УДК 519.7+681.3

©2010. **В.В. Скобелев**

АНАЛИЗ МОДЕЛЕЙ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ

Данная работа представляет собой обзор по теории компьютерной безопасности. В ней дан ретроспективный анализ моделей, оказавших основное влияние на развитие этой теории. Охарактеризован класс ДП-моделей, проработке которого уделяется значительное внимание в последнее время, и который предоставляет унифицированные средства преодоления целого комплекса уязвимостей современных сетевых компьютерных систем. Указан ряд задач, связанных с обеспечением взаимодействия формальных моделей безопасности компьютерных систем с криптосистемой.

Ключевые слова: *модели безопасности, компьютерные системы, ДП-модели*

1. Введение. В 70-х годах XX столетия систематическое применение компьютеров для совместного использования, а также появление компьютерных сетей выдвинули в число одной из наиболее актуальных проблему обеспечения корректной работы с большой базой данных, к которой различные субъекты имеют различный доступ.

Формальной основой для представления состояния компьютерной системы (КС) в каждый момент $t \in \mathbf{Z}_+$ является динамическая система $\mathcal{S}_t = (S_t, O_t, R_t)$, где конечные множества S_t и O_t, представляют, соответственно, субъекты (их, как правило, отождествляют с процессами, представляющими пользователей) и объекты (т.е. сущности, доступ к которым контролируется), а R_t – множество таких бинарных отношений $\rho_t^{(i)} \subseteq S_t \times O_t$ $(i = 1, \ldots, n)$, что $\rho_t^{(i)}$ определяет i-й вид доступа субъектов к объектам (в общем случае множество видов доступа представляет собой решетку $(L, \leq)$ $(|L| = n)$, т.е. частично упорядоченное множество, в котором для любых двух элементов существуют наименьшая верхняя грань и наибольшая нижняя грань).

В рамках построения той или иной алгебраической системы на основе динамической системы $\mathcal{S}_t$ $(t \in \mathbf{Z}_+)$ и решаются две основные задачи: моделирование условий передачи прав доступа в КС и реализация информационных потоков в КС. Именно на основе такого подхода в 70-х – 80-х годах XX столетия был разработан ряд формальных моделей безопасности КС.

Цель настоящей работы – анализ существующих моделей безопасности КС.

2. Ретроспективный анализ. Одной из первых моделей, предназначенных для анализа условий безопасности передачи прав доступа в КС, является модель HRU [35]. В ней множеством состояний является множество матриц доступов (субъектов к объектам), а переход из текущего состояния в следующее осуществляется с помощью команд, каждая из которых определяется множеством параметров, условием ее выполнения и конечной последовательностью примитивных операций, преобразующих матрицу доступов.

Начальное состояние называется безопасным относительно права доступа r, если

из него невозможен переход в состояние, в котором r появилось в ячейке матрицы доступов, до этого r не содержавшей. Доказано, что задача проверки безопасности начального состояния относительно данного права алгоритмически неразрешима для HRU с командами общего вида и алгоритмически разрешима для HRU с командами специального вида: моно-моделей (каждая команда состоит из одной операции) и монотонных моделей (в командах отсутствуют опереции delete и destroy). В [36] показано, что проверка безопасности начального состояния для некоторых классов HRU имеет линейную сложность.

В HRU впервые использовалось дискреционное управление доступом (DAC), состоящее в том, что доступ субъектов к объектам осуществляется исключительно на основе матрицы доступов. В результате детализации HRU за счет выделения типов субъектов и объектов появился класс моделей TMD [40].

Для разработки алгоритмов управления доступом на основе HRU были разработаны DAC-модели ADEPT-50 и H [25].

В ADEPT-50 множество уровней безопасности линейно-упорядочено и выделено 4 типа объектов: пользователи, задания, терминалы и файлы. Состояние каждого объекта o представлено набором $A(o) \times C(o) \times F(o) \times M(o)$, где $A(o)$ – уровень безопасности объекта o, $C(o)$ – множество рубрик, характеризующих свойства объекта o, не зависящие от его уровня секретности (например, «только для просмотра»), $F(o)$ – множество пользователей, имеющих доступ к объекту o, а $M(o)$ – множество видов доступа к объекту o. Управление доступом пользователя u для выполнения задания j осуществляется следующим образом. Пользователь u получает доступ: 1) к КС тогда и только тогда, когда $u \in U$ (U – множество всех пользователей КС); 2) к терминалу t тогда и только тогда, когда $u \in F(t)$; 3) к файлу f тогда и только тогда $u \in F(f)$, $A(j) \geq A(f)$, $C(j) \supseteq C(f)$ и $M(j) \supseteq M(f)$. Таким образом, в ADEPT-50 впервые реализовано унифицированное управление доступом (на основе прав задания, а не пользователя) над неоднородными множествами данных и программ, файлов, пользователей и терминалов.

В модели H область безопасности – подмножество множества $A \times U \times E \times R \times S$, где A – множество установленных полномочий, U – множество пользователей, E – множество операций, R – множество ресурсов, а S – множество состояний. Запрос на доступ имеет вид $q = (u, e, r, s)$ ($u \in U, e \in E, r \subseteq R, s \in S$). Для групп пользователей U', требующих ресурс r' ($r' \subseteq R$), обработка каждого запроса $q = (u, e, r, s)$ осуществляется (посредством теоретико-множественных операций) следующим образом: 1) строится множество $F(u)$ полномочий для u, множество полномочий $F(e)$ для e и множество полномочий $F(r)$ для $r' \cap r$; 2) строится домен полномочий запроса $D(q) = F(u) \cap F(e)F(r)$; 3) если полномочия ресурса r не содержатся в $D(q)$, то выдается отказ на запрос q, иначе строится фактическая привилегия $F(u, q)$ пользователя u для запроса q, т.е. разбиение множества $D(q)$, где полномочия попадают в один блок тогда и только тогда, когда они определяют одну и ту же единицу ресурса; 3) если $F(u, q)$ покрывает r, то доступ разрешается, в противном случае – отказ на запрос q.

Для формального анализа безопасности передачи прав в DAC-моделях была по-

строена модель TG [32,34]. В ней КС представлена размеченным орграфом, вершины которого соответствуют объектам и субъектам, а отметки дуг отражают операции над правами (брать, давать, создать, убрать). Интерес к модели TG существенно возрос с появлением распределенных КС. Эта модель реализована в ОС E1.

Безусловное достоинство рассмотренных выше DAC-моделей – простота их реализации. Основные недостатки – возможность неосознанной или осознанной передачи прав доступа нарушителю (так как любой пользователь самостоятельно определяет передачу прав доступа) и полная незащищенность от троянских программ (они используют скрытые от пользователя управляемые ОС операции, с помощью которых организуется утечка информации нарушителю).

В модели BL [29,30,38], построенной в процессе разработки ОС Multics и частично реализованной в ней, впервые использовалось мандатное управление доступом (MAC). В BL следующим образом реализован принцип: пользователи имеют право читать только документы, уровень секретности которых не превышают уровень их допуска, и не могут создавать документы ниже своего уровня допуска. Пусть S и O – множество, соответственно, субъектов и объектов, L – решетка уровней безопасности, а V – множество состояний, т.е. пар (f, M), где $f : S \cup O \to L$ – функция, определяющая уровни безопасности в данном состоянии, а M – матрица доступа субъектов к объектам. КС представляется начальным состоянием $v_0 \in V$ и функцией переходов $\delta : V \times R \to V$ (R – множество запросов). Состояние (f, M) называется безопасным по чтению (по записи), если из того, что для всех $s \in S$ и $o \in O$ чтение (запись) принадлежит $M[s, o]$, следует, что $f(s) \geq f(o)$. Состояние (f, M) называется безопасным, если оно безопасно и по чтению, и по записи. Модель называется безопасной, если при безопасном начальном состоянии после выполнения любой конечной последовательности запросов она переходит в безопасное состояние. Для BL в терминах функции переходов δ определен язык безопасных последовательностей запросов. Переход из состояния (f, M) в состояние (f^*, M^*) является безопасным тогда и только тогда, когда для всех $s \in S$ и $o \in O$ выполнены следующие условия: 1) если чтение принадлежит $M^*[s, o]$ и не принадлежит $M[s, o]$, то $f^*(s) \geq f^*(o)$; 2) если чтение принадлежит $M[s, o]$ и $f^*(s) < f^*(o)$, то чтение не принадлежит $M^*[s, o]$; 3) если запись принадлежит $M^*[s, o]$ и не принадлежит $M[s, o]$, то $f^*(o) \geq f^*(s)$; 4) если запись принадлежит $M[s, o]$ и $f^*(o) < f^*(s)$, то запись не принадлежит $M^*[s, o]$.

Для контроля целостности информации в различных вариантах BL была построена модель B [31].

Безусловное достоинство BL – простота ее реализации, а основные недостатки состоят в следующем: 1) обеспечение конфиденциальности осуществляется в ущерб эффективности; 2) не проработаны задачи повышения уровня секретности совокупности данных по сравнению с уровнями секретности отдельных компонент и понижения уровня секретности отдельных компонент данных по сравнению с уровнем секретности этих данных, а также задача рассекречивания информации; 3) не проработаны ситуации, когда пользователи должны работать с данными, которые они не должны видеть; 4) в распределенных КС запрос на удаленное чтение вызывает протекание потоков информации в обоих направлениях между компонентами, что

является нарушением безопасности для BL; 5) процессы, действующие в интересах администраторов КС, не могут управляться BL. Формальный анализ недостатков BL осуществлен в терминах системы L [39], представляющей собой алгебру различных вариантов BL, определяемых возможностями изменения субъектами своей классификации.

В модели MMS [37] каждый сеанс пользователя начинается с процедуры login, состоящей в том, что он представляет свой идентификатор. Если аутентификация прошла успешно, то пользователь осуществляет запрос на операции с объектами или контейнерами (иерархическими структурами объектов). Допустимые для пользователя операции зависят от его идентификатора и роли. Таким образом, в MMS впервые использовалось ролевое управление доступом (RAC).

В основе MMS лежат следующие предположения безопасности. Офицер безопасности присваивает уровни доверия и роли пользователям и осуществляет классификацию устройств, а пользователь: 1) корректно классифицирует информацию при ее изменении; 2) так классифицирует создаваемые им сущности (т.е. объекты или контейнеры), что только пользователь с требуемой благонадежностью может иметь доступ к этой информации; 3) должным образом контролирует информацию объектов, требующих благонадежности.

В MMS ограничения безопасности поддерживаются непосредственно КС и состоят в следующем. Пользователь может получить доступ к операции над сущностями, только если его идентификатор или его текущая роль присутствуют во множестве доступов к этой сущности вместе с этой операцией. Информация, переносимая из объекта, всегда наследует классификацию этого объекта, а вставляемая в объект информация всегда должна иметь классификацию ниже классификации объекта (таким образом, классификация контейнера всегда не ниже классификации содержащихся в нем сущностей). Пользовать может просматривать только сущности, классификация которых не превосходит степени доверия к нему. Сущности, просмотренные пользователем, помечаются его степенью доверия. Понижение уровня классификации информации или уничтожение информации могут осуществляться только офицером безопасности или пользователями, обладающими соответствующими ролями.

На основе анализа MMS в [33] предложена модель CW, предназначенная для обеспечения безопасти автоматизированных бухгалтерских операций и осуществляющая контроль целостности информации в КС.

Несмотря на неоспоримые достоинства, в MMS возможно наличие скрытых каналов утечки информации. Для их выявления в 80-х годах XX столетия были разработаны принципы анализа в КС информационных потоков и контроля совместно используемых ресурсов.

Рассмотренные выше модели и определили основные направления развития теории компьютерной безопасности. При этом определяющими оказались следующие два фактора.

Во-первых, любая модель безопасности КС представляет собой машину состояний, анализ которой осуществляется на основе моделей и методов дискретной мате-

матики, математической логики и современной алгебры с использованием программных систем автоматического доказательства теорем.

Во-вторых, средства обеспечения компьютерной безопасности образуют ядро, реализующее концепцию монитора обращений, и должны быть встроены в КС на уровне ОС (возможно, частично, на аппаратном уровне).

Следует отметить, что отсутствие глубокой проработки концепции ядра приводит к его «разбуханию» при переходе к новым модификациям ОС. Ярким таким примером является семейство ОС Windows [1].

В настоящее время при построении моделей безопасности КС, как дополнительное средство, используются информационные и вероятностные модели безопасности.

Информационная модель применяется для реализации ограничений на ввод/вывод в КС через интерфейс программных модулей. Выделяют модели невмешательства (в них ввод высокоуровневого пользователя не может смешиваться с выводом низкоуровневого пользователя) и модели невыводимости (в них информационные потоки за счет специальных трассировок организованы так, что наличие или отсутствие высокоуровневых пользователей не изменяет информацию о КС, которую могут получить низкоуровневые пользователи).

Вероятностная модель применяется для исследования вероятности преодоления модели безопасности за определенное время. Выделяют игровые модели (при каждом преодолении модели безопасности строится ее модификация, устойчивая к этой атаке, т.е. реализуется процесс эволюции модели безопасности) и модели с полным перекрытием (в них реализуется, по крайней мере, одно средство для обеспечения безопасности на каждом возможном пути проникновения в КС). Примером применения вероятностной модели при построении реальной системы безопасности КС является разработка системы безопасности MS-DOS.

Современное состояние теории компьютерной безопасности систематически изложено в [3,5,15,24,25,27,28], а анализ различных проблем, связанных с разработкой современных политик безопасности КС, представлен в [4,8,10,12,17,21,26].

3. ДП-модели безопасности КС. В последнее время значительное внимание уделяется исследованию класса ДП-моделей безопасности КС [2], построенному на основе моделей BL, TG и MMS.

Базовая ДП-модель [6] – это представленная в виде размеченного орграфа система $G = (E, S, R \cup A \cup F, H)$, где $E = O \cup C$ $(O \cap C = \emptyset)$ – множество сущностей, представляющее вершины орграфа (O и C – соответственно, множество объектов и контейнеров), $S \subseteq E$ – множество субъектов, $R \subseteq S \times E \times R_r$, $A \subseteq S \times E \times R_a$ и $F \subseteq S \times E \times R_f$ – множества размеченных дуг, соответствующих правам доступа субъектов к сущностям, доступам субъектов к сущностям и информационным потокам между сущностями (R_r – множество видов прав доступа, R_a – множество видов доступа, а R_f – множество видов информационных потоков (по памяти и по времени)), а $H : E \to 2^E$ – функция иерархии сущностей, определяющая для каждого $c \in C$ множество сущностей $H(c) \subseteq E$, непосредственно содержащихся в контейнере c. В [6] построены правила преобразования системы G и установлены критерии, при которых возможна передача прав от одного субъекта к другому при

условии, что в КС не выделены доверенные субъекты, но все субъекты действуют в кооперации друг с другом. В [9] предложен метод предотвращения реализации в базовой ДП-модели запрещенных информационных потоков по времени.

В [7] базовая ДП-модель детализирована для случая, когда сущности функционально ассоциированы с субъектами (т.е. данные сущности влияют на вид преобразований, которые в данном состоянии субъект может осуществить с этой сущностью). В такой модели для каждого состояния с помощью функции $f_s : S \to L$ определяется уровень доступа каждого субъекта, а с помощью функции $f_e : E \backslash S \to L$ – уровень конфиденциальности каждой сущности, не являющейся субъектом. Показано, что при такой модели безопасности недоверенные субъекты, используя информационные потоки по памяти, могут получать контроль над доверенными субъектами КС. Предотвращение такой ситуации обеспечивается с помощью специальных средств администрирования и управления доступом в КС. В [16,20] исследована ДП-модель,в которой кроме функционально ассоциированных сущностей допускаются и параметрически ассоциированные сущности.

В [11] построена ролевая ДП-модель. Для этого в базовую ДП-модель добавлено множество пользователей U, разбитое на множества L_U доверенных и N_U недоверенных пользователей, множество S субъект-сессий, разбитое на множества L_S доверенных и N_S недоверенных сессий, множество $\mathtt{R}$ ролей, множество $\mathtt{R}_A$ административных ролей, множество $\mathtt{P} \subseteq E \times R_r$ прав доступа к сущностям, функция $f_{\mathtt{R}} : U \to 2^{\mathtt{R}}$ авторизованных ролей пользователей, функция $f_{\mathtt{R}_A} : U \to 2^{\mathtt{R}_A}$ авторизованных административных ролей пользователей, функция $g_{\mathtt{P}} : \mathtt{R} \to 2^{\mathtt{P}}$ прав доступа ролей, функция $h_u : S \to U$ принадлежности субъект сессии пользователю, функция $h_r : S \to 2^{\mathtt{R}} \cup 2^{\mathtt{R}_A}$ текущих ролей субъект сессии и функция $h_{cmr} : \mathtt{R}_A \to 2^{\mathtt{R}}$ администрирования прав доступа ролей. Установлен ряд допустимых условий передачи прав доступа ролей сессиями пользователей. Критерий возможности получения субъект сессией, функционирующей от имени недоверенного пользователя, доступа к другой субъект-сессии при отсутствии информационных потоков по памяти установлен в [13].

В [18] предложены алгоритмы построения замыканий для основных типов ДП-моделей. Эти замыкания являются основой для разработки топологических моделей анализа защищенности сетевых КС, т.е. моделей, учитывающих взаимосвязи субъектов и объектов, их свойства и характеристики. Реализации таких моделей называются топологическими сканерами безопасности сетевых КС. Таким образом, показано [18,21], что семейство ДП-моделей может быть использовано для моделирования сетевых КС с целью предотвращения уязвимостей, связанных с ошибками программного обеспечения, с доверием субъектов, с доступом к паролям субъектов и с раскрытием параметров КС. В частности, для сетевых КС, построенных на основе ОС Windows [1] или LINUX [19].

4. Заключение. В работе дан ретроспективный обзор формальных моделей безопасности КС, определивших современное состояние теории компьютерной безопасности. Охарактеризованы основные направления развития этой теории. Показано,что семейство ДП-моделей дает возможность обеспечить унифицированный под-

ход к решению целого спектра проблем, связанных с преодолением уязвимости сетевых КС.

Тем не менее, в настоящее время отсутствуют исследования взаимодействия формальных моделей безопасности КС со специализированными формальными моделями защиты информации в КС, такими, как криптосистема. Наличие последней в КС определяет свою топологию и предполагает присущее только ей администрирование. Поэтому возникает целый комплекс проблем, связанных с взаимодействием этих моделей. В частности, усложняется классификация сущностей. Анализ уязвимостей КС, возникающих при этом, является одним из возможных направлений исследований. Другое направление исследований связано с обеспечением специальных трассировок, обеспечивающих безопасность работы пользователей с расшифрованной информацией, а также специальных трассировок (там, где это возможно) при реализации процесса обмена сеансовыми ключами. Решение этой проблемы дает возможность сузить возможные атаки на криптосистему до класса атак, основанных на наличии только шифртекста.

1. *Брагг Р.* Система безопасности Windows 2000. – М.: Вильямс, 2001. – 592 с.
2. *Буренин П.В.* Подходы к построению ДП-модели файловых систем // Прикладная дискретная математика. – 2009. – № 1. – С. 93-112.
3. *Девянин П.Н., Михальский О.О., Правиков Д.И. и др.* Теоретические основы компьютерной безопасности. – М: Радио и связь, 2000. – 192 с.
4. *Девянин П.Н.* Подходы к обеспечению безопасности информационных потоков в системах мандатного разграничения доступа // Вестник Томского государственного университета. Приложение. – 2004. – № 9(I). – С. 100-105.
5. *Девянин П.Н.* Модели безопасности компьютерных систем. – М.: Издательский центр «Академия», 2005. – 144 с.
6. *Девянин П.Н.* Моделирование условий передачи прав доступа и реализации информационных потоков в компьютерных системах с дискреционным управляемым доступом // Вестник Томского государственного университета. Приложение. – 2005. – № 14. – С. 105-110.
7. *Девянин П.Н.* Анализ безопасности информационных потоков по памяти на функционально ассоциированные с субъектом сущности // Вестник Томского государственного университета. Приложение. – 2006. – № 17. – С. 151-156.
8. *Девянин П.Н.* Анализ безопасности управления доступом и информационными потоками в компьютерных системах. – М.: Радио и связь, 2006. – 176 с.
9. *Девянин П.Н.* Метод предотвращения реализации информационных потоков по времени в компьютерных системах с мандатным управлением доступом // Вестник Томского государственного университета. Приложение. – 2007. – № 23. – С. 165-168.
10. *Девянин П.Н.* Опыт преподавания безопасности компьютерных систем с мандатным управляемым доступом // Вестник Томского государственного университета. Приложение. – 2007. – № 23. – С. 169-173.
11. *Девянин П.Н.* Базовая ролевая ДП-модель // Прикладная дискретная математика. – 2008. – № 1. – С. 64-70.
12. *Девянин П.Н.* Обзорные лекции по моделям безопасности компьютерных систем // Прикладная дискретная математика. – 2009. – № 2. – С. 151-190.
13. *Девянин П.Н.* Анализ условий получения доступа владения в рамках базовой ролевой модели без информационных потоков по памяти // Прикладная дискретная математика. – 2009. – № 3. – С. 69-84.
14. *Девянин П.Н.* Анализ в рамках базовой ролевой ДП-модели безопасности систем с простыми траекториями функционирования // Прикладная дискретная математика. – 2010. – № 1. – С.

16-36.
15. *Зегжда Д.П., Ивашко А.М.* Основы безопасности информационных систем. – М.: Горячая линия-Телеком, 2000. – № 1. – 452 с.
16. *Колегов Д.Н.* ДП-модель компьютерной системы с функционально и параметрически ассоциированными сущностями // Вестник Сибирского государственного аэрокосмического университета. – 2009. – Вып. 1., Ч.1. – С. 49-54.
17. *Колегов Д.Н.* Проблемы синтеза и анализа графов атак // Вестник Томского государственного университета. Приложение. – 2007. – № 23. – С. 180-188.
18. *Колегов Д.Н.* Применение ДП-моделей для анализа защищенности сетей // Прикладная дискретная математика. – 2008. – № 1. – С. 71-78.
19. *Колегов Д.Н., Качанов М.А.* Расширение функциональности системы безопасности ядра Linux на основе подмены системных вызовов // Прикладная дискретная математика. – 2008. – № 2. – С. 76-80.
20. *Колегов Д.Н.* Анализ безопасности информационных потоков по памяти в компьютерных системах с функционально и параметрически ассоциированными сущностями // Прикладная дискретная математика. – 2009. – № 1. – С. 117-126.
21. *Колегов Д.Н.* Об использовании формальных моделей для анализа уязвимостей // Прикладная дискретная математика. – 2009. – № 1. – С. 113-117.
22. *Назаров И.О.* Обеспечение безопасности управления доступом и информационными потоками в веб-системе на основе СУБД // Вестник Казанского государственного технического университета. – 2008. – Вып. 2. – С. 56-59.
23. *Робачевский А.* Операционная система Unix. – СПб.: БХВ-Петербург, 2000. – 528 с.
24. *Столлингс В.* Криптография и защита сетей. – М: Вильямс, 2001. – 672 с.
25. *Хоффман Дж.* Современные методы защиты информации. – М.: Советское радио, 1980.
26. *Шнайер Б.* Секреты и ложь: безопасность данных в цифровом мире. – СПб: Питер, 2003. - 368с.
27. *Щербаков А.Ю.* Введение в теорию и практику компьютерной безопасности. – М: Издатель Молгачева С.В., 2001. – 352 с.
28. *Щербаков А.Ю.* Современная компьютерная безопасность. Теоретические основы. Практические аспекты. – М.: Книжный мир, 2009. – 352 с.
29. *Bell D.E., LaPadula L.J.* Secure cumputer systems: mathematical foundations // MITRE Corporation, 1976. – ESD-TR-73-278, V.1.
30. *Bell D.E., LaPadula L.J.* Secure cumputer systems: Unified exposition and multics interpretation. – Bedford, Mass.: MITRE Corp., 1976. – MTR-2997, Rev. 1.
31. *Biba K.J.* Integrity considerations for secure computer systems. // MITRE Corporation, 1977. – N MTR-3153.
32. *Bishop M.* Computer security: art and science. – ISBN 0-201-44099-7, 2002. – 1084 p.
33. *Clarke D., Wilson D.* A comparision of commercial and military computer systems // Proceedings of IEEE Symposium on Security and Privacy. – 1987. – P. 101 -117.
34. *Frank J., Bishop M.* Extending the take-grant protection system. Dept. of Computer Sci.: Univ. of California at Davis, 1984. – 28 p.
35. *Harrison M., Ruzzo W., Ullman J.* Protection in operating systems // Commumication of ACM. – 1976. –V. 19. – N 8. – P.461-471.
36. *Jones A., Lipton R., Snyder L.A.* A linear time algorithm for deciding security // Proc. of 17^{th} Annual Symposium on the Foundations of Computer Science, 1976. – P. 33-41.
37. *Lanawehrm E. Heitmeyer L., McLean J.* A security model for military message system // ACM Transactions on Computer Systems. – 1984. – Vol. 9. – N 3. – P. 198-222.
38. *LaPadula L.J., Bell D.E.* Secure cumputer systems: a mathematical model // MITRE Corporation, 1976. – ESD-TR-73-278, V.2.
39. *McLean J., John D.* The specification and modeling of computer security // Computer. – 1990. – V. 23. –N 1. – P. 118- 125.
40. *Sandhu R.* The typed access matrix model // Proc. of the IEEE Symposium on Research in Security and Privacy, 1992. – P. 122-136.

V.V. Skobelev

Analysis of security models for computer systems.

The given is some survey of the theory of computer security. It is presented retrospective analysis of models exerted a major influence on the development of this theory. It is characterized the class of AF-models, elaboration of which received considerable attention in recent and which provides a unified means to overcome the whole range of vulnerabilities of modern nets of computer systems. Some problems connected with interaction of formal models of computer security with any crypt-system are pointed.

Keywords: *security models, computer systems, AF-models.*

В.В. Скобелєв

Аналіз моделей безпеки комп'ютерних систем.

Дана стаття є оглядом з теорії комп'ютерної безпеки. У ній представлено ретроспективний аналіз моделей, які здійснили найбільший вплив на розвиток цієї теорії. Охарактеризовано клас ДП-моделей, опрацюванню якого приділяється значна увага в останній час, та який надає уніфіковані засоби для подолання цілого комплексу вразливостей сучасних мереж комп'ютерних систем. Зазначено низку задач, пов'язаних із забезпеченням взаємодії формальних моделей безпеки комп'ютерних систем з криптосистемою.

Ключові слова: *моделі безпеки, комп'ютерні системи, ДП-моделі.*

Ин-т прикл. математики и механики НАН Украины, Донецк
vv_skobelev@iamm.ac.donetsk.ua

Получено 27.10.10