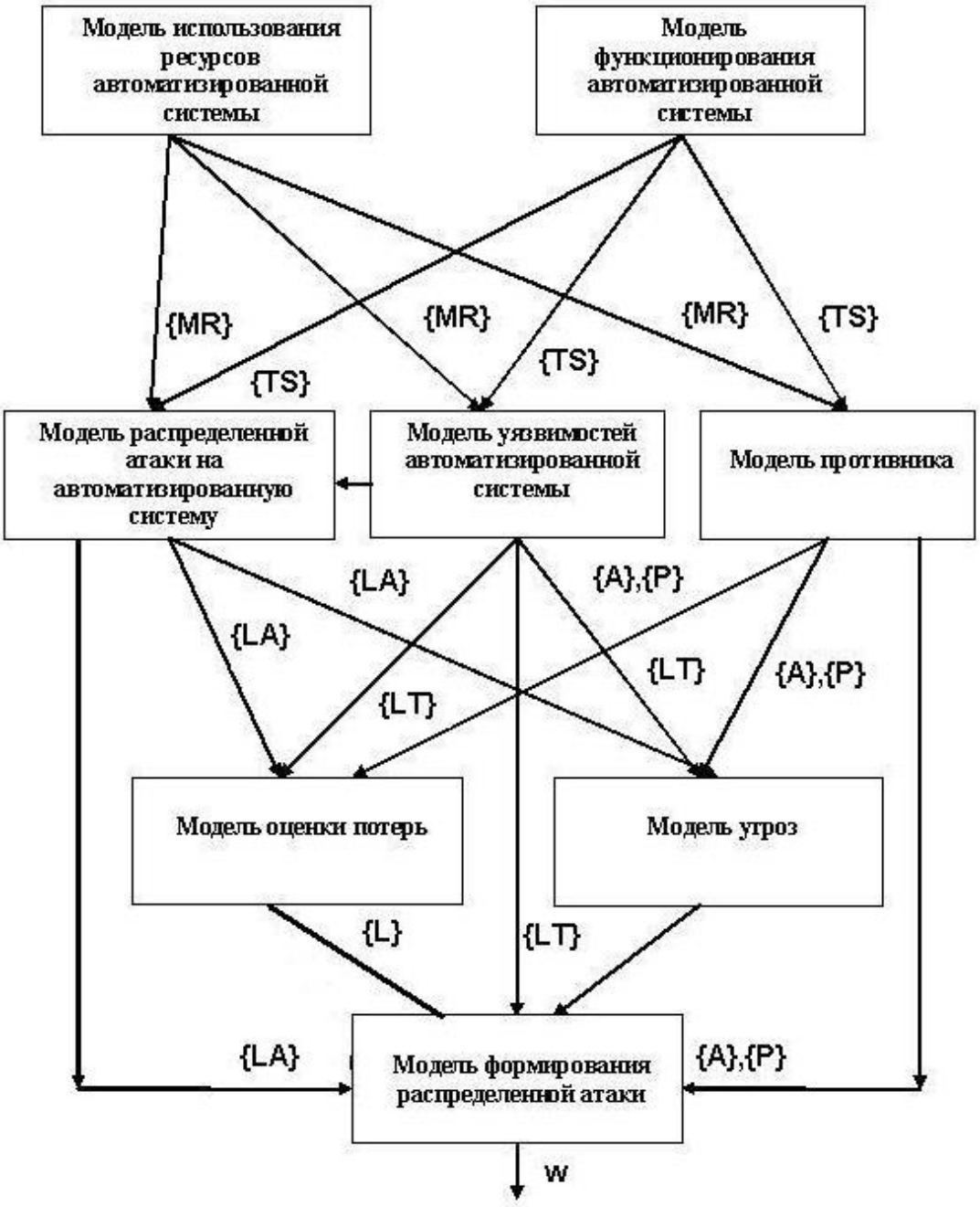

Рисунок 1 - Общая модель процесса формирования распределенной атаки на АС

Модель функционирования АС может быть формально представлена в виде функции:

$$F\_MF(AS) \rightarrow \{TS\}$$

В качестве исходных данных функции будет выступать АС. Результатом указанной функции будет формальное описание технологии функционирования системы.

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.

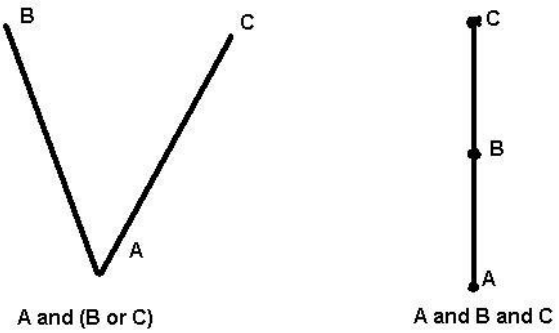

Рисунок 2 - Правила формирования графа распределенной атаки на АС

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}*.

8. Все найденные в пункте 7 разрезы графа распределенной атаки на АС занести в таблицу вида < *RZ(i)* ><{*NL*} ><{ γ_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.

9. 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).

$$R(\gamma) = \sum_{i=1}^{N} L_i (P_i - \sum_{j=1}^{M} G_{ij} \cdot \gamma_j); \qquad (1)$$

$$C_d = \sum_{j=1}^{M} \gamma_j \cdot (C(\gamma)_j + X(\gamma)_j); \qquad (2)$$

10. В результате будет сформирована таблица, в которой первый столбец - вектор *RZ(i)*, второй - размер остаточного риска при использовании варианта (*R*), третий - размер затрат на построение КСЗИ (C_d).

Описание переменных, используемых в модели формирования КСЗИ АС приведены в таблице 1.

Таблица 1 - Параметры переменных, используемых в модели формирования КСЗИ АС

Обозначения переменных	Значения переменных	Ограничения переменных	Размерности переменных
R	размер остаточного риска	$R_i > 0$	гривны
N	число угроз информации	$N > 0$	-
L_i	оценка стоимости потерь в случае реализации *i*-ой угрозы	$L_i > 0$	гривны
P_i	вероятность реализации *i*-ой угрозы	$0 \le P_i \le 1$	-
M	число существующих средств защиты	$M > 0$	-
G_{ij}	эффективность *j*-го механизма защиты информации по нейтрализации i-ой угрозы	$0 \le G_{ij} \le 1$	-
γ_i	признак использования *i*-го механизма защиты информации в составе КСЗИ АС (равен 1, если механизм задействован в составе КСЗИ, в противном случае равен нулю)	$\gamma_i \in (0;1)$	-
C_d	средства, которые могут быть выделены на защиту информации в АС	$C_d > 0$	гривны
C_j	затраты на приобретение (разработку) и использование *j*-го механизма защиты информации	$C_j > 0$	гривны
X_j	размер потерь АС, вызванных использованием *j*-го механизма защиты информации в составе КСЗИ АС	$X_j > 0$	гривны

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.

Таблица 2 содержит способы оценки потерь для таких угроз информации, где 1 - свойства информации, нарушаемые распределенной атакой (Д – доступности, К – конфиденциальности, Ц – целостности).

Таблица 2 - Использование методов теории графов для описания распределенной атаки

1	Защита от распределенной атаки	Методы теории графов
К	Не дать проложить трассу к ОЗ	Построение пути минимальной стоимости
Д	Не дать разорвать все трассы доступа к ОЗ	Построение неполного разреза графа распределенной атаки
Ц	Не дать атакующей стороне проложить хотя бы одну трассу доступа с правами на модификацию	Построение пути минимальной стоимости

Выводы из исследования и перспективы дальнейших разработок

Предложенная методика имеет следующие преимущества:

– учитываются принципы организации распределенных атак на АС;

– при создании КСЗИ АС можно определить значение величины C_{d};

– применение предлагаемой методики при модификации существующей КСЗИ АС наглядно демонстрирует возможные затраты на защиту информации (ΔC_{d}) и ожидаемые результаты применения новых механизмов защиты информации (ΔR);

– модифицированный способ формирования КСЗИ АС обладает меньшей вычислительной сложностью, чем по способу, основанному на методах нелинейного программирования [9].

Список использованной литературы

11. 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.
12. Гроздов Г.Г. Модифицированный способ решения задачи формирования эффективной комплексной системы защиты информации автоматизированной системы: моногр. / Г.Г. Гроздов. – К.: ГУИКТ, 2009 – 32 с.
13. Комаров А.А. Тесты на проникновение: методики и современные подходы / А.А. Комаров // Журнал "IT-спец". – М., 2009. – № 2. – С. 48-53.
14. Лукацкий А.В. Обнаружение атак / А.В. Лукацкий. – СПб.: BHV, 2001. – 611 с.
15. Майника Э. Алгоритмы оптимизации на сетях и графах / Э. Майника. – М.: Мир, 1981. – 328 с.
16. Official BSI site. – [Электрон. дан.] – Режим доступа: http://www.bsi.de/english/publications/studies/penetrations.pdf. -Загл. с экрана.
17. Official ISACA site. – [Электрон. дан.] – Режим доступа: http://www.isaca.org. -Загл. с экрана.
18. Official ISSAF site. – [Электрон. дан.] – Режим доступа: http://www.oissg.org/issaf. -Загл. с экрана.

Надійшла до редакції 10.03.2015

Г.Г. Гроздов

МЕТОДИКА ПОБУДОВИ ЗАХИСТУ ВІД РОЗПОДІЛЕНОЇ АТАКИ, ЯКА ОПИСУЄТЬСЯ ЗА ДОПОМОГОЮ ТЕОРІЇ ГРАФІВ

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

A METHOD FOR PROTECTION FROM DISTRIBUTED ATTACKS BASED ON GRAPH THEORY

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

Keywords: penetration test, effective system for data protection.