УДК 681.3

Н. А. Калинина

МОДЕЛИРОВАНИЕ АТАКУЮЩИХ ВОЗДЕЙСТВИЙ И СРЕДСТВ ЗАЩИТЫ КОРПОРАТИВНОЙ СЕТИ С ПОМОЩЬЮ СЕТЕЙ ПЕТРИ

Представлена обучающая система настройки сетевой безопасности на основе моделирования атакующих воздействий и средств защиты с помощью иерархических сетей Петри. Рассмотрены особенности такого моделирования с учетом уязвимостей программного обеспечения.

Ключевые слова: иерархическая сеть Петри, моделирование, обучающая система.

Организация системы защиты локальной компьютерной сети является сложной задачей, в которой приходится учитывать большое количество параметров. Влияние этих параметров нередко взаимно противоположно, а часто неопределенно и плохо предсказуемо. Такое положение объясняется тем, что нужно организовать защиту не сети как таковой, а сети со всеми функционирующими внутри нее информационными системами, которые содержат огромное множество компонентов. Обычна ситуация, когда на различных сетевых узлах установлены разные операционные системы (ОС) (иногда две или несколько ОС одновременно), жесткие диски имеют разные файловые системы, состав категорий пользователей и их права на использование ресурсов компьютера различны и, наконец, программное обеспечение в высшей степени разнообразно. А поскольку все эти факторы влияют на возможность реализации конкретных атак, построение системы защиты, учитывающей их в полной мере, является весьма трудоемкой задачей.

В такой ситуации может быть полезна система, способная моделировать процесс атакующих воздействий в зависимости от наличия или отсутствия всех перечисленных (а также неперечисленных) факторов. В Сибирском государственном технологическом университете (СибГТУ) разработана обучающая программная система, моделирующая этот процесс на основе использования иерархических сетей Петри.

Процесс моделирования атак с помощью сетей Петри рассматривался в нескольких работах зарубежных авторов [1–3].

Так, Дж. П. Дермотт [1] предложил моделирование сетевых атак сетями Петри, в которых позиции представляют собой состояния, важные для безопасности системы. Переходы в этих сетях – это события, команды или данные, которые могут быть важными для изменения состояния системы в отношении безопасности. Фишки в такой сети Петри переходят от позиции к позиции, показывая развитие атаки. При данном способе моделирования этапы атаки представлены разными позициями, подобно вершинам в дереве атак. Этот способ моделирования хорошо показывает процесс развития атаки с помощью положения фишек, однако созданная с его помощью модель не поддерживает представление мер защиты против атак. Кроме того, совершенно не ясно, как эта модель может способствовать получению требований к безопасности или как архитектура системы влияет на безопасность.

В работе [2] рассмотрено моделирование атак с помощью цветных сетей Петри (*Colored Petri Net*, CPN). Такая модель является достаточно гибкой для моделирования сетевых вторжений из Интернета, включая статические и динамические аспекты атаки. В этой работе представлены процедуры и методы построения модели на сети CPN, исходя из дерева атак. Чтобы оценить возможный ущерб от вторжения, в полученную модель введены стоимостные оценки. Также показано, как можно использовать ее для моделирования методов защиты.

В работе О. Дахла и С. Волтусена [3] предложен механизм для имитационного моделирования сложных многостадийных и многоагентных уязвимостей в сетевых и распределенных системах, основанный на стохастических и спланированных по времени CPN. Авторы использовали модель гипотетических изъянов (FHM) для создания теста на проникновение (*penetration test*) в информационную систему на базе использования CPN.

Однако ни в одной из этих работ не было попыток связать возможность проведения атаки со свойствами компонентов информационных систем, настройками систем защиты (например, правилами фильтрации межсетевых экранов) и создать обучающую систему такого типа. Система имитационного моделирования атакующих воздействий, разработанная в СибГТУ, является обучающей системой, которая позволяет учесть не только настройки информационной системы, но и уязвимости установленного программного обеспечения.

Реальный процесс возникновения и развития атакующего воздействия на сеть является вероятностным в нескольких аспектах: во-первых, вероятностным событием является само возникновение нарушителя (он может появиться или не появиться в случайный момет времени); во-вторых, случайной величиной будет возможная квалификация нарушителя, которая является очень важным параметром для реализации атаки; в-третьих, при наличии всех необходимых условий успешная реализация атаки – тоже процесс, реализуемый с определенной вероятностью, а не строго детерминированный. Поэтому сеть Петри, моделирующая эти процессы, будет сетью со случайными срабатываниями переходов.

Квалификация нарушителя является параметром, имеющим большое значение для дальнейшей реализации атак, поскольку эта квалификация определяет, какие виды атак доступны нарушителю. Возможные значения квалификации, аналогично общепринятой градации [4], назначим следующими: высокая, средняя и низкая. Нарушителю с высокой квалификацией доступны все виды атак, нарушителю со средней квалификацией – атаки, требующие средней или низкой квалификации, наруши-

телю с низкой квалификацией – только атаки, требующие низкой квалификации.

Когда степень квалификации определена, возможны два варианта проведения атаки: предпринята либо успешна, либо неуспешная атака (даже при наличии всех условий для ее проведения неуспех атаки может определяться субъективными или неучтенными факторами). В обоих случаях после этого нарушитель может либо прекратить деятельность, либо продолжить ее (квалификация при этом не изменяется). Переход, соответствующий успешной атаке, является составным переходом, внутри которого функционирует сеть Петри, соответствующая выбранной атаке.

Рассмотрим иерархическую сеть Петри со случайными срабатываниями переходов, дающую один из возможных вариантов представления описанной выше модели (рис. 1).

Обозначим позиции буквами PL, переходы – буквами T, вероятности срабатывания переходов – буквами P. Прямоугольниками покажем составные переходы, внутри которых будет присутствовать сеть Петри, моделирующая конкретную атаку. При этом набор моделей, которые могут появиться внутри составного перехода, определяется уровнем квалификации нарушителя. Таким образом, набор моделей в составном переходе T6 является подмножеством множества моделей T5, а набор моделей в составном переходе T5 – подмножеством множества моделей T4.

Позиции и переходы на рис. 1 имеют следующий смысл:

– PL1 – появление нарушителя;

– PL2 – нарушитель обладает высокой квалификацией;

– PL3 – нарушитель обладает средней квалификацией;

– PL4 – нарушитель обладает низкой квалификацией;

– PL5, PL7, PL9 – атака, требующая соответственно высокой, средней или низкой квалификации, реализована;

– PL6, PL8, PL10 – атака, требующая соответственно высокой, средней или низкой квалификации, не реализована;

– PL11 – нарушитель прекратил атакующую деятельность;

– T1, T2, T3 – определение квалификации нарушителя (соответственно высокой, средней, низкой);

– T4, T5, T6 – составные переходы, внутри которых находится сеть Петри, реализующая успешную попытку конкретной атаки;

– T7, T9, T11 – неуспешная попытка реализации атаки;

– T8, T10, T12, T17, T19, T21 – принятие решения о продолжении атакующей деятельности;

– T13, T14, T15, T18, T20, T22 – принятие решения о прекращении атакующей деятельности.

Вероятности срабатываний переходов P1, P2, P3, соответствующие переходам T1, T2, T3, определяют вероятность появления нарушителя с высокой, средней и низкой квалификацией. Этот параметр является в системе настраиваемым и может принимать любые значения (при

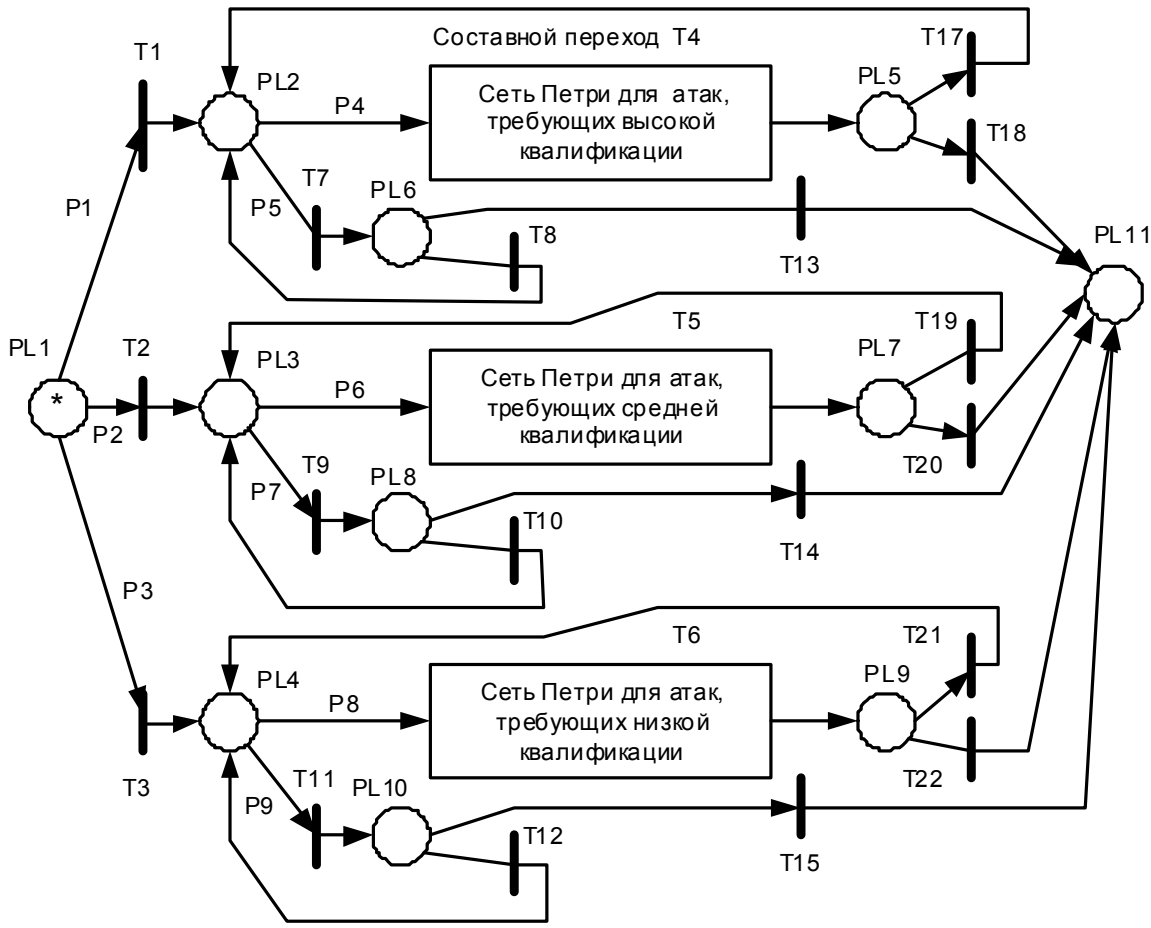

Рис. 1. Иерархическая сеть Петри, моделирующая общую схему атакующего воздействия (обозначения см. в тексте)

условии, что P1 + P2 + P3 = 1). Вероятности переходов P4, P6, P8 определяют вероятность успешного проведения атаки, вероятности P5, P7, P9 – вероятность неудачи при реализации атаки (при этом P4 + P5 = 1, P6 + P7 = 1, P8 + P9 = 1). Эти вероятности являются результатом экспертных оценок специалистов и для известных типов атак приводятся в соответствующих базах данных [5; 6]. Попытка определения того, какая атака будет предпринята нарушителем, находится случайным образом генератором случайных чисел, делающим выбор из совокупности имеющихся моделей атак. Вероятность принятия решения о прекращении нарушителем деятельности может в общем случае определяться множеством разных вариантов. В предварительной версии системы предполагается, что нарушитель ведет атакующую деятельность до полной компрометации сети.

Рассматриваемая в данной статье система имитационного моделирования атакующих воздействий может помочь в определении конфигурации сети, операционных систем и программного обеспечения (ПО), минимизирующих риск реализации атаки. Однако для работы в условиях реального функционирования сети необходима разработка полной базы данных сетей Петри по отдельным видам атак. Создание такой базы в полном объеме и ее поддержка в актуальном состоянии является весьма трудоемкой задачей, требующей к тому же непрерывного сопровождения. Однако в целях обучения навыкам правильного конфигурирования сетевых компонентов может быть использована неполная база данных.

На основе подобной базы в СибГТУ была создана обучающая система, которая позволяет приобретать практические навыки конфигурирования сети, минимизирующего риск компрометации сетевых узлов от различного вида атак. При срабатывании составного перехода в этой системе случайным образом выбирается вид атаки из имеющейся базы данных. Каждому виду атак соответствует конкретная сеть Петри, которая моделирует условия, необходимые для ее выполнения, и сам процесс ее реализации. Пример такой сети, моделирующей атаку типа SQL Injection, приведен ниже (рис. 2).

Сети Петри для конкретных атак не имеют целью показать продвижение нарушителя по хостам сети или отдельные этапы выполнения атаки. В данном случае их цель состоит в том, чтобы показать совокупность условий, необходимых для успешного проведения атаки. Если эти условия существуют, то атака не обязательно будет успешной. Но если их нет, то атака не может быть проведена в принципе.

В сети Петри (см. рис. 2) позиции и переходы имеют следующий смысл:

– P1 – наличие открытого порта для работы по протоколу HTTP (чаще всего это 80-й порт);

– P2 – наличие веб-сервера в составе ПО (тип хоста – веб-сервер);

– P3 – наличие СУБД в составе ПО;

–P4 – наличие в ПО уязвимости, позволяющей реализовать данную атаку;

– P5 – появление нарушителя;

– P6 – SQL-инъекция реализована;

– P7 – модификация данных СУБД;

– P8 – похищение информации;

– P9 – запуск вредоносного кода;

– P10 – расширение привилегий атакующего;

– T1 – открытие порта для работы по протоколу HTTP в межсетевом экране;

– T2 – включение веб-сервера в состав ПО (выбор типа хоста – веб-сервер);

– T3 – включение СУБД в состав ПО;

– T4 – выбор в качестве веб-сервера ПО, имеющего уязвимость к данной атаке;

– T5 – появление нарушителя необходимой квалификации;

– T6 – атака выполняется;

– T7 – нарушитель производит модификацию данных СУБД;

– T8 – нарушитель производит похищение информации;

– T9 – нарушитель производит запуск вредоносного кода;

– T10 – нарушитель производит расширение своих привилегий;

– T11 – атака завершается.

Наличие в ПО уязвимости, позволяющей реализовать данную атаку, зависит от установленного на сетевом узле программного обеспечения. Например, популярный веб-сервер Apach HTTP Server v.2.x имеет уязвимости CVE-2008-2384 и CVE-2007-6342, которые позволяют реализовать атаку SQL Injection. Это значит, что при наличии всех

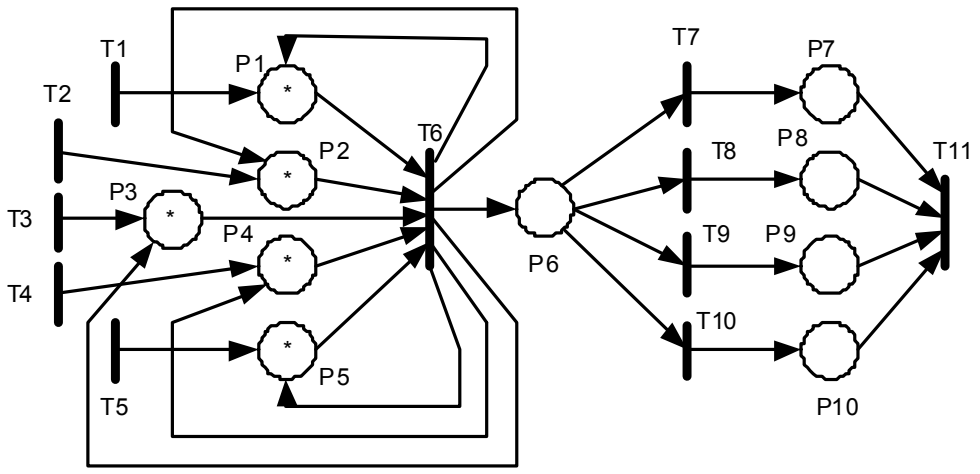

Рис. 2. Сеть Петри, моделирующая атаку SQL Injection (обозначения см. в тексте)

остальных условий установка Apach HTTP Server v.2.x приведет к возможности реализации такой атаки.

База данных моделей атак в рассматриваемой системе частично составлена в соответствии с известной общедоступной базой данных CAPEC (*Common Attack Pattern Enumeration and Classification*) [4], частично – по другим источникам [6; 7]. Кроме сети Петри, описывающей модель атаки, атака включает следующие реквизиты:

– список портов (сетевых протоколов), которые должны быть открыты для реализации атаки;

– степень опасности атаки для сетевого узла;

– типовую вероятность выполнения атаки;

– степень квалификации нападающего, необходимую для выполнения атаки;

– перечень возможных результатов атаки;

– краткое описание атаки.

Внешней оболочкой для процесса моделирования атакующего воздействия является эмуляция сегмента корпоративной сети. При эмуляции учитываются следующие параметры:

– конфигурация сегмента сети, которая учитывается наличие межсетевых экранов и правила фильтрации сетевого трафика, наличие и количество демилитаризованных зон (DMZ);

– тип сетевого узла (рабочая станция, веб-сервер, FTP-сервер, файловый сервер и т. п.);

– вид операционной системы сетевого узла;

– количество разделов жесткого диска и вид файловой системы на каждом разделе;

– права доступа пользователей к каждому разделу;

– программное обеспечение, установленное на сетевом узле.

Каждый из этих параметров оказывает свое влияние на защищенность сети, и в зависимости от их сочетания каждая конкретная атака может быть либо реализована, либо не реализована.

Например, установка конкретного программного обеспечения приводит к наличию уязвимостей, свойственных данной программе, и позволяет осуществить атаку определенного типа. Это связано с тем, что каждая операционная система имеет свой набор уязвимостей и каждая файловая система в свою очередь тоже влияет на этот процесс, поскольку некоторые уязвимости (а следовательно, и атаки) возможны только на определенных файловых системах. Например, реализация файловой системы NTFS в Linux kernel v.2.6.x позволяет нарушителю произвести DoS-атаку при использовании функции _find_get_block_slow.

Учет влияния уязвимостей программного обеспечения на возможность реализации атак приводит к необходимости ведения базы данных уязвимостей каждого программного продукта (рис. 3) и каждой операционной системы. В общем случае это весьма трудоемкая и дорогостоящая процедура, которая финансируется либо государственными структурами развитых стран, либо крупными компаниями. Однако для учебных целей возможно ведение выборочной, неполной базы уязвимостей, что и сделано в представленной обучающей системе (рис. 4).

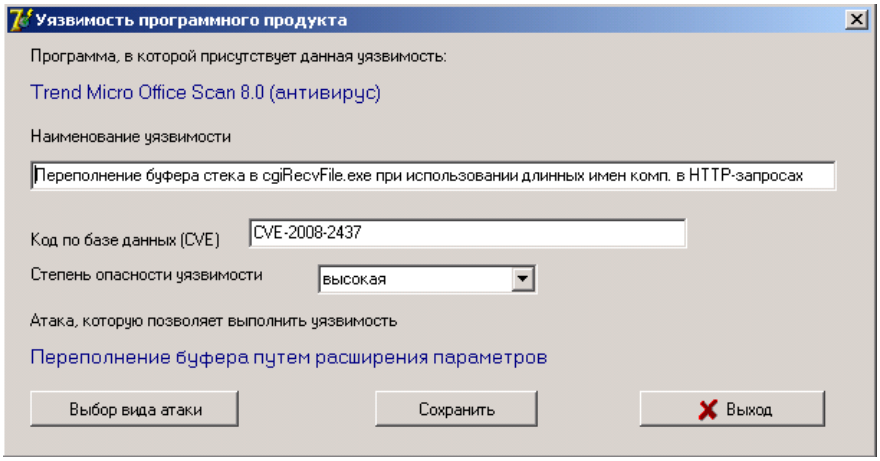

Рис. 3. Вид описания уязвимости CVE-2008-2437

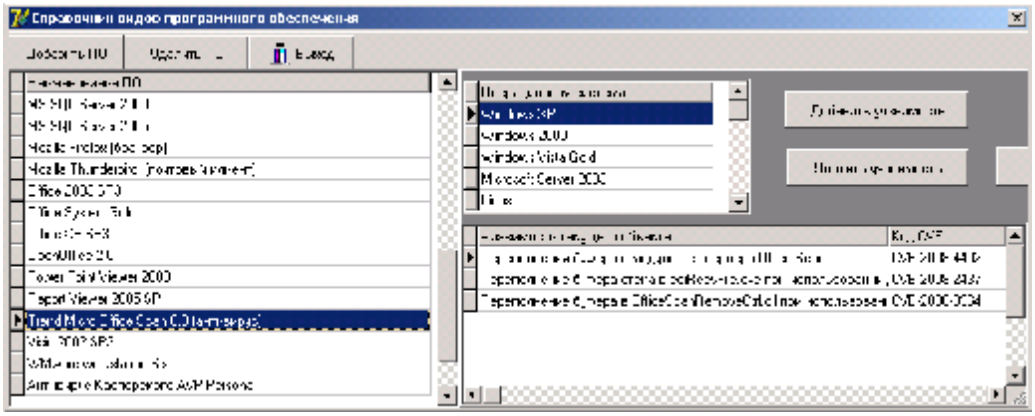

Рис. 4. Режим справочника видов программного обеспечения

Попытка реализации каждой проводимой атаки анализируется системой на каждом конкретном сетевом узле отдельно, поскольку каждый сетевой узел имеет свой набор условий, влияющих на возможность проведения атаки. Прежде всего анализируется квалификация нарушителя, предпринявшего атаку. В базе данных моделей атак использованы оценки этой квалификации, взятые из известной базы данных CAPEC [4]. Если квалификация достаточна, то далее проводится анализ всех условий, необходимых для проведения атаки. При анализе этих условий используется сеть Петри, моделирующая атаку. При отсутствии условий атака считается нереализованной. При наличии всех условий моделируется случайный процесс, с заданной для этой атаки вероятностью приводящий к ее реализации либо нереализации.

Кроме моделирования процесса реализации атаки на конкретном хосте, большой практический интерес представляет моделирование процесса распространения атаки по сети. Этот процесс может быть смоделирован только на имеющейся модели конкретной сети с конкретной топологией сетевых узлов. Поскольку в описанной выше обучающей системе выполняется эмуляция сегмента сети, то такое моделирование также может быть проведено. В реальной локальной сети, как правило, существует только одна точка входа из внешней сети, и в этом случае графическим выражением процесса может быть ориентированное дерево, корнем которого будет точка входа в сеть, вершинами – сетевые узлы, а дугами – сетевые соединения с указанием направления атаки. Возможны два варианта моделирования: первый (упрощенный) – при условии, что скомпрометированный хост (хост, на котором успешно реализована атака) больше не подвергается атакам, второй – при условии, что атаки производятся на все хосты независимо от наличия успешно проведенных атак. Во втором случае граф становится мультиграфом, поскольку он может иметь неограниченную кратность дуг. Однако в рассматриваемой нами системе принят первый вариант.

Распространение атаки в любом варианте может быть произведено только с уже взломанного хоста. В ходе моделирования процесса атакующих воздействий этот результат графически выводится на экран. Кроме того, в процессе работы системы формирует три протокола: протокол появления нарушителей, протокол вредоносной активности каждого нарушителя (рис. 5) и протокол компрометации сетевых узлов.

Представленная в данной статье система имитационного моделирования атакующих воздействий и средств защиты может быть полезна в практических занятиях по информационной безопасности при обучении студентов по специальности «Программное обеспечение вычислительной техники и автоматизированных систем».

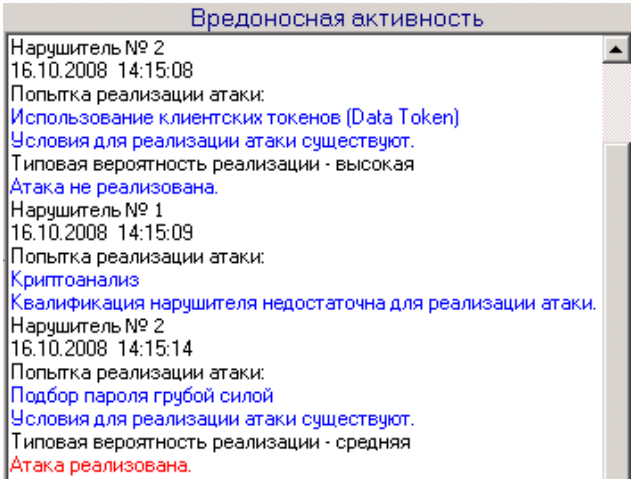

Рис. 5. Фрагмент протокола вредоносной активности

Библиографический список

1. McDermott, J. P. Attack Net Penetration Testing / J. P. McDermott // Proc. of the 2000 Workshop on New Security Paradigm. New York : ACM Press, 2000. P. 15–21.

2. Colored Petri Net Based Attack Modeling / Shijie Zhou, Zhiguang Qin, Feng Zhang et al. // Rough Sets, Fuzzy Sets, Data Mining, and Granular Computing : Proc. of the 9th Intern. Conf. Chongqing, China, 2003. P. 715–718.

3. Modeling and Execution of Complex Attack Scenarios using Interval Timed Colored Petri Nets / O. M. Dahl, S. D. Wolthusen // Proc. of the 4th IEEE Intern. Inform. Workshop. Royal Holloway, UK, 2006. P. 157–168.

4. Common Attack Pattern Enumeration and Classification [Electronic resource]. Electronic data. Access mode: http://capec.mitre.org/data/dictionary.html. Title from display.

5. Common Vulnerabilities and Exposures [Electronic resource]. Electronic data. Access mode: http://Cve.mitre.org. Title from display.

6. National Vulnerability Database [Electronic resource]. Electronic data. Access mode: http://Nvd.nist.gov. Title from display.

7. Низамутдинов, М. Ф. Тактика защиты и нападения на web-приложения / М. Ф. Низамутдинов. СПб. : БХВ-Петербург, 2005.

N. A. Kalinina

ATTACK MODELING OF NETWORK SECURITY BY MEANS OF PETRI NETS

It covers instruction system of network security setting on the basis of attack modeling and network security settings by means of hierarchical Petri Nets. It covers modeling features taking into consideration program vulnerabilities.

Keywords: hierarchical Petri Net, modeling, instruction system.