Литература: 1. Е. Ю. Зайченко, Ю. П. Зайченко. Нахождение максимального потока и анализ показателей живучести сети при отказах. – Автоматика и телемеханика, – 1996, №6. с. 102 – 113. 2. Зайченко О. Ю. Структурный синтез глобальних мереж з технологією АТМ за заданими показниками якості. – Наукові вісті НТУУ "КПІ", – 2001. – №5. с. 5 – 11. 3. Зайченко Ю. П., Зайченко Е. Ю., Поспелов И. В. Комплекс программ анализа и синтеза структуры региональных и глобальных вычислительных сетей: – Управляющие системы и машины. – 2000.– №516. – с. 71–87.

УДК 004.056.5

НЕКОТОРЫЕ ПОДХОДЫ К МОДЕЛИРОВАНИЮ АТАК В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Денис Кудин, Владислав Корольков*

Центр информационной безопасности,

** Запорожский национальный технический университет*

Аннотация: **Анализируется статистика инцидентов компьютерной безопасности, оценивается динамика роста количества инцидентов в год, предлагается усовершенствованная классификация категорий нарушителей, а также улучшенные методы анализа и моделирования атак на информационные системы.**

Summary: **Analyses statistics of computer security incidents, gives an evaluation of annual increase of incidents committed using high information technologies. New improved methods of intruders classification and attack modeling are proposed.**

Ключевые слова: **Атака, нарушитель, моделирование, угроза, безопасность.**

I Введение

Исследование и моделирование атак на информационно-вычислительные сети является одним из ключевых вопросов информационной безопасности (ИБ) автоматизированных и информационных систем. На практике данные вопросы традиционно решаются путем учета известных атак и классифицированием их относительно общих характеристик осуществления атак, таких как: цель атаки, удаленность, уровень модели OSI и т. п. Недостатком указанного подхода является невозможность моделирования атак в виде проявления множества всевозможных угроз ИБ, а значит, определения их первопричин и полного набора факторов, реально влияющих на ИБ системы.

II Анализ статистики инцидентов компьютерной безопасности

По данным Координационного Центра CERT® [1] на 18 июля 2002 г. за период с 1988 по второй квартал 2002 года зарегистрировано **143505** инцидентов компьютерной безопасности. Сведения о количестве инцидентов за указанный период представлены в табл. 1 и на рис. 1.

Таблица 1 – Количество инцидентов компьютерной безопасности за период 1988–2002 гг.

Год	Количество инцидентов	Год	Количество инцидентов
1	**2**	**1**	**2**
1988	6	1996	2573
1989	132	1997	2134
1990	252	1998	3734
1991	406	1999	9859
1992	773	2000	21756
1993	1334	2001	52658
1994	2340	2002 (I-II кварталы)	43136
1995	2412		

Рисунок 1 – Количество инцидентов компьютерной безопасности в период 1988-2001 гг.

Исходя из приведенных выше данных, можно приблизительно спрогнозировать общее количество инцидентов на текущий год.

Пусть P_i – общее количество инцидентов за год i, n – количество лет, S_n – средняя динамика роста количества инцидентов за n лет в процентах. Тогда

$$S_n = \frac{\sum_{i=1}^{n-1} \frac{P_{i+1}}{P_i}}{n} \times 100 . \qquad (1)$$

Возьмем данные за последние 5 лет, с 1997 по 2001 гг. Тогда P_1=2134, P_2=3734, P_3=9859, P_4=21756, P_5=52658, n=5. Подставив эти значения в (1), получим:

$$S_5 = \frac{3734/2134 + 9859/3734 + 21756/9859 + 52658/21756}{5} \times 100 = 180{,}34(\%) . \qquad (2)$$

То есть, **в течение последних пяти лет количество инцидентов в год увеличивается в среднем на 180,34% по сравнению с предыдущим годом.**

Пусть P_6^* – прогнозируемое количество инцидентов на 2002 год. Тогда

$$P_6^* = \frac{P_5 \times S_5}{100} = \frac{52658 \times 180.34}{100} \approx 94963 . \qquad (3)$$

Как видно из табл. 1, за первые 2 квартала 2002 г. уже зарегистрировано 43136 инцидентов компьютерной безопасности, что составляет 45% от годового прогнозируемого значения (3), т. е. можно сделать вывод, что, при неизменной динамике роста числа инцидентов, данный прогноз окажется достаточно достоверным.

Но главным является другой вывод, который можно сделать из анализа приведенных статистических данных – при столь высоком темпе роста различного рода нарушений, осуществляемых с помощью компьютерных технологий, особенно актуальным является вопрос разработки эффективных методов противодействия и предотвращения этих нарушений.

III Категории нарушителей

Под атакой будем понимать преднамеренную попытку реализации угроз конфиденциальности, целостности, доступности или наблюдаемости информации в компьютерной, автоматизированной или информационной системе (ИС).

В качестве нарушителя рассматривается лицо, которое может получить доступ к работе с включенными в состав компьютерной системы (КС) средствами. Предполагается, что нарушитель является специалистом высшей квалификации, имеющим полную информацию о компьютерной системе и комплексе средств защиты в ней. Нарушители классифицируются по уровню возможностей, предоставляемых им штатными средствами КС. Согласно [2] выделяется четыре уровня этих возможностей. Классификация является иерархической, т. е. каждый последующий уровень включает в себя функциональные возможности предыдущего.

Введем следующие обозначения:

$\mathbf{L_1}$ – первый уровень, определяет самый низкий уровень возможностей ведения диалога в КС – возможность запуска фиксированного набора задач (программ), реализующих заранее предусмотренные функции по обработке информации;

$\mathbf{L_2}$ – второй уровень, определяется возможностью создания и запуска собственных программ с новыми функциями по обработке информации;

$\mathbf{L_3}$ – третий уровень, определяется возможностью управления функционированием КС, т. е. воздействием на базовое программное обеспечение системы, а также на состав и конфигурацию ее оборудования;

$\mathbf{L_4}$ – четвертый уровень, определяется всем объемом возможностей лиц, осуществляющих проектирование, реализацию и ремонт аппаратных компонентов КС, вплоть до включения в состав КС собственных средств с новыми функциями по обработке информации.

При этом

$$\mathbf{L_1} \subset \mathbf{L_2} \subset \mathbf{L_3} \subset \mathbf{L_4}. \quad (4)$$

Однако приведенная выше классификация недостаточно четко отражает характер угроз. Поэтому целесообразно, на наш взгляд, описать уровни возможностей нарушителя следующим образом:

$\mathbf{L_1}$ – первый уровень – возможность **несанкционированного чтения критичной информации**;

$\mathbf{L_2}$ – второй уровень – возможность **несанкционированного исполнения программ**;

$\mathbf{L_3}$ – третий уровень – возможность **несанкционированной модификации** (включая удаление) **критичной информации**;

$\mathbf{L_4}$ – четвертый уровень – возможность **несанкционированного получения прав администратора КС либо прав уровня системы**;

$\mathbf{L_5}$ – пятый уровень – возможность посредством уязвимой КС **получения полных прав доступа к ресурсам автоматизированной или информационной системы**, в состав которой входит данная КС.

В данном случае, в отличие от предыдущего (4), не сохраняется явной "вложенности" уровней, поскольку нарушитель, обладая правами модификации критичной информации, необязательно будет обладать правами запуска произвольных программ и т. д. Здесь имеет место следующее соотношение:

$$\left\{\mathbf{L_1} \cap \mathbf{L_2} \cap \mathbf{L_3}\right\} \subset \mathbf{L_4} \subset \mathbf{L_5}. \quad (5)$$

Категория нарушителя будет соответствовать уровню его возможностей.

Такая классификация нарушителей является полезной для использования в процессе оценки рисков, анализа уязвимости системы, эффективности существующих и планируемых мер защиты.

IV Моделирование атак

Рассмотрим некоторые подходы к моделированию атак в информационных системах.

В работе [3] предложен подход, основанный на рассмотрении вариантов (сценариев) атак как реализации совокупности преднамеренных угроз ИБ – событий или действий, способных потенциально снизить степень безопасности системы. Преимуществом такого подхода являются определение полного множества первопричин атак и факторов ИБ, а также возможность моделирования различных сценариев осуществления атак.

Согласно [3] угрозы разделяются на два класса:

- операционные дефекты;
- ошибки администрирования.

Операционные дефекты характеризуют технологическую безопасность информационного ресурса и являются результатом ошибок проектирования и реализации программного обеспечения ИС. Для удобства создания систем защиты и моделирования проникновения в ИС целесообразно классифицировать ошибки проектирования по механизмам (подсистемам) безопасности системы.

При этом основными типами операционных дефектов являются:

- недостатки механизма аутентификации;
- недостатки механизма разграничения доступа;
- недостатки механизма целостности данных;
- недостатки механизма криптографии;
- недостатки сетевых протоколов;
- ошибки программной реализации;
- и др.

Ошибки администрирования характеризуют эксплуатационную безопасность и являются результатом некорректных настроек операционной системы (ОС) и ее приложений по отношению к назначению ИС и требованиям к ее безопасности. Причинами ошибок администрирования могут быть различные

некомпетентные, халатные или злонамеренные действия администраторов и пользователей ИС. Основными типами ошибок администрирования являются:

- ошибки параметров подключения пользователей;
- ошибки настройки парольной защиты и использование легко подбираемых паролей;
- ошибки конфигурирования сервера, назначения полномочий;
- и др.

С учетом потенциальных угроз ИБ можно построить обобщенную модель атаки в виде четверки:

$$A = \{O, T, R_t, R_{ot}\}, \tag{6}$$

где:

O – множество защищаемых объектов (целевое множество атак);

$T = \{T_d, T_a\}$ – множество угроз, T_d – множество операционных дефектов, T_a – ошибки администрирования;

$R_t = T \times T$ – декартово множество угроз;

$R_{ot} = R_t \times O$ – декартово множество угроз и объектов.

Таким образом, получается некоторое пространство факторов, влияющих на реальную степень безопасности.

Недостатком данного подхода является, с нашей точки зрения, двухуровневая классификация возможных угроз на операционные дефекты и ошибки администрирования. Как показывают исследования и практический опыт ошибки пользователей целесообразно выделить в отдельную категорию. Конечный пользователь ресурсов информационной системы, как правило, не имеет никакого отношения к ее администрированию и настройке каких-либо параметров системы. Тем не менее, его преднамеренные или случайные действия могут нести серьезную угрозу безопасности ИС. Кроме того, обобщенную модель атаки предлагается расширить множеством объектов комплекса средств защиты, которые должны противодействовать осуществлению атаки. Исходя из этого, можно видоизменить выражение (6) следующим образом:

$$A = \{O, T_d, T_a, T_u, R_t, R_{ot}, K\}, \tag{7}$$

где:

O – множество защищаемых объектов (целевое множество атак);

T_d – множество операционных дефектов;

T_a – множество ошибок администрирования;

T_u – множество ошибок пользователей;

$R_t = T \times T$ – декартово множество угроз ($T = \{T_d, T_a, T_u\}$);

$R_{ot} = R_t \times O$ – декартово множество угроз и объектов;

K – множество объектов комплекса средств защиты ИС.

Другой подход к моделированию атак предлагается в работе [4]. Суть его состоит в том, что ход атаки подробно документируется в структурированной форме, после чего строятся палитры (patterns) и деревья (trees) типовых атак. Далее из деревьев выделяются все возможные сценарии атак, которые и передаются разработчикам для создания эффективных средств обнаружения вторжений.

Дерево атаки состоит из узлов, которые представляют собой цели или подцели атаки. При этом узел дерева атаки может состоять из:

- набора подцелей атаки, каждая из которых должна быть достигнута для успешного осуществления атаки (И-декомпозиция);
- набора подцелей атаки, хотя бы одна из которых должна быть достигнута для успешного осуществления атаки (ИЛИ-декомпозиция).

Представление для И-декомпозиции:

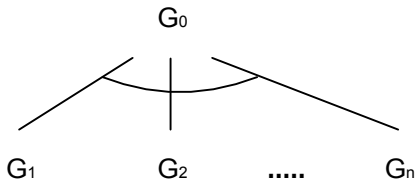

Рисунок 2 – И-декомпозиция

Цель G_0 будет достигнута лишь в том случае, если будет достигнута каждая из подцелей $G_1, G_2, \ldots, G_n$.

Представление для ИЛИ-декомпозиции:

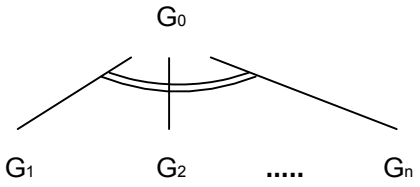

Рисунок 3 – ИЛИ-декомпозиция

Цель G_0 будет достигнута в том случае, если будет достигнута хотя бы одна из подцелей G_1, G_2, …, G_n.

Дерево атаки может состоять из любого набора И- и ИЛИ-декомпозиций. Каждый индивидуальный сценарий атаки генерируется путем обхода дерева от корня к листьям.

Приведем простейший пример:

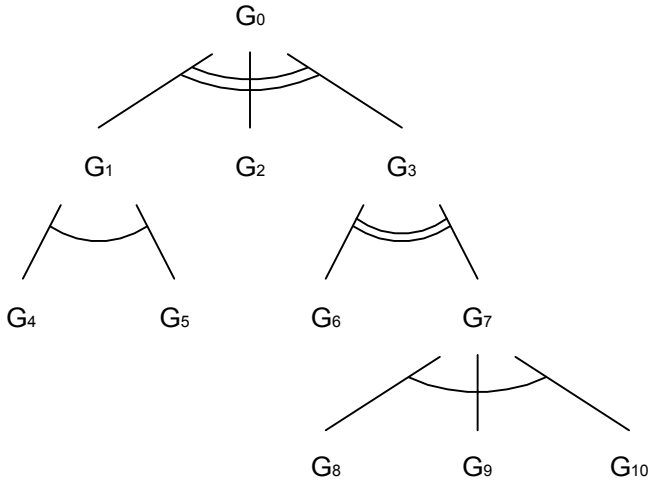

Рисунок 4 – Пример дерева атаки на цель G_0

По данному дереву можно сгенерировать четыре возможных сценария атак:

(G_4, G_5)
(G_2)
(G_6)
(G_8, G_9, G_{10})

Моделирование атак с помощью деревьев позволяет детализировать сценарий до уровня, выбранного разработчиком.

Недостатком данного подхода является низкий уровень "эвристики", привязанность к известным типам атак. Можно обнаруживать и блокировать действия нарушителя, когда они идут по типовому сценарию. Но если атака развивается по сценарию, не заложенному в систему обнаружения вторжений, то обнаружить ее будет невозможно.

Однако универсальность данной схемы увеличивается путем повышения уровня абстракции. В качестве листьев дерева предлагаем использовать все возможные методы атак, в качестве промежуточных узлов – множества сценариев действий атакующего, которые приводят к успешной реализации данного типа атаки, в качестве корня – уровень угроз $\mathbf{L_5}$ или $\mathbf{L_4}$, предложенные выше.

Существуют и другие подходы к моделированию атак, рассмотренные в [5–8].

V Выводы

Статистика инцидентов компьютерной безопасности говорит об огромном росте количества совершаемых атак с использованием компьютерных сетей и систем из года в год. Так, если за 1997 год было зарегистрировано 2134 инцидентов, то в 2001 году это количество составило уже 52658, что почти в 25 раз больше. Показано, что в течение последних пяти лет количество инцидентов в год увеличивается в среднем на **180,34%** по сравнению с предыдущим годом. На основании этих данных было спрогнозировано количество инцидентов на текущий год – **94963**. Рассмотрены существующие методы классификации

нарушителей и моделирования атак, их достоинства и недостатки. На основании анализа предложены усовершенствованные схемы моделирования.

Литература: 1. CERT/CC Statistics 1988-2002 – http://www.cert.org/stats/. 2. НД ТЗИ 1.1-002-99. Общие положения по защите информации в компьютерных системах от несанкционированного доступа. // Департамент специальных телекоммуникационных систем и защиты информации Службы безопасности Украины. – Киев, 1999. 3. Парр Г. Л., Марков А. С. Анализ атак на автоматизированные системы на основе угроз информационной безопасности. (Балтийский государственный технический университет "ВОЕНМЕХ"). 4. Andrew P. Moore, Robert J. Ellison, Richard C. Linger. Attack Modeling for Information Security and Survivability. Technical Note CMU/SEI-2001-TN-001, 2001. 5. Joshua W. Haines, Lee M. Rossey, Richard P. Lippmann. Extending the DARPA Off-Line Intrusion Detection Evaluations. Lincoln Laboratory, Massachusetts Institute of Technology. 6. Jan Steffan, Markus Schumacher. Collaborative Attack Modeling. Department of Computer Science, Darmstadt University of Technology. 7. Nikhil Ashok Joshi. Resource/Attack Modeling and Optimal Intrusion Recovery. Master of science Thesis. University of California at Davis, 2002. 8. Wenke Lee, Wei Fan, Matthew Miller, Salvatore J. Stolfo, and Erez Zadok. Toward Cost-Sensitive Modeling for Intrusion Detection and Response. Journal of Computer Security, 2001.

УДК 33.140

КОМПЛЕКС ДЛЯ ПРОВЕДЕННЯ СПЕЦІАЛЬНИХ ДОСЛІДЖЕНЬ “АСТРА-В” – НОВА ТЕХНОЛОГІЯ ДОСЛІДЖЕНЬ ПОБІЧНИХ ЕЛЕКТРОМАГНІТНИХ ВИПРОМІНЮВАНЬ І НАВОДІВ

Володимир Свириденко, Володимир Угрімов, Сергій Джигамон, Анатолій Передерко, Олександр Шпіта*, Михайло Прокофьєв**

*Міністерство оборони, *ПП “Бумекс”, **НДЦ “ТЕЗІС” НТУУ “КПІ”*

Анотація: **Комплекс забезпечує виявлення радіосигналів, аналіз характеристик електромагнітного поля, проведення спеціальних досліджень ПЕМВН, реєстрацію, зберігання, обробку і документування одержаних результатів.**

Summary: **A complex provides exposure of signals radio, descriptions analysis of electromagnetic field, bowing of special SERNP researches, registration out, keeping, treatment and documenting of obtained results.**

Ключові слова: **Комплекс, спеціальні дослідження, пакет прикладних програм.**

Вступ

Глобальна автоматизація практично всіх сфер людської діяльності привела до виникнення ряду нових проблем, однією з яких є збільшення можливості несанкціонованого витоку інформації за рахунок побічних електромагнітних випромінювань і наведень (ПЕМВН). Основними причинами цієї проблеми стали:

- різке збільшення граничної частоти задавальних генераторів і, як наслідок, виникнення можливості витоку інформації за рахунок як розширення діапазону частот, так і нових фізичних ефектів;
- поява сучасних, більш ефективних, засобів знімання інформації.

Вирішення вищеназваної проблеми в значній мірі забезпечує використання комплексу для проведення спеціальних досліджень “АСТРА-В”, в якому реалізовані нові методологія і технологія проведення досліджень ПЕМВН. Відповідно до НД ТЗІ 1.5-001-2000 комплекс відноситься до групи Г2 (аналізувальні радіовиявлювачі).

Комплекс забезпечує виявлення радіосигналів, аналіз характеристик електромагнітного поля, проведення спеціальних досліджень ПЕМВН, реєстрацію, зберігання, обробку і документування одержаних результатів.

Комплекс має такі характерні особливості:

- відкритість архітектури на рівні апаратних і програмних засобів;
- використання спеціальної методології, алгоритмів і програмних засобів обробки результатів спеціальних досліджень;
- наявність засобів автоматизації розрахунку результатів досліджень з видачею актів обстеження.