**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
ФГБОУ ВО «ТВЕРСКОЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ
СПЕЦИАЛЬНОСТЬ «КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ»**

**КАФЕДРА КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ И МАТЕМАТИЧЕСКИХ МЕТОДОВ УПРАВЛЕНИЯ**

**КУРСОВАЯ РАБОТА**

 по дисциплине: «Модели безопасности компьютерных систем»
на тему: «Автоматная модель безопасности информационных потоков»

 Выполнила:

 студентка 4 курса, группа м-44

 Федорова С.О.

 Научный руководитель:

 к. ф.–м. н., доц.

 Семыкина Н.А.

г. Тверь 2017 г.

**Содержание**

1. Введение…………………………………………………………….…3-4
2. Описание модели………………………………………………….......5-7
3. Критерий безопасности…………………………………………….....8
4. Положительные и отрицательные стороны модели………………...9
5. Примеры………………………………………………………………..10
6. Заключение………………………………………………………….....11
7. Список литературы…………………………………………………....12

**1.Введение**

Одной из, пожалуй, самых трудно решаемых проблем безопасности в КС является проблема скрытых каналов утечки информации.

**Определение 1.1**. Скрытым каналом утечки информации называется механизм, посредством которого в КС может осуществляться информационный поток (передача информации) между сущностями в обход политики (правил) разграничения доступа.

Теоретические основы подходов к решению проблемы скрытых каналов базируются на работах Д. Денинга, исследовавшего принципы анализа потоков данных в программном обеспечении и принципы контроля совместно используемых ресурсов. Отталкиваясь от идей Денинга Дж. Гогеном, Дж. Мезигером был предложен автоматный подход к исследованию вопросов скрытых каналов, относящийся к интерфейсу защищенных КС.

Другой подход к анализу скрытых каналов утечки информации базируется на теоретико-информационной интерпретации процессов функционирования КС в идеологии информационной не выводимости и информационного невмешательства.

Идеи информационной не выводимости и информационного невмешательства послужили теоретической основой широко применяемых для разграничения доступа в современных КС технологий "представлений" (views) и "разрешенных процедур". Эти технологии исторически возникли как программно-технологические решения разграничения доступа в СУБД и впоследствии получили распространение на другие разновидности программного обеспечения компьютерных систем.

Техника "представлений", хотя и является эффективным средством решения проблемы скрытых каналов утечки информации, тем не менее, не может перекрыть весь их спектр, в особенности, скрытые каналы второго и третьего вида, основывающиеся на анализе временных и статистических параметров процессов КС.

Часть из подобных проблем разграничения доступа связана с интерфейсом КС, а их разрешение основывается на технике "разрешенных процедур".

**Определение 1.2**. "Системой разрешенных процедур" назовем разновидность интерфейса КС, когда при входе в систему аутентифицированным пользователям предоставляется только лишь возможность запуска и исполнения конечного набора логико- технологических процедур обработки информации без возможности применения элементарных методов доступа (read, write, append, create, delete и т. п.) к информационным объектам системы.

Таким образом, в системах с интерфейсом "разрешенных процедур" идеология разграничения доступа доведена, если так можно выразиться, до крайности, т. е. пользователи не "видят" информационные объекты системы вовсе, а имеют возможность только лишь "нажимать кнопки" и выполнять операции на уровне логико-технологических процедур предметной области КС.

Нетрудно заметить, что компьютерная система при этом для пользователей превращается в дискретный автомат, получающий команды на входе и выдающий обработанную информацию на выходе.

Впервые подобный подход к представлению КС был рассмотрен Гогеном (J. Goguen) и Мезигером (J. Meseguer), предложившими автоматную модель информационного не влияния (невмешательства).

Целью данной работы является исследование автоматной модели безопасности информационных потоков.

**2.Описание модели**

В автоматной модели безопасности информационных потоков система защиты представляется детерминированным автоматом, на вход которого поступает последовательность команд пользователей.

**Определение 2.1.** Автоматом А называется совокупность пяти элементов:

- конечный входной алфавит;

 - конечное множество состояний;

 - конечный выходной алфавит;

 - функция переходов автомата;

 - функция выходов автомата.

 Начнем с простейшего случая системы с «фиксированной» защитой. Пусть V – множество состояний системы (V – конечное и определяется программами, данными, сообщениями и пр.), C – множество команд, которые могут вызывать изменения состояния (также конечное множество), S – множество пользователей (конечное множество). Смена состояний определяется функцией:

do:.

Некоторые действия пользователей могут не разрешаться системой. Вся информация о том, что разрешено пользователям сведена в с-таблицу t. В рассматриваемом случае «возможности» в с-таблице t совпадают с матрицей доступа. Если пользователь не может осуществить некоторую команду с, то

do (v, S, c) = v.

 Предположим, что для каждого пользователя S и состояния v определено, что «выдается» этому пользователю (что он видит) на выходе системы. Выход определяется функцией

out: Out,

где Out – множество всех возможных выходов.

Таким образом получили определение некоторого класса автоматов.

**Определение 2.2.** Автомат М состоит из множеств:

 S – называемых пользователями;

 V – называемых состояниями;

 C – называемых командами;

 Out – называемых выходами;

и функций:

* выходной функции​ *out*:*Out*, которая «говорит, что данный пользователь видит, когда автомат находится в данном состоянии»;
* функции переходов *do: *, которая «говорит, как изменяется состояние автомата под действием команд»;

и начального состояния .

Системы с изменяющимися «возможностями» защиты определяются следующими образами.

Пусть Capt – множество всех таблиц «возможностей», СС – множество с-команд (команд управления «возможностями»). Их эффект описывается функцией:

cdo: **.**

При отсутствии у пользователя S права на с-команду положим cdo (t, s, c) = t. Пусть VC – множество команд, изменяющих состояние. Теперь можем определить С-автомат.

**Определение 2.3.** С-автомат М определяется множествами:

S **–** «пользователи»;

V **–** «состояния»;

VC **–** «команды состояния»;

Out **–** «выходы»;

Capt **–** «с-таблицы»;

CC **–** «с-команды»;

и функциями:

* выхода out:  Out, которая «говорит, что данный пользователь видит, когда автомат находится в данном состоянии v, а допуски определяются с-таблицей»;
* переходов do: , которая «говорит, как меняются состояния под действием команд»;
* изменения с-таблиц cdo: , которая «говорит, как меняется с – таблица под действием с»,

и начального состояния, которое определяется с-таблицей t и состоянием v.

То, что мы определили на языке теории автоматов­, называется последовательным соединением автоматов.

**3.Критерий безопасности**

Введем понятие информационного влияния одной группы на другую, смысл которого состоит в том, что, используя некоторые возможности одна группа пользователей не влияет на то, что видит каждый пользователь другой группы. Для этого определим [[W]]*s*– выход для S при выполнении входного слова W С-автомата М:

[[W]]*s* = out ([[W]], S),

где

Out ([[W]]*s*, S) = (… out(v, t, s)…),

[[W]]= (…, (vi, ti), …).

Пусть GS – подмножество множества пользователей, AC – подмножество множества команд, W \* - последовательность команд пользователей.

**Определение 3.1**. Pg (W) - последовательность W, получающаяся выбрасыванием всех пар (S, c) при SG, PА(W) - последовательность W, получающаяся выбрасыванием из W всех пар (S, c) при сА, PGA(W) - последовательность W, получающаяся выбрасыванием пар (S, c), SG и сА.

**Определение 3.2.** Пусть GS, G’S. G информационно не влияет на G’,обозначается G: | G’, если

 W\* и  S G’ [[W]]*s* = [[PG(W)]]*s*

**Определение 3.3.** А информационно не влияет на G,обозначается А: | G, если

 W\* и  S G[[W]]*s* = [[PА(W)]]*s*

**Определение 3.4.** Пользователи G, используя возможности АБ информационно не влияют на G’, обозначается G,A: | G’, если

 W\* и  S G’ [[W]]*s* = [[PGA(W)]]*s*

**Определение 3.5.** Политика безопасности в автоматной модели безопасности информационных потоков – это набор требований информационного не влияния.

**4.Положительные и отрицательные стороны модели**

Выявим **положительные** стороны модели:

* Модель проста и понятна для понимания и реализации;
* Является эффективной в управлении (в зависимости от команды пользователя на входе КС-автомат формирует реакцию – вывод системы, который "видит" пользователь на выходе).
* В данной модели при переходе системы из одного разрешенного состояния в другое используются транзакции, что обеспечивает общую целостность системы.

**Недостатки:**

При проектировании систем с подобной идеологией интерфейса необходимо рассмотреть все множество условий и спецификаций, имеющих отношение к возможному смешиванию вводов/выводов пользователей, и верифицировать на этой основе безопасность системы.

**5.Примеры**

**Пример 1.** Пусть *f*⎯ файл, *s*∈ *U*⎯ пользователь, *A*= {*create*(*f*), *write*(*f*), *modify*(*f*), *delete*(*f*)} ⎯ набор команд. Тогда {*s*}, *A*:| {*s*}, означает, что пользователь *s*может осуществлять только чтение из файла *f*.

**Пример 2.**  Если А: | {S}, то команды из А не влияют на выход, выданный S. Если А = {create, write, modify, deleted} для файла F, то А: | {S} означает, что информация, читаемая S в F не может измениться любой из команд в А. Если F не существовал, то для S будет всегда выдаваться информация, что F не существует.

**Пример 3.** Мандатную политику безопасности в автоматной модели безопасности информационных потоков, которая состоит в том, что пользователи с большим уровнем доступа не должны информационно влиять на пользователей с меньшим уровнем доступа, можно выразить следующим образом.

Используем обозначения:

(*L*, ≤) ⎯ шкала уровней доступа к информации;

*level*: *U*→ *L*⎯ функция уровней доступа пользователей;

*U*[– ∞, *x*] = {*s*∈ *U*: *level*(*s*) ≤ *x*} ⎯ множество пользователей с уровнем доступа не большим *x*∈ *L*;

*U*[*x*, + ∞] = {*s*∈ *U*: *level*(*s*) ≥ *x*} ⎯ множество пользователей с уровнем доступа не меньшим *x*∈ *L*.

Тогда мандатная политика безопасности есть совокупность требований информационного невлияния:

для *x*, *x*’∈ *L*, *x*< *x*’выполняется *U*[*x*’, + ∞] :| *U*[– ∞, *x*].

**6.Заключение**

 Мы рассмотрели одну из моделей политики безопасности информационных потоков – автоматную модель безопасности информационных потоков, как она работает, её положительные и отрицательные стороны. В заключении отметим, несмотря на недостатки этой модели, она очень важна и значима, поскольку на её основе построена большая часть всех современных систем безопасности.

**7.Список литературы**

1. П. Н. Девянин, Обзорные лекции по моделям безопасности компьютерных систем, Институт криптографии, связи и информатики, г. Москва, Россия, 2009.
2. Грушо А.А.,Тимонина Е.Е. Теоретические основы защиты информации. М.:Яхтсмен, 1996. - 192с.
3. Гайдамакин Н.А. Разграничение доступа к информации в компьютерных системах. - Екатеринбург: изд-во Урал. Ун-та, 2003. – 328 с.