ББК 33973.202

О КЛАССИФИКАЦИИ СЦЕНАРИЕВ КОМПЬЮТЕРНЫХ АТАК*

Г.Э. Яхъяева

Новосибирский государственный университет

Рецензент В.Е. Подольский

Ключевые слова и фразы: базовые критерии формирования модели компьютерной атаки; киберпреступность; методика построения классификации; модели компьютерной атаки; сценарий компьютерной атаки.

Аннотация: Предлагается методика построения классификации, базирующейся на описании модели компьютерной атаки. Сформулированы основные определения, которые могут рассматриваться как базовые критерии для формирования модели компьютерной атаки.

С каждым днем компьютерные технологии входят все глубже и глубже в нашу жизнь, все больше и больше отдельных компьютеров и целых компьютерных сетей подключаются к Интернету. Все больше и больше мы начинаем зависеть от компьютеров. Проникновение компьютерных технологий во все сферы государственной и общественной жизни многих стран повлекло формирование нового поля деятельности и для преступников. Появились такие термины, как «киберпреступность», преступления в «сфере высоких технологий», «компьютерные преступления».

Сейчас в Интернете тема компьютерного терроризма очень популярна, но информация в большинстве случаев представлена в неструктурированном, либо слабоструктурированном виде. Существующие ресурсы по данной тематике обладают некоторыми серьезными недостатками, связанными, прежде всего, с необходимостью поиска нужной информации из сотен и тысяч предоставленных в данном ресурсе текстов. Поэтому сегодня, как никогда ранее, остро встает вопрос о составлении классификации «деятельности» киберпреступников.

Какая бы хорошая классификация моделей кибератак не была бы проделана, она очень быстро устаревает, требует дополнительной переработки или даже полного пересмотра.

*Поддержано грантом Федерального агентства по науке и инновациям № 02.442.11.7305.

Яхъяева Г.Э. – кандидат физико-математических наук, доцент факультета информационных технологий Новосибирского государственного университета.

В связи с этим необходима методика, позволяющая:

– исходя из имеющейся в базе знаний информации о реально происшедших кибератаках, быть способной выдавать классификацию сценариев атак;

– отслеживая информацию о появлении принципиально новых «изобретений» киберпреступников, быть гибкой для расширения списка существующих характеристик атак.

Мы предлагаем методику построения классификации, базирующейся на описании модели компьютерной атаки. Впервые описание модели компьютерной атаки было предложено в работе [1]. Сформулируем основные определения, которые могут рассматриваться как базовые критерии для формирования модели компьютерной атаки.

M_1 : **Первичный объект** [1] – компьютеры или комплексы компьютеров.

M_2 : **Первичная цель** – искажение работы или уничтожение отдельных компонентов первичного объекта.

M_3 : **Вторичный объект** [1] – персона или группа людей, материальные объекты различного назначения, информационные системы, которые могут быть подвержены деструктивным воздействиям со стороны первичных объектов, вплоть до уничтожения.

M_4 : **Вторичная цель** – конечная цель террористического действия.

M_5 : **Субъект действия** [1, 2] – персона или группа лиц, имеющих целью проведение террористических действий против вторичных объектов посредством воздействия на первичные объекты.

M_6 : **Средства действия («оружие»)** – средства уничтожения, искажения или хищения информационных массивов с первичных объектов, средства преодоления систем защиты первичных объектов, дезорганизации работы первичных объектов и т.п.

M_7 : **Способ осуществления** – стратегия воздействия субъекта на первичный объект данного террористического действия.

Таким образом, каждый сценарий компьютерной атаки может быть классифицирован по семи различным классификациям (критериям). Распишем эти классификации.

I *Классификация* M_1 : ***Первичный объект*** [1].

M_1^1 : персональный компьютер;

M_1^2 : компьютерный комплекс для относительно узкой области применения;

M_1^3 : большая интегрированная система распределенных информационно-вычислительных ресурсов.

II *Классификация* M_2 : ***Первичная цель*** [4, 6].

M_2^1 : информационные ресурсы;

M_2^2 : операционные системы ;

M_2^3 : сетевое программное обеспечение;

M_2^4 : системы управления базами данных;

M_2^5 : аппаратные средства (железо).

III *Классификация* M_3 : ***Вторичный объект*** [1].

M_3^1 : персона или группа людей;

M_3^2 : материальные объекты различного назначения;

M_3^3 : информационные системы.

IV *Классификация* M_4 : ***Вторичная цель*** [7].

M_4^1 : нанесение ущерба;

M_4^2 : кража;

M_4^3 : шантаж.

V. *Классификация* M_5 : ***Субъект действия*** [3].

M_5^1 : *внешний* – не имеющий санкционированного доступа к данному первичному объекту;

M_5^2 : *внутренний* – имеющий санкционированный доступ к данному первичному объекту.

VI *Классификация* M_6 : ***Средства действия*** [3, 5].

M_6^1 : *вирусные программы* – способны размножаться, внедряться в программы, передаваться по линиям связи, сетям передач данных, выводить из строя системы управления и т.п.;

M_6^2 : *логические бомбы* – запрограммированные устройства, которые внедряют в информационно-управляющие центры военной или гражданской инфраструктуры, чтобы по сигналу или в установленное время привести их в действие;

M_6^3 : *взломщики парольной защиты операционной системы*;

M_6^4 : *зомби* – программы, инициализирующие распределенные атаки на отказ от обслуживания, нацеленные на конкретные Web-узлы, вызывающие переполнение последних за счет преднамеренного направления на них Internet-трафика большого объема;

M_6^5 : *средства подавления информационного обмена в телекоммуникационных сетях* – фальсифицируют информацию в каналах государственного и военного управления;

M_6^6 : *средства нейтрализации тестовых программ*;

M_6^7 : *ошибки* различного рода, сознательно вводимые лазутчиками в программное обеспечение объекта.

VII *Классификация* M_7 : ***Способ осуществления*** [3, 4].

M_7^1 : *структурированная атака* – атака, направленная против конкретного первичного объекта;

M_7^2 :*неструктурированная атака* – атака, адресуемая по принципу «кому бог пошлет»;

M_7^3 :*явная атака* – открытая, понятная и однозначно предсказуемая;

M_7^4 :*скрытая атака* – не очевидная, требующая для противодействия ей дополнительных предположений о первичной и/или вторичной цели данной атаки.

Список литературы

1 Васенин, В.А. Информационная безопасность и компьютерный терроризм / В.А. Васенин // Научные и методологические проблемы информационной безопасности : под. ред. В.П. Шерстюка. – М.: МЦНМО, 2004.

2 Грушко, А.А. Языки в скрытых каналах / А.А. Грушко, Е.Е. Тимонина // Труды международной конференции «Информационные технологии в науке, образовании, телекоммуникациях, бизнесе». – Украина, Крым, Ялта-Гурзуф, 2003.

3 Соколов, А. Защита от компьютерного терроризма : справочное пособие / А. Соколов, О. Степанюк. – БХВ-Петербург, Арлит, 2002. – 496 с.

4 Щеглов, А.Ю. Защита компьютерной информации от несанкционированного доступа / А.Ю. Щеглов. – СПб: Наука и техника, 2004. – 384 с.

5 Голубев, В. / В. Голубев, Т. Сайтарлы // Проблемы борьбы с кибертерроризмом в современных условиях (www.crime-reserch.ru).

6 Самоучитель по защите информации (http://webhost.urbannet.ru/Firewall/Protection_to_information/index.html).

7 Старостина, Е. Кибертерроризм – подход к проблеме / Е. Старостина (www.crime-reserch.ru).

To Classification of Computer Attacks Scenarios

G.E. Yakhyva

Novosibirsk State University

Key words and phrases: basic criteria of formation of computer attack model; cybercrime; methodology of classification construction; computer attacks models; computer attack scenarios.

Abstract: The methodology of construction of classification based on the description of computer attack model is proposed. Basic notions, which can be used as basic criterions for formation of computer attack model, are formulated.
