DOI 10.17223/20710410/5/10

УДК 681.322

МОДЕЛИРОВАНИЕ СЕТЕВЫХ КОМПЬЮТЕРНЫХ СИСТЕМ С УЯЗВИМОСТЯМИ[1]

Д. Н. Колегов

Томский государственный университет, г. Томск, Россия

E-mail: d.n.kolegov@gmail.com

Предлагается дискреционная ДП-модель сетевых компьютерных систем (КС), построенная на основе ДП-модели с функционально и параметрически ассоциированными с субъектами сущностями (ФПАС ДП-модели) и отражающая специфичные условия функционирования сетевых КС с уязвимостями. Показывается возможность применения этой модели для построения всех путей нарушения безопасности в рассматриваемых КС, погружения в неё других моделей, построенных с этой целью, и для проверки условий получения недоверенным субъектом права доступа владения к доверенному субъекту.

Ключевые слова: *сетевые компьютерные системы, тестирование безопасности, граф атак, математические модели безопасности, ДП-модели.*

Введение

Будем рассматривать КС, управляющие доступом и информационными потоками в компьютерных сетях. Будем называть их сетевыми КС. Одним из механизмов обеспечения безопасности таких КС является их тестирование. Среди многих задач тестирования безопасности КС важное место занимает задача обнаружения возможных путей её нарушения, понимаемого как получение недоверенным субъектом права доступа владения к доверенному субъекту КС. Исчерпывающее решение этой задачи предполагает разработку подходящей математической модели безопасности КС — модели, ориентированной именно на построение всех возможных путей нарушения безопасности КС. Моделями с такой ориентацией являются модели формального описания и верификации политик безопасности КС и модели анализа графов атак. Такие модели реализуются подсистемами компьютерного моделирования безопасности в системах автоматизированного тестирования возможности проникновения, управления уязвимостями и предотвращения атак КС.

В известных моделях [1 – 5], ориентированных на построение возможных путей нарушения безопасности КС, обычно строится алгоритм, который из начального состояния КС путем последовательного применения всех определенных в модели правил преобразования состояний, удовлетворящих текущему состоянию КС, получает все возможные траектории ее функционирования. Каждая траектория проверяется на принадлежность к множеству запрещенных траекторий функционирования КС в соответствии с требованиями априорно заданной политики управления доступом и информационными потоками. Основное отличие разных моделей друг от друга заключается в математическом аппарате (формальные грамматики, конечные автоматы, методы верификации, логическое программирование), применяемом для получения всех

[1]Работа выполнена в рамках реализации ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 годы. Результаты работы докладывались на Международной конференции с элементами научной школы для молодёжи, г. Омск, 7–12 сентября 2009 г.

возможных траекторий функционирования КС и построения по ним возможных путей нарушения безопасности. В каждой из этих моделей используются свои, часто не встречающиеся в других моделях определения элементов и механизмов защиты КС, а реализуемый математический аппарат часто недостаточен для определения условий получения недоверенным субъектом права доступа владения к доверенным субъектам. Всё это затрудняет построение и обоснование правил управления доступом, реализация которых в КС позволяет предотвратить нарушение безопасности последних.

В данной работе в основу построения математической модели безопасности сетевых КС положена одна из дискреционных ДП-моделей [6] — ФПАС ДП-модель [7, 8], наиболее полно отражающая особенности современных КС и обеспечивающая возможность алгоритмической проверки условий получения недоверенными субъектами права доступа владения к доверенным субъектам и построения всех возможных путей нарушения безопасности КС. На её основе строится СДУ ДП-модель, представляющая собой ДП-модель сетевой дискреционной КС с уязвимостями, связанными с ошибками в программном обеспечении (ПО), с доверием субъектов, с доступом к паролям субъектов и раскрытием параметров КС, и ориентированная на применение в системах компьютерного моделирования безопасности КС. В ней ФПАС ДП-модель уточняется с учетом существенных особенностей реализации механизмов защиты и их нарушений в современных сетевых КС. После определения СДУ ДП-модели в статье показывается, как такой моделью может быть описана любая реальная сетевая КС и каким образом с её помощью могут быть построены всевозможные пути нарушения безопасности в КС. На примере модели VTG [2] демонстрируется возможность погружения в СДУ ДП-модель других моделей тестирования безопасности КС.

В изложении материала широко используются определения, предположения и обозначения из [6 – 8]. Кроме того, в соответствии с [9, 10] под уязвимостью КС понимается некоторое свойство КС, которое может быть использовано для нарушения ее безопасности.

1. ДП-модель безопасности сетевой дискреционной КС с уязвимостями

ФПАС ДП-модель, на базе которой строится СДУ ДП-модель, предназначена для адекватного моделирования КС широкого класса, а именно всех таких КС управления доступом и информационными потоками, в которых сущности могут ассоциироваться с субъектами функционально или параметрически. Ввиду своей общности ФПАС ДП-модель, естественно, может не отражать всех существенных деталей КС из более узкого класса, в частности конкретных КС, и тем самым не обеспечивать возможной точности результата моделирования последних. Для ориентации общей модели на подкласс требуется прописать в ней все элементы КС в подклассе и все условия получения в них недоверенными субъектами прав доступа владения к доверенным субъектам. Именно так по ФПАС ДП-модели построена в [11] ДП-модель файловых систем КС с дискреционным управлением доступом, и именно так определяется здесь СДУ ДП-модель — путём определения в ФПАС ДП-модели, во-первых, тех элементов, которые присущи сетевым дискреционным КС с уязвимостями, и, во-вторых, тех условий применения в ней правила $know()$ для получения права доступа владения к субъекту, которые адекватны этому процессу в рассматриваемых КС.

1.1. Основные элементы СДУ ДП-модели

Определение 1. Под состоянием сетевой КС $\Sigma(G^*, OP)$ понимается граф доступов $G = (S, E, R \cup A \cup F, H)$, где

E — множество сущностей, в состав которого входят: $EC \subset E$ — подмножество сущностей-контейнеров (узлов, или компьютеров КС) и $IC \subset E$ — подмножество сущностей-интерфейсов (субъектов или объектов), в которые записывают данные одни субъекты, и из которых считывают данные другие субъекты, осуществляющие взаимодействие;

S — множество субъектов КС;

R — множество ребер графа-состояния G, соответствующих правам доступа пользователей к сущностям;

A — множество ребер графа-состояния G, соответствующих доступам пользователей к сущностям;

F — множество ребер графа-состояния G, соответствующих информационным потокам между сущностями;

H: $E \to 2^E$ — функция иерархии сущностей, ее значения на множестве сущностей соответствуют распределению сущностей по узлам КС, и каждая сущность $e \in E$ либо является узлом КС ($e \in EC$), либо размещена на некотором единственном для каждой сущности узле (для сущности e существует единственный узел $c \in EC$, такой, что $e < c$).

Для нарушения безопасности КС субъекты-нарушители используют, как правило, следующие уязвимости [12 – 15], приводящие к получению ими прав доступа владения к доверенным субъектам:

- пропущенные в системных функциях операционных систем (ОС), применяемых в узлах КС, механизмы проверки на наличие прав использования административных полномочий;
- ошибки в ПО (например, [16, 17]), реализующем прикладные и системные процессы ОС;
- отсутствие аутентификации и авторизации пользователей при доступах к ресурсам узлов КС (доверие);
- ошибки в реализации, конфигурировании и использовании КС, приводящие к реализации информационных потоков по памяти между нарушителем и субъектами КС;
- наличие информационных потоков по памяти от сущностей-паролей к субъектам-нарушителям;
- возможность получения или изменения некоторых параметров КС, позволяющих идентифицировать используемое на узлах системное и прикладное ПО, установленные обновления ОС и зарегистрированных в них пользователей.

Таким образом, будем исходить из следующего предположения.

Предположение. В каждом состоянии $G = (S, E, R \cup A \cup F, H)$ компьютерной системы $\Sigma(G^*, OP)$ выполняются следующие условия.

1. Для каждого узла $c \in EC$ определены доверенные пользователи, обладающие правом доступа владения к каждой сущности, размещенной на данном узле. Если пользователь $os_c \in S$ является доверенным пользователем узла $c \in EC$, то он обладает правом доступа владения к каждой сущности, размещенной на данном узле.

2. Множества I и EC не пересекаются. Множества E, S и функция H не изменяются на всех траекториях функционирования КС. Сущности-интерфейсы из IC используются как для передачи данных между субъектами одного узла, так и между субъектами разных узлов КС. В последнем случае управление доступом к таким интерфейсам может реализовываться КС межсетевого экранирования (МЭ). Дан-

ные сущности ассоциированы с субъектами, которые осуществляют к ним доступ на чтение.

3. Если субъект-пользователь $u \in S$ активизировал процесс $p \in S$, то последний наследует все права пользователя u и является функционально ассоциированным с ним. Если известно, что в некотором процессе $p \in S$ имеются ошибки, приводящие к утечке права доступа, то существует сущность-ошибка, функционально ассоциированная с данным процессом, т. е. существует сущность f в E, такая, что $f \in [p]$ и $(p, f, write_r) \in R$.

4. Существуют подмножества $U_L, S_L \subset S$, такие, что субъекты из U_L могут иметь права доступа к сущностям только на чтение, и если $s \in S_L$, то существуют один или несколько субъектов $u \in U_L$, таких, что $s \in]u[$.

5. Если сущность $p \in E$ является паролем, на основе которого субъекту-пользователю $u_1 \in S$, передавшему пароль через интерфейс $l \in IC$ процессу $r \in S$, последний предоставляет права доступа субъекта $u_2 \in S$ к другим сущностям КС, то $p \in [u_2]$, $p \in]u_2[$, $l \in (r)$, $(u_1, l, write_r) \in R$. Кроме того, если получение прав доступа пользователя u_1 позволяет получить права пользователя u_2, то $(u_1, u_2, own_r) \in R$.

Замечание 1. Из условия 3 следует, что в множество S при моделировании сетевой КС достаточно включить только субъектов-пользователей ее узлов. Для каждого субъекта-пользователя могут существовать несколько сущностей-интерфейсов из IC, в которые записывают и из которых считывают эти субъекты данные.

Замечание 2. Примерами субъектов из S_L в условии 4 являются сетевые службы NetBIOS, позволяющие получать доступ к чувствительной информации КС с правами анонимного пользователя $u \in U_L$ через нулевые сессии в ОС семейства Windows 2000/XP/2003/Vista [13].

Замечание 3. Примерами выполнения условия 5 являются возможность сквозной аутентификации пользователей на Citrix-сервере (аутентифицированный в домене пользователь при доступе к Citrix-серверу домена автоматически аутентифицируется на нем) и механизмы аутентификации служб rlogin, rsh и rexec в ОС семейства UNIX [13].

1.2. Правило *know*() в СДУ ДП-модели

По определению в ФПАС ДП-модели если сущность $z \in E$ параметрически ассоциирована с субъектом $y \in S$ в состоянии G, то чтение данных из z субъектом $x \in S$ позволяет ему получить право доступа владения к субъекту y в этом или последующих состояниях КС с помощью правила $know()$. В ДП-модели файловых систем [11] недоверенный субъект $x \in N_S$ может, применив правило преобразования состояний $know()$, получить право доступа владения к субъекту $y \in S$ тогда и только тогда, когда в КС реализованы информационные потоки по памяти к субъекту x от всех сущностей, параметрически ассоциированных с субъектом y.

В сетевых КС для получения субъектом-нарушителем x права владения к субъекту y ему, как правило, требуется получить доступ не только к сущности z, но и доступ на запись к некоторой сущности $l \in E$, являющейся интерфейсом или портом некоторого субъекта-процесса $r \in S$, осуществляющего предоставление x прав доступа y на основе данных в сущности l. При этом сущности z и l являются ассоциированными с субъектом r; сущности l и r, как правило, размещены на одном узле КС, а сущности z и y могут быть размещены на разных узлах КС. На рис. 1 изображен пример получе-

ния прав доступа субъекта y субъектом-нарушителем x, получившим доступ к паролю z и к интерфейсу l субъекта r. Здесь сущности z, y, r, l размещены на одном узле КС.

Например, для защиты от записи в сущность-интерфейс l субъекта r могут использоваться следующие механизмы защиты: группы доступа (ОС FreeBSD), фильтрация по IP-адресам узлов КС, с которых осуществляется доступ (механизм ACL, выделенные сети управления), и именам пользователей (служба SSH).

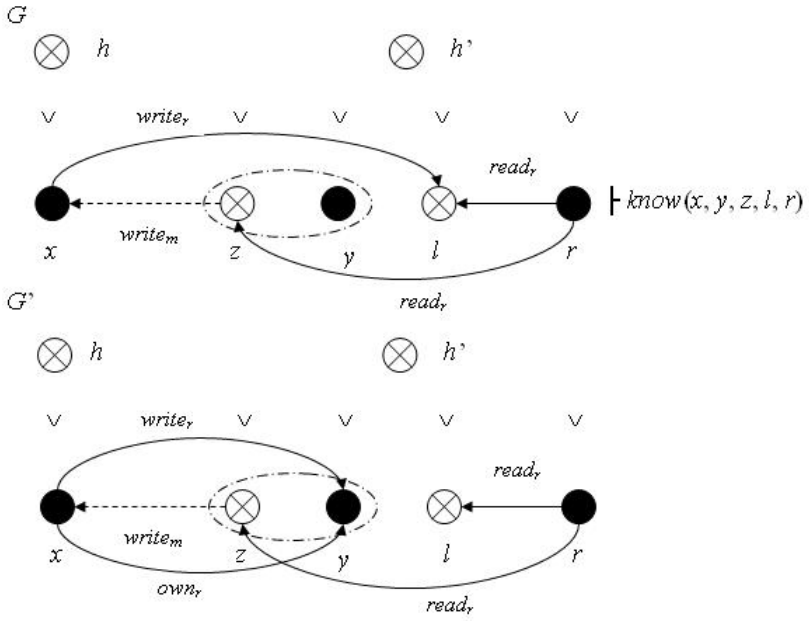

Рис. 1. Правило преобразования состояний $know(x, y, z, l, r)$ СДУ ДП-модели

Соответственно этому в ДП-модели сетевых КС правило $know()$ определяется формально, как показано в табл. 1.

Таблица 1

Условия и результаты применения правила *know(x, y, z, l, r)*

Правило	Исходное состояние $G = (S, E, R \cup A \cup F, H)$	Результирующее состояние $G' = (S', E', R' \cup A' \cup F', H')$
$know(x, y, z, l, r)$	$x, y, r \in S$, $l, z \in E$, $l \in (r)$, $(x, l, write_r) \in R$, $z \in]y[$ и или $x = z$, или $(z, x, write_m) \in F$	$S' = S$, $E' = E$, $A' = A$, $H' = H$, $F' = F$, $R' = R \cup (x, y, own_r)$

1.3. Определение СДУ ДП-модели

Определение 2. ДП-модель компьютерной системы $\Sigma(G^*, OP)$ с множеством правил преобразования состояний ФАС ДП-модели, заданных без учета использования информационных потоков по времени, и правилом преобразования $know()$, определенным в табл. 1, называется сетевой ДП-моделью с уязвимостями, или СДУ ДП-моделью, если её состояния подчиняются определению 1 и удовлетворяют условиям предположения в п. 1.1.

Таким образом, для моделирования безопасности сетевых КС с уязвимостями требуется модифицировать, как показано в табл. 1, условия применения правила преобразования $know()$ ФПАС ДП-модели и построить соответствующее уточнение последней по известной в теории ДП-моделей методике, а именно: в рамках модели сформулировать и обосновать условия возможности получения недоверенным субъектом права доступа владения к доверенному субъекту, скорректировать метод предотвращения получения недоверенным субъектом права доступа владения к доверенному субъекту, разработать алгоритмы построения замыкания графа доступов, графов распространения прав доступов и информационных потоков и сформулировать алгоритмы нахождения всех возможных путей нарушения безопасности. Это построение может быть осуществлено аналогично [7, 8, 18] и выходит за пределы данной статьи.

2. Построение СДУ ДП-модели для реальных КС

Для использования средств анализа безопасности сетевых КС с уязвимостями в рамках их ДП-моделей на практике необходимо представлять реальные КС их СДУ ДП-моделями. Эта задача решается следующим методом.

Метод. Пусть в КС идентифицированы узлы, открытые порты, ОС, сетевые службы, ПО, реализующее последние, и его уязвимости, а также пользователи. Пусть задана политика управления доступом и информационными потоками, реализованная в сетевой подсистеме КС.

Шаг 1. Описать множество EC узлов КС и определить функцию иерархии сущностей H. Для каждого узла КС определить одного доверенного субъекта-пользователя и множество недоверенных пользователей, от имени которых функционируют недоверенные процессы ОС этого узла. Включить пользователей в множество S.

Шаг 2. С помощью систем управления уязвимостями (сканеров безопасности) определить известные уязвимости процессов, запущенных на узлах КС, и наличие сетевых служб, использующих доверие и предоставляющих доступ к параметрам КС. В соответствии с этим определить функционально (найденные известные уязвимости) или параметрически (чувствительная информация) ассоциированные с субъектами-пользователями сущности.

Шаг 3. Описать множество файлов, в которых содержатся данные аутентификации субъектов-пользователей. Определить параметрически ассоциированные сущности с субъектами-пользователями, а также службы регистрации пользователей, удаленного управления и доступа и их интерфейсы в IC.

Шаг 4. Определить сущности-интерфейсы обмена данными между процессами узлов КС и права доступа к ним субъектов узлов КС, исходя из политики управления доступом и информационными потоками (права доступа, таблицы маршрутизации, списки ACL, правила МЭ и систем предотвращения атак). Включить такие сущности в множество IC и построить множество R.

Применение данного метода позволяет получить граф доступов начального состояния G_0 СДУ ДП-модели сетевой КС $\Sigma(G^*, OP)$ с уязвимостями.

3. Применение СДУ ДП-модели

СДУ ДП-модель может быть использована в задачах построения и анализа возможных путей нарушения безопасности КС, а также для представлении известных моделей формального описания и верификации политик безопасности КС и моделей анализа графов атак с целью алгоритмической проверки условий нарушения безопасности в них.

3.1. Построение путей нарушения безопасности КС

Граф доступов G', полученный из графа доступов G ДП-модели КС применением правил преобразования состояний этой ДП-модели, называется замыканием графа доступов G, если применение к графу G' данных правил не приводит к появлению в нем новых ребер.

Пусть требуется построить все пути нарушения безопасности, т. е. все последовательности, состоящие из ребер графа начального состояния и правил преобразования состояний, описывающие переход КС из начального состояний G_0 в некоторое состояние G, в котором нарушена безопасность КС. Для этого следует аналогично [18] построить замыкание графа доступов СДУ ДП-модели, в котором по определению содержатся все запрещенные доступы или информационные потоки, а затем по нему построить граф распространения прав доступов и информационных потоков, что позволит найти все возможные пути данного нарушения безопасности КС в рамках ее модели.

3.2. Разработка и обоснование условий и метода предотвращения возможности получения права доступа владения

В рамках построенной СДУ ДП-модели аналогично [7, 8] могут быть установлены и обоснованы необходимые и достаточные условия возможности получения недоверенным субъектом права доступа владения к доверенному субъекту КС. Затем на основе этих условий можно аналогично методу 4.1 из [6] разработать и теоретически обосновать метод предотвращения в КС такой возможности. Результатом применения этого метода к некоторой КС является КС $\Sigma(G^*, OP, G_0)$, в которой для каждого недоверенного субъекта $x \in N_S \cap S_0$ и доверенного субъекта $y \in L_S \cap S_0$ предикат $can\_share\_own(x, y, G_0, L_S)$ является ложным, что как раз и означает невозможность получения в КС недоверенным субъектом права доступа владения к доверенному субъекту.

3.3. Погружение других моделей в СДУ ДП-модель

Как правило, известные модели КС, ориентированные на поиск возможных путей нарушения их безопасности, не являются субъектно-объектными, поэтому их правила преобразования состояний описываются на языке с высоким уровнем абстракции (например, язык модели абстрактных классов [3]), что требует большого числа правил описания уязвимостей КС. ДП-модели относятся к классу субъектно-объектных моделей. В них все вопросы безопасности (в соответствии с основной аксиомой теории компьютерной безопасности) описываются доступами субъектов к объектам КС, что позволяет моделировать известные уязвимости КС для анализа их безопасности с помощью небольшого числа правил. Основные известные модели, используемые на практике для построения возможных путей нарушения безопасности КС (например, модель REM [1] и расширение [2] модели Take-Grant для КС с уязвимостями (VTG-модель)), могут быть представлены в рамках СДУ ДП-модели.

Покажем возможность представления VTG-модели в рамках разработанной СДУ ДП-модели. Опишем основные положения модели VTG:

- каждому узлу КС соответствует некоторое множество известных уязвимостей;
- дополнительно к стандартным видам прав доступа модели Take-Grant добавлены следующие виды прав доступа: h — принадлежности сущности к узлу, x — выполнения, o — владения;
- наличие уязвимостей в сущностях обозначается с помощью метки последних;

— рассматриваются три класса уязвимостей: переполнение буфера в сегменте стека, доступ к паролям, отношение доверия между сущностями КС;
— возможность использования уязвимостей отражается в новых правилах преобразования состояний $bof\_rule()$, $pc\_rule()$ и $rt\_rule()$ соответственно;
— для проверки возможности получения субъектом x права доступа к сущности y вводится предикат $can\_access(\alpha, x, y, VTG_0)$, истинность которого проверяется путем построения замыкания графа доступов.

Для представления VTG-модели в рамках СДУ ДП-модели следует:

— по уязвимостям КС в первой из них определить ассоциированные, функционально или параметрически ассоциированные с субъектами сущности и права доступа к ним, как в условиях 3 и 5 предположения;
— пометить ребра, используемые в отношении доверия между сущностями, правом own_r;
— вместо прав доступа r, w и x использовать права доступа $read_r$, $write_r$, $execute_r$ соответственно;
— вместо видов прав доступа t, g и o использовать право доступа own_r;
— вместо права h определить функцию H (дуге графа доступов VTG-модели из вершины x в вершину y, помеченной правом h, соответствует отношение $y < x$ в ДП-модели);
— вместо правил $bof\_rule()$ и $pc\_rule()$ использовать правила преобразования $control()$ и $know()$ ФПАС ДП-модели.

Тем самым VTG-модель может быть погружена в СДУ ДП-модель. Возможность представления модели REM [1], реализованной в сканере безопасности NetSPA, в рамках СДУ ДП-модели показывается аналогично в [18].

Таким образом, представление моделей безопасности КС, ориентированных на построение возможных путей нарушения их безопасности, действительно возможно в рамках семейства ДП-моделей с дискреционным управлением доступом.

Заключение

Данное исследование позволяет сделать следующий вывод: семейство ДП-моделей может быть использовано для моделирования сетевых КС с уязвимостями, связанными с ошибками в ПО, с доверием субъектов, с доступом к паролям субъектов и раскрытием параметров КС, для построения всех возможных путей нарушения их безопасности, алгоритмической проверки условий получения недоверенным субъектом прав доступа доверенного субъекта и предотвращения возможности этого как непосредственно в рамках предложенной СДУ ДП-модели, так и посредством представления в ней других моделей безопасности сетевых КС с уязвимостями (например, REM и VTG).

ЛИТЕРАТУРА

1. *Artz M.* NETspa, A Network Security Planning Architecture: M.S. Thesis; Cambridge: Massachusetts Institute of Technology, 2002.
2. *Shahriary H. R., et al.* Network Vulnerability Analysis Thorough Vulnerability Take-Grant Model // Proc. of 7th International Conference on Information and Communications Security. 2005.
3. *Danforth M.* Models for Threat Assessment in Networks: Ph.D. dissertation; Davis: University of California, 2006.

4. *Jajodia S.* Topological Analysis of Network Attack Vulnerability // Managing Cyber Threats: Issues, Approaches and Challenges, 2003.
5. *Sheyner O.* Scenario Graphs and Attack Graphs: Ph.D. dissertation; Carnegie Mellon University. Pittsburgh, 2004.
6. *Девянин П. Н.* Анализ безопасности управления доступом и информационными потоками в компьютерных системах. М.: Радио и связь, 2006. 176 с.
7. *Колегов Д. Н.* ДП-модель компьютерной системы с функционально и параметрически ассоциированными с субъектами сущностями // Вестник Сибирского государственного аэрокосмического университета имени академика М. Ф. Решетнева. 2009. Вып. 1(22). Часть 1. С. 49–54.
8. *Колегов Д. Н.* Анализ безопасности информационных потоков по памяти в компьютерных системах с функционально и параметрически ассоциированными сущностями // Прикладная дискретная математика. 2009. № 1(3). С. 117–126.
9. *Souppaya M. et al.* Technical Guide to Information Security Testing and Assessment. Recommendations of the National Institute of Standards and Technology. 2008.
10. ФСТЭК России. Руководящий документ. Безопасность информационных технологий. Концепция оценки соответствия автоматизированных систем требованиям безопасности информации. М., 2004.
11. *Буренин П. В.* Подходы к построению ДП-модели файловых систем // Прикладная дискретная математика. 2009. № 1(3). С. 93–113.
12. *Касперский К.* Техника сетевых атак. Т. 1: Приемы противодействия. М.: СОЛОН-пресс, 2001. 400 с.
13. *Козиол Дж., Личфилд Д., Эйтэл Д. и др.* Искусство взлома и защиты систем. СПб.: Питер, 2006. 416 с.
14. *Проскурин В. Г., Крутов С. В., Мацкевич И. В.* Защита в операционных системах: Учеб. пособие для вузов. М.: Радио и связь, 2000. 168 с.
15. *McNab C.* Network Security Assessment, second edition. ISBN-10:0-596-51030-6, 2007. 478 p.
16. База уязвимостей SecurityFocus [Электронный ресурс]. Режим доступа: http://www.securityfocus.com/bid.
17. База уязвимостей NVD [Электронный ресурс]. Режим доступа: http://nvd.nist.gov.
18. *Колегов Д. Н.* Применение ДП-моделей для анализа защищенности сетей // Прикладная дискретная математика. 2008. № 1. С. 71–88.