МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

DOI 10.17223/20710410/12/2
УДК 004.94

ФОРМИРОВАНИЕ СЛОВАРЯ ТЕРМИНОВ ТЕОРИИ МОДЕЛИРОВАНИЯ БЕЗОПАСНОСТИ УПРАВЛЕНИЯ ДОСТУПОМ И ИНФОРМАЦИОННЫМИ ПОТОКАМИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ[1]

П. Н. Девянин

Институт криптографии, связи и информатики, г. Москва, Россия

E-mail: peter_devyanin@hotmail.com

Рассматривается проект словаря терминов, применяемых в теории моделирования управления доступом и информационными потоками в компьютерных системах. Словарь разработан на основе существующих стандартов в области компьютерной безопасности, а также с использованием определений основных элементов классических моделей и ДП-моделей безопасности компьютерных систем.

Ключевые слова: *компьютерная безопасность, управление доступом, словарь терминов.*

Введение

Существующие отечественные и зарубежные стандарты, учебные и научные издания, другие работы, в которых приводится терминология в области защиты информации (например, в [1 – 7] и др.), обеспечивают основу для стандартизации понятийного аппарата в данной области. В то же время содержащиеся в этих работах определения терминов часто отражают только организационно-правовые или общетехнические вопросы защиты информации, иногда в разных работах определения одних и тех же терминов не соответствуют друг другу. При этом крайне мало приводится терминов в области теории моделирования управления доступом и информационными потоками в компьютерных системах (КС), а имеющиеся термины часто не соответствуют ее современному уровню развития.

Формирование словаря терминов, применяемых в теории моделирования управления доступом и информационными потоками в КС, может оказать благотворное влияние на развитие данной теории, а также на процессы стандартизации понятийного аппарата и совершенствования образовательного процесса по направлению информационной безопасности.

Предлагаемый словарь следует рассматривать как промежуточный. Он подготовлен на основе существующих стандартов в области компьютерной безопасности, а также с использованием определений основных элементов классических моделей и ДП-моделей безопасности компьютерных систем [8].

В словаре содержатся определения терминов, разработанные автором или заимствованные (полностью или частично) из других работ. Для некоторых терминов да-

[1]Работа выполнена при поддержке гранта МД-2.2010.10

ется несколько определений. При этом в тексте словаря курсивом в определениях терминов выделены слова, соответствующие терминам, также содержащимся в словаре. Если определения термина заимствовано, то указывается источник заимствования.

Словарь терминов

Актив —
1) информация или ресурсы КС, подлежащие защите (на основе [2]);
2) подлежащие защите в КС *сущности*, *субъекты* и *информационные потоки*.

Атрибут безопасности — информация, связанная с *субъектами*, *пользователями* и/или *сущностями* и используемая для осуществления *политики безопасности управления доступом и информационными потоками* (на основе [2]).

Атрибут способа доступа к содержимому контейнера (*CCR*) — в рамках моделей КС с *мандатным управлением доступом* атрибут *контейнеров*, принимающий значения `true` или `false` и задающий порядок доступа к его содержимому (`true` — с учетом *уровня конфиденциальности* всего контейнера; `false` — с учетом только уровня конфиденциальности *сущности* в составе контейнера, к которой непосредственно осуществляется доступ).

Базовая теорема безопасности — теорема, обосновывающая в рамках *формальных моделей мандатного управления доступом*, построенных на основе *классической модели Белла — ЛаПадулы*, достаточные (в ряде случаев и необходимые) условия *безопасности системы*, заключающиеся в требовании *безопасности* всех *состояний* на *траекториях системы*. При этом в условии теоремы накладываются ограничения либо на множество действий системы (например, в *классической модели Белла — ЛаПадулы*), либо на *функцию переходов системы* (например, в *модели СВС)*.

Безопасность в смысле Белла — ЛаПадулы — выполнение в *системе* с *мандатным управлением доступом* $*$*-свойства* и *ss-свойства* безопасности или их аналогов (в *классической модели Белла — ЛаПадулы* дополнительно требуется выполнение *ds-свойства*).

Безопасность информации (данных) — состояние защищенности *информации* (*данных*), при котором обеспечены ее (их) *конфиденциальность*, *доступность* и *целостность* [3].

Граф доступов [прав доступа, информационных потоков] — конечный помеченный ориентированный без петель граф, описывающий *состояние системы* в рамках *формальной модели*. Вершинами графа являются *сущности* (*объекты*), *субъекты* или *роли*. Каждое ребро соответствует *доступу*, *праву доступа* или *информационному потоку* от вершины, соответствующей началу ребра, к вершине, соответствующей концу ребра.

Граф [прав] доступов в классической модели *Take-Grant* — *граф доступов* в рамках *классической модели Take-Grant*. Вершинами графа являются *объекты* и *субъекты* (обозначаются соответственно $\otimes$ и $\bullet$). Каждое ребро помечено непустым подмножеством множества видов *прав доступа* и задает наличие данных прав доступа у объекта или субъекта, соответствующих началу ребра, к объекту или субъекту, соответствующих концу ребра.

Граф [прав] доступов и информационных потоков в расширенной модели *Take-Grant* — *граф доступов* в рамках *расширенной модели Take-Grant*. Вершинами графа являются *объекты* и *субъекты* (обозначаются соответственно $\otimes$ и $\bullet$). Каждое «реальное» ребро (обозначается сплошной линией со стрелкой) помечено непустым подмножеством множества видов *прав доступа* и задает наличие данных прав досту-

па у объекта или субъекта, соответствующих началу ребра, к объекту или субъекту, соответствующих концу ребра. Каждое «мнимое» ребро (обозначается прерывистой линией со стрелкой) помечено непустым подмножеством множества видов информационных потоков (на чтение или на запись) и задает наличие данных информационных потоков от объекта или субъекта, соответствующих началу ребра, к объекту или субъекту, соответствующих концу ребра.

Граф прав доступа, доступов и информационных потоков в ДП-моделях — *граф доступов* в рамках *ДП-моделей*. Вершинами графа являются *сущности* и *субъекты* (обозначаются соответственно $\otimes$ и $\bullet$). Каждое ребро, соответствующее праву доступа *субъекта* к *сущности* (обозначается сплошной линией со стрелкой), помечено элементом множества видов *прав доступа*. Каждое ребро, соответствующее доступу субъекта к сущности (обозначается двойной сплошной линией со стрелкой), помечено элементом множества видов *доступов*. Каждое ребро, соответствующее *информационному потоку по памяти* (обозначается прерывистой линией со стрелкой и помечено $write_m$) или *по времени* (обозначается линией точек со стрелкой и помечено $write_t$), задает наличие информационного потока соответствующего вида от сущности или субъекта, являющегося началом ребра, к сущности или субъекту, являющемуся концом ребра. В описание графа также входит *функция иерархии сущностей*.

Граф создания в модели ТМД — ориентированный граф, вершины которого соответствуют *типам*, в котором ребро от вершины u к вершине v существует тогда и только тогда, когда в системе имеется *команда*, в которой u является *родительским типом*, а v — *дочерним типом*.

Данные —

1) факты, понятия или команды, представленные в формализованном виде и позволяющие осуществлять их передачу или обработку как вручную, так и с помощью средств автоматизации [3];

2) конечные последовательности бит.

Доступ — способ обращения *субъекта* к *сущности* для выполнения операции над нею.

Доступ блокирующий [информационные потоки по времени] — в рамках *ДП-моделей* любой *доступ доверенного субъекта* к *сущности* (такой доступ препятствует реализации *информационных потоков по времени* с использованием данной сущности и *иерархии сущностей*, в которую она входит).

Доступ владения — *доступ субъекта* (*субъект-сессии*) к субъекту, позволяющий первому субъекту получить полный контроль над вторым субъектом, заключающийся в возможности использования его *прав доступа*, *ролей* и *доступов*.

Доступ запрещенный/разрешенный — *доступ субъекта* к *сущности*, запрещенный/разрешенный априорно заданной *политикой безопасности управления доступом* и *информационными потоками*.

Доступы разрешенные совместные к сущности — задаваемое *субъектами*, обладающими *доступами* к данной *сущности* в некотором *состоянии системы*, множество *видов доступа*, которыми к данной сущности в этом состоянии одновременно могут обладать субъекты.

Доступность информации —

1) состояние информации, при котором *субъекты*, имеющие *права доступа*, могут реализовать их беспрепятственно [6];

2) свойство КС, в которой обрабатывается информация, характеризующееся способностью КС обеспечивать своевременный *доступ субъектов*, имеющих на это право, к запрашиваемой ими информации.

Замкнутая программная среда —

1) программная среда КС, в которой разрешено порождение *субъектов* только для фиксированного множества пар *активизирующих субъектов* и *сущностей источников* (на основе [7]);

2) программная среда КС, в которой функционирует *монитор безопасности субъектов* (на основе [7]).

Замыкание графа доступов [прав доступа, информационных потоков] — *граф доступов*, полученный из исходного графа доступов в результате применения к нему конечной последовательности *правил преобразования графов доступов*, принадлежащих некоторому подмножеству правил, заданных в рамках *формальной модели*. При этом дальнейшее применение к результирующему графу данных правил не приводит к появлению в нем новых элементов (вершин, соответствующих *сущностям*, или ребер, соответствующих *доступам*, *правам доступа* или *информационным потокам*).

Замыкание *tg* графа доступов [и информационных потоков] в рамках расширенной модели *Take-Grant* — *граф доступов*, полученный из исходного графа доступов в результате создания для каждого его *субъекта объекта* с ребром к нему, помеченным *правами доступа*: t (*take*), g (*grant*), r (*read*), w (*write*), а также применения к полученному графу конечной последовательности *де-юре правил преобразования графов доступов* вида *take* и *grant*, приводящих к добавлению в граф новых ребер, помеченных t или g. При этом дальнейшее применение к результирующему графу правил вида *take* и *grant* не приводит к появлению в нем новых ребер, помеченных t или g.

Замыкание де-факто графа доступов [и информационных потоков] в рамках расширенной модели *Take-Grant* — *граф доступов*, полученный из исходного графа доступов в результате создания для каждого его *субъекта объекта* с ребром к нему, помеченным *правами доступа*: t (*take*), g (*grant*), r (*read*), w (*write*), а также применения к полученному графу конечной последовательности *де-юре правил преобразования графов доступов* вида *take*, *grant* и *де-факто правил*. При этом дальнейшее применение к результирующему графу данных правил не приводит к появлению в нем новых ребер.

Замыкание де-юре графа доступов [и информационных потоков] в рамках расширенной модели *Take-Grant* — *граф доступов*, полученный из исходного графа доступов в результате создания для каждого его *субъекта объекта* с ребром к нему, помеченным *правами доступа*: t (*take*), g (*grant*), r (*read*), w (*write*), а также применения к полученному графу конечной последовательности *де-юре правил преобразования графов доступов* вида *take* и *grant*. При этом дальнейшее применение к результирующему графу правил вида *take* и *grant* не приводит к появлению в нем новых ребер.

Идентификатор —

1) представление уполномоченного *пользователя* (например, строка символов), однозначно его идентифицирующее [2];

2) некоторое представление (например, строкой символов или числом) *субъекта*, *сущности*, *роли*, *учетной записи пользователя* и др., однозначно их *идентифицирующее*.

Идентификация — присвоение *субъектам*, *сущностям*, *роли* или *учетной записи пользователя идентификатора* и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов (на основе [1]).

Иерархия ролей (административных ролей) — отношение *частичного порядка*, заданное на множестве *ролей*, удовлетворяющее условию: если две роли подчинены одна другой в иерархии ролей и старшая роль содержится в множестве авторизованных ролей некоторого *пользователя* (*учетной записи пользователя*), то младшая роль также содержится в этом множестве.

Иерархия сущностей — отношение *частичного порядка* на множестве *сущностей*, как правило, удовлетворяющее условию: если некоторая сущность x подчинена сущностям y и z, то из сущностей y и z одна подчинена другой (в ОС семейства *Unix* допускается размещение сущностей-объектов одновременно в нескольких сущностях-каталогах).

Изолированная программная среда (ИПС) — *замкнутая программная среда*, все *субъекты* которой из порождаемого множества, *монитор безопасности субъектов* и *монитор безопасности обращений попарно абсолютно корректны в смысле изолированной программной среды* (на основе [7]).

Информационный поток [от сущности-источника к сущности-приемнику] — преобразование *данных* в *сущности*-приемнике, реализуемое *субъектами системы*, зависящее от данных, содержащихся в сущности-источнике.

Информационный поток запрещенный —

1) *информационный поток*, запрещенный априорно заданной *политикой безопасности управления доступом и информационными потоками*;

2) в рамках КС с *мандатным управлением доступом* или их моделей информационный поток от *сущностей* с большим *уровнем конфиденциальности* к сущностям с меньшим уровнем конфиденциальности;

3) в рамках КС с *мандатным контролем целостности* или их моделей *информационный поток по памяти* от *сущностей* с *меньшим уровнем целостности* к сущностям с большим уровнем целостности;

4) в рамках *ДП-моделей информационные потоки по памяти* от *недоверенных субъектов* к *сущностям*, *функционально ассоциированным* с *доверенными субъектами*, или к недоверенным субъектам от сущностей, *параметрически ассоциированных* с доверенными субъектами.

Информационный поток по памяти — *информационный поток*, при реализации которого фактор времени является несущественным, и используются *сущности* (память), в которые передающий *субъект* (субъекты) записывает *данные*, а принимающий субъект (субъекты) считывает их (на основе [4]).

Информационный поток по времени — *информационный поток*, при реализации которого фактор времени является существенным, и передающий *субъект* (субъекты) модулирует передаваемые *данные* на некоторый изменяющийся во времени несущий процесс (последовательность событий) в КС, а принимающий субъект (субъекты) демодулирует передаваемые данные, наблюдая несущий процесс во времени (на основе [4]).

Информационный поток разрешенный — *информационный поток*, разрешенный априорно заданной *политикой безопасности управления доступом* и *информационными потоками*.

Команда в моделях ХРУ или ТМД — в рамках *моделей ХРУ* или *ТМД правило преобразования состояний* (задаваемых *матрицей доступов*), определяемое па-

раметрами (типизированными в модели ТМД), являющимися *субъектами* или *объектами*, условиями проверки у субъектов *прав доступа* к объектам и конечной последовательностью *примитивных операторов*.

Команда преобразования состояний — см. *правило преобразования состояний*.

Контейнер — *сущность*, которая содержит или получает информацию, над которой *субъекты* выполняют операции и могут получать к ней *доступ* или *права доступа* либо целиком, либо отдельно к входящим в ее состав сущностям (*объектам* или другим контейнерам).

Конфиденциальность информации — субъективно определяемая характеристика информации, указывающая на необходимость введения ограничений на множество *субъектов*, имеющих *права доступа* к данной информации.

Кооперация субъектов — взаимодействие *субъектов* КС при передаче *прав доступа* или реализации *информационных потоков*.

Мандатный контроль целостности (управление доступом с мандатным контролем целостности) — *управление доступом*, соответствующее следующим требованиям: все *сущности* должны быть *идентифицированы*; задана *решетка уровней целостности информации*; каждой сущности присвоен *уровень целостности*, задающий установленные ограничения на доступ к данной сущности; каждому *субъекту* системы присвоен *уровень целостности*, задающий уровень полномочий данного субъекта; субъект может получить *доступ* к сущности только в случае, когда уровень целостности субъекта позволяет предоставить ему данный доступ к сущности с заданным уровнем целостности, и реализация доступа не приведет к возникновению *запрещенных информационных потоков* от сущностей с низким уровнем целостности к сущностям с высоким уровнем целостности.

Матрица доступов — матрица, используемая при реализации *дискреционного управления доступом*, каждая строка которой соответствует *субъекту* КС, столбец — *сущности* КС, ячейка содержит список *прав доступа* субъекта к сущности, представляющий собой подмножество множества видов прав доступа, реализованных в КС.

Модели безопасности логического управления доступом и информационными потоками (ДП-модели) — семейство автоматных моделей КС с *дискреционным*, *мандатным* или *ролевым управлением доступом*, ориентированных на анализ условий передачи *прав доступа* к *сущностям* КС и возникновения между ними *информационных потоков по памяти* или по *времени* с учетом следующих существенных особенностей функционирования КС: возможности кооперации части *субъектов* при передаче прав доступа и создании информационных потоков, возможности реализации в КС *доверенных* и *недоверенных субъектов* с различными условиями функционирования, возможности противодействия доверенными субъектами КС передаче прав доступа или созданию информационных потоков недоверенными субъектами, различия условий реализации в КС информационных потоков по памяти и по времени, наличия в КС *иерархии сущностей* и возможности ее использования при создании информационных потоков по времени, а также изменения функциональности субъекта при реализации информационного потока по памяти на *функционально ассоциированные* с ним *сущности* или от *параметрически ассоциированных* с ним *сущностей*, необходимости в ряде случаев определения различных правил управления доступом и информационными потоками для распределенных компонент КС. Основные элементы: *граф прав доступа*, *доступов и информационных потоков* (включая *функцию иерархии сущностей*), задающий состояние системы, и фиксированное множество *правил преобразования состояний*.

Модели безопасности логического управления доступом и информационными потоками дискреционные (дискреционные ДП-модели) — базовые модели всего семейства *ДП-моделей*, ориентированные на анализ в КС с *дискреционным управлением доступом и информационными потоками* условий передачи *прав доступа* к *сущностям* и возникновения между ними *информационных потоков по памяти* или *по времени*. Основные модели семейства: ДП-модель с функционально или параметрически ассоциированными с субъектами сущностями (ФПАС ДП-модель), ДП-модель файловых систем (ФС ДП-модель) и ДП-модель управления доступом и информационными потоками в защищенных операционных системах (ЗОС ДП-модель).

Модели безопасности логического управления доступом и информационными потоками мандатные (мандатные ДП-модели) — модели семейства *ДП-моделей*, ориентированные на анализ в КС с *мандатным управлением доступом и информационными потоками* условий возникновения *запрещенных информационных потоков по времени* от *сущностей* с большим *уровнем конфиденциальности* к сущностям с меньшим уровнем конфиденциальности и запрещенных *информационных потоков по памяти* от *субъектов* с низким *уровнем доступа* к субъектам с высоким уровнем доступа или к сущностям, *функционально ассоциированным* с субъектами с высоким уровнем доступа. Основная модель семейства — мандатная ДП-модель.

Модели безопасности логического управления доступом и информационными потоками ролевые (ролевые ДП-модели) — модели семейства *ДП-моделей*, ориентированные на анализ в КС с *ролевым управлением доступом и информационными потоками* условий передачи *прав доступа ролей* и возникновения *информационных потоков*. Основные модели семейства: базовая ролевая ДП-модель (БР ДП-модель) и базовая ролевая ДП-модель управления доступом и информационными потоками в операционных системах (БРОС ДП-модель). Помимо элементов *дискреционных ДП-моделей* и *базовой ролевой модели* ($RBAC$) дополнительно используются следующие основные элементы: *доступы владения субъект-сессий* к субъект-сессиям, *фактические роли*, *права доступа* и *возможные действия* субъект-сессий, кроме того, в БРОС ДП-модель включены *фактические доступы* и *функции уровней целостности пользователей*, *сущностей*, *ролей* и *текущих уровней целостности субъект-сессий*.

Модель администрирования ролевого управления доступом ($ARBAC$) — автоматная модель КС с *ролевым управлением доступом и информационными потоками*, построенная на основе *базовой ролевой модели* ($RBAC$) и предназначенная для задания правил администрирования *иерархии ролей*, множеств авторизованных *ролей* пользователей и *прав доступа* ролей. Кроме элементов модели $RBAC$, основными элементами являются: *административные роли*, административные *права доступа*, функции авторизованных административных ролей *пользователей*, административных прав доступа административных ролей и иерархия административных ролей.

Модель Белла — ЛаПадулы классическая — автоматная базовая модель КС с *мандатным управлением доступом и информационными потоками*. Включает описание требований безопасности (*$*$-свойства*, *ss-свойства* и *ds-свойства*), направленных на предотвращение возможности реализации *запрещенных информационных потоков по памяти*. Основные элементы: *субъекты*, *объекты*, множество текущих *доступов* субъектов к объектам, *решетка многоуровневой безопасности*, *функции уровней доступа субъектов*, *текущих уровней доступа субъектов* и *уровней конфиденциальности объектов*, множество действий *системы*.

Модель Белла — ЛаПадулы в интерпретации «безопасность переходов» — автоматная модель КС с *мандатным управлением доступом и информаци-*

онными потоками, являющаяся интерпретацией *классической модели Белла — ЛаПадулы*, ориентированная на анализ условий реализации *информационных потоков по памяти* от *объектов* (*сущностей*) с высоким *уровнем конфиденциальности* к объектам с низким уровнем конфиденциальности. Основные элементы: *субъекты*, объекты, множество текущих *доступов* субъектов к объектам, *решетка многоуровневой безопасности*, *функции уровней доступа субъектов* и *уровней конфиденциальности объектов*, *функция переходов системы*.

Модель Биба — автоматная модель КС с *мандатным контролем целостности*, основанная на реализации требований *политики low-watermark*, направленных на предотвращение возможности возникновения *запрещенных информационных потоков по памяти* от *объектов* (*сущностей*) с низким *уровнем целостности* к *объектам* с высоким уровнем целостности. Основные элементы: *субъекты*, объекты, множество текущих *доступов* субъектов к объектам, *решетка уровней целостности*, *функции уровней целостности субъектов*, *текущих уровней целостности субъектов* и *уровней целостности объектов*, *функция переходов системы*.

Модель политики безопасности КС — структурированное представление *политики безопасности*, которая должна быть осуществлена в КС (на основе [2]).

Модель ролевая базовая (*RBAC*) — автоматная базовая модель КС с *ролевым управлением доступом и информационными потоками*, предоставляющая шаблон описания таких систем. Основные элементы: *пользователи*, *сессии*, *роли*, *права доступа*, *функции авторизованных ролей пользователей*, *прав доступа ролей* и *текущих ролей сессий*, *иерархия ролей* и *ограничения*.

Модель ролевого мандатного управления доступом (*MRBAC*) — автоматная модель КС с *ролевым управлением доступом и информационными потоками*, построенная на основе *базовой ролевой модели* (*RBAC*) и предназначенная для задания *мандатного управления доступом*. Кроме элементов модели *RBAC*, основными элементами являются: *решетка многоуровневой безопасности*, функции *уровней доступа пользователей* и *уровней конфиденциальности объектов* (*сущностей*), ограничения на *функции авторизованных ролей пользователей*, *прав доступа ролей* и *текущих ролей сессий*.

Модель систем военных сообщений (СВС) — автоматная модель КС с *мандатным управлением доступом и информационными потоками*, основанная на *классической модели Белла — ЛаПадулы*, изначально ориентированная на реализацию в электронных почтовых системах. Основные элементы: *пользователи*, *сущности* (в том числе сущности-«устройства вывода»), *косвенные* и *непосредственные ссылки на сущности*, *решетка многоуровневой безопасности*, *роли*, *функции иерархии сущностей*, *уровней доступа пользователей*, *уровней конфиденциальности сущностей*, максимальных уровней конфиденциальности информации, выводимой на сущностях-«устройствах вывода», *функция переходов системы*.

Модель субъектно-ориентированная изолированной программной среды — автоматная модель, основанная на *дискреционном управлении доступом*, предназначенная для анализа условий реализации в КС *изолированной программной среды*. Основные элементы: *субъекты*, в том числе *монитор безопасности обращений* и *монитор безопасности субъектов*, *объекты* (*сущности*), в том числе *функционально ассоциированные* с субъектами, *информационные потоки по памяти*.

Модель типизированной матрицы доступов (ТМД) — автоматная модель КС с *дискреционным управлением доступом*, развивающая *модель ХРУ*. Основные элементы: *матрица доступов*, *команды*, состоящие из типизированных параметров,

условий проверки наличия *прав доступа* в *матрице доступов* и *примитивных операторов*, изменяющих содержимое матрицы доступов. В рамках модели обосновывается *алгоритмическая разрешимость* задачи проверки безопасности *ациклических монотонных систем ТМД*.

Модель Харрисона — Руззо — Ульмана (ХРУ) — автоматная модель КС с *дискреционным управлением доступом*, предоставляющая шаблон описания таких систем. Основные элементы: *матрица доступов* и *команды*, состоящие из параметров, условий проверки наличия *прав доступа* в матрице доступов и *примитивных операторов*, изменяющих содержимое матрицы доступов. В рамках модели доказывается *алгоритмическая неразрешимость* задачи проверки безопасности КС с дискреционным управлением доступом, а также существование алгоритма проверки безопасности *монооперационных систем ХРУ*.

Модель угроз [безопасности информации] — физическое, математическое, описательное представление свойств или характеристик *угроз безопасности информации* [3].

Модель *Take-Grant* классическая — автоматная модель КС с *дискреционным управлением доступом*, ориентированная на анализ путей передачи *прав доступа* между *объектами* системы. Основные элементы: *граф доступов*, фиксированный набор *де-юре правил преобразования графов доступов* (*take*, *grant*, *create*, *remove*).

Модель *Take-Grant* расширенная — автоматная модель КС с *дискреционным управлением доступом и информационными потоками*, ориентированная на анализ путей реализации *информационных потоков* между *объектами* системы. Основные элементы: *граф доступов и информационных потоков*, фиксированный набор *де-юре* (*take*, *grant*, *create*, *remove*) и *де-факто правил преобразования графов доступов* (*find*, *pass*, *post*, *spy*). В рамках модели описывается также алгоритм построения *замыкания графа доступов* и информационных потоков и обосновывается корректность этого алгоритма.

Монитор безопасности обращений (МБО) — *монитор обращений*, допускающий возникновение в *системе* только *разрешенных информационных потоков* (на основе [7]).

Монитор безопасности субъектов (МБС) — *монитор порождения субъектов*, разрешающий порождение субъектов только для фиксированного множества пар *активизирующих субъектов* и *сущностей-источников* (на основе [7]).

Монитор обращений —

1) концепция абстрактной машины, реализующей *политику управления доступом* в КС (на основе [2]);

2) *субъект* (множество субъектов), активизирующийся при возникновении любого *информационного потока* между *сущностями* КС (на основе [7]).

Монитор порождения субъектов — *субъект* (множество субъектов), активизирующийся при любом порождении субъектов (на основе [7]).

Мост в модели *Take-Grant* — проходящий через вершины-*объекты* путь в *графе доступов*; концами пути являются вершины-*субъекты*, а его словарная запись имеет один из следующих видов: $\overrightarrow{t^*}$, $\overleftarrow{t^*}$, $\overrightarrow{t^*}\,\overrightarrow{g}\,\overleftarrow{t^*}$, $\overrightarrow{t^*}\,\overleftarrow{g}\,\overleftarrow{t^*}$, где t — *take*, g — *grant* и символ «$*$» означает многократное (в том числе нулевое) повторение.

Нарушение безопасности системы — переход КС в *состояние*, в котором либо получен *запрещенный доступ субъекта* к *сущности*, либо произошла *утечка запрещенного права доступа* субъекта к сущности, либо реализован *запрещенный информационный поток* между сущностями КС.

Нарушитель [правил доступа, разграничения доступа] —

1) *субъект доступа*, осуществляющий *несанкционированный доступ к информации* [5];

2) *недоверенный субъект*.

Неиерархическая категория конфиденциальности информации — элемент *решетки многоуровневой безопасности*, характеризующий субъективно принадлежность информации некоторому множеству *пользователей* КС (например, информация для отдела № 1, информация для отдела № 2) или указывающий на ее принадлежность определенной области, категории (например, информация военная, политическая, экономическая).

Несанкционированный доступ к информации (НСД) — *доступ* к информации, нарушающий *правила разграничения доступа* с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами [5].

Неформальный — выраженный на естественном языке [2].

Объект — *сущность*, которая содержит или получает информацию, над которой *субъекты* выполняют операции (на основе [2]) и могут получать к ней *доступ* или *права доступа* только целиком.

Ограничение — в рамках *моделей* КС с *ролевым управлением доступом* требование, которому должны удовлетворять *функции авторизованных ролей пользователей*, *прав доступа ролей* или *текущих ролей сессий* (*субъект-сессий*).

Ограничение динамическое — в рамках *моделей* КС с *ролевым управлением доступом ограничение* на *функцию текущих ролей сессий* (*субъект-сессий*).

Ограничение инвариантное относительно немонотонных правил преобразования состояний — *ограничение* в рамках *ролевых ДП-моделей*, обладающее следующим свойством: если в *системе* задано только данное ограничение, то для любой *траектории системы* применение или неприменение на ней любого *немонотонного правила* не влияет на выполнение ограничений у последующих за ним правил преобразования состояний.

Ограничение статическое — в рамках *моделей* КС с *ролевым управлением доступом ограничение* на *функцию авторизованных ролей пользователей* или *функцию прав доступа ролей*.

Остров в модели *Take-Grant* — максимальный *tg-связный* подграф, состоящий только из вершин *субъектов*.

Отношение порядка строгого — бинарное отношение «$<$» на конечном множестве, обладающее свойствами антирефлексивности (не $a < a$), транзитивности ($(a < b \,\&\, b < c) \Rightarrow a < c$) и антисимметричности (не одновременно $a < b$ и $b < a$).

Отношение порядка частичного — бинарное отношение «$\leqslant$» на конечном множестве, обладающее свойствами рефлексивности ($a \leqslant a$), транзитивности ($(a \leqslant b \,\&\, \&\, b \leqslant c) \Rightarrow a \leqslant c$) и антисимметричности ($(a \leqslant b \,\&\, b \leqslant a) \Rightarrow a = b$).

Параметр команды дочерний — в рамках *модели ТМД* параметр *команды*, соответствующий создаваемому в результате ее выполнения *субъекту* или *объекту*.

Параметр команды родительский — в рамках *модели ТМД* параметр *команды*, соответствующий *субъекту* или *объекту*, который не создается в результате ее выполнения.

Политика безопасности *low-watermark* — *политика управления доступом и информационными потоками* в КС с *мандатным контролем целостности*, направленная на предотвращение возможности реализации *запрещенных информационных*

потоков по памяти от *сущностей* с низким *уровнем целостности* к *сущностям* с высоким уровнем целостности.

Политика безопасности КС — совокупность правил, регулирующих управление *активами*, их защиту и распределение в КС (на основе [2]).

Политика безопасности [управления] информационных потоков — *политика безопасности*, основанная на разделении всех возможных *информационных потоков* между *сущностями* КС на два непересекающихся множества: множество *разрешенных информационных потоков* и множество *запрещенных информационных потоков* — и заключающаяся в обеспечении невозможности возникновения в КС запрещенных информационных потоков.

Политика безопасности управления доступом — совокупность правил управления *доступом субъектов* к *сущностям* КС.

Политика безопасности управления доступом дискреционная/мандатная/ролевая — *политика безопасности*, соответствующая требованиям *дискреционного/мандатного/ролевого управления доступом.*

Политика изолированной программной среды — *политика безопасности*, заключающаяся в задании порядка безопасного взаимодействия *субъектов* КС, обеспечивающего невозможность воздействия ими на систему защиты КС и модификации ее параметров или конфигурации, результатом которого могло бы стать изменение априорно заданной в КС *политики безопасности управления доступом и информационными потоками.*

Полуформальный — выраженный на языке с ограниченным синтаксисом и определенной семантикой [2].

Пользователь — любая *сущность* (человек-пользователь или внешний объект информационной технологии) вне КС, которая взаимодействует с КС (на основе [2]).

Пользователь доверенный/недоверенный — *пользователь системы в рамках формальной модели*, от имени которого функционируют *доверенные/недоверенные субъекты.*

Потенциальная модификация сущности с источником — способ задания в рамках *модели СВС* условий *возникновения информационного потока.* При этом предполагается, что информационный поток от *сущности*-источника к сущности-приемнику возникает при переходе *системы* из *состояния* в состояние по запросу *пользователя*, приводящему к изменению данных в сущности-приемнике в зависимости от данных в *сущности*-источнике.

Похищение права доступа — получение *субъектом права доступа* к *сущности* без активного участия субъектов, которые изначально этим правом обладали.

Правило преобразования графов доступов и информационных потоков де-факто в расширенной модели *Take-Grant* — *правило преобразования графов доступов и информационных потоков* (*find*, *pass*, *post*, *spy*), в результате применения которого в графе создаются ребра («мнимые» ребра), соответствующие *информационным потокам.*

Правило преобразования графов доступов [и информационных потоков] де-юре в классической или расширенной моделях *Take-Grant* — *правило преобразования графов доступов и информационных потоков* (*take*, *grant*, *create*, *remove*), в результате применения которого в графе создаются ребра («реальные» ребра), соответствующие правам доступа *субъектов* или *объектов* друг к другу.

Правило (команда) преобразования состояний (графов доступов, матриц доступов) — правило, задающее порядок перехода автомата (*системы в рамках формальной модели*) из *состояния* в состояние.

Правило преобразования состояний монотонное — *правило преобразования состояний*, в результате применения которого из *состояния системы* не происходит удаления любых его элементов (*субъектов*, *сущностей*, *прав доступа*, *доступов*, *информационных потоков* и др.).

Правило преобразования состояний немонотонное — *правило преобразования состояний*, в результате применения которого из *состояния системы* происходит удаление хотя бы одного его элемента (*субъекта*, *сущности*, *права доступа*, *доступа*, *информационного потока* и др.).

Право доступа —

1) совокупность правил доступа к защищаемой информации, установленных правовыми документами или собственником, владельцем информации [3];

2) совокупность правил *доступа*, задающих порядок и условия доступа *субъектов* к *сущностям* КС.

Право доступа запрещенное/разрешенное — *право доступа субъекта* к *сущности*, запрещенное/разрешенное априорно заданной *политикой безопасности управления доступом* и *информационными потоками*.

Предварительное условие — в рамках *модели администрирования ролевого управления доступом* (*ARBAC*) условие, которому должна удовлетворять *роль* или *право доступа* перед тем, как соответственно роль будет включена в множества *авторизованных ролей* некоторого *пользователя* или право доступа будет включено в множество прав доступа некоторой роли.

Примитивный оператор — используемое для задания *команд* в рамках *моделей ХРУ* или *ТМД* преобразование *матрицы доступов*, заключающееся в добавлении или удалении одного *права доступа субъекта* к *объекту*, создании или удалении одного субъекта или объекта.

Проблема массовая алгоритмически неразрешимая/разрешимая — массовая проблема, для которой не существует/существует алгоритм, вычисляющий ее характеристическую функцию [9].

Пролет моста конечный в модели *Take-Grant* — проходящий через вершины-объекты путь в *графе доступов* в рамках *модели Take-Grant*, началом которого является вершина-*субъект*, концом — вершина-*объект*; словарная запись пути имеет вид $\overrightarrow{t^*}$, где t — *take* и символ «$*$» означает многократное ненулевое повторение.

Пролет моста начальный в модели *Take-Grant* — проходящий через вершины-объекты путь в *графе доступов* в рамках *модели Take-Grant*, началом которого является вершина-*субъект*, концом — вершина-*объект*; словарная запись пути имеет вид $\overrightarrow{t^*}\,\overrightarrow{g}$, где t — *take*, g — *grant* и символ «$*$» означает многократное (в том числе нулевое) повторение.

Путь [*tg*-путь] в модели *Take-Grant* — проходящий через вершины-*субъекты* путь в *графе доступов* без учета направления ребер, каждое ребро которого помечено *правами доступа* t (*take*) или g (*grant*).

Путь [*own*-путь] в базовой ДП-модели — проходящий через вершины-*субъекты* путь в *графе прав доступа*, *доступов и информационных потоков* (описывающем *состояние системы* в рамках *базовой ДП-модели*) без учета направления ребер, каждое ребро которого помечено *правом доступа* владения (own_r).

Решетка уровней конфиденциальности [линейная] — линейно упорядоченное конечное множество *уровней конфиденциальности* (например, несекретно $<$ конфиденциально $<$ секретно).

Решетка многоуровневой безопасности (*MLS*-решетка) — решетка $(X \times L, \leqslant)$ с бинарным отношением частичного порядка «$\leqslant$», где $(L, \leqslant)$ — *линейная решетка уровней конфиденциальности*, $(X, \leqslant)$ — решетка подмножеств множества *неиерархических категорий конфиденциальности*, и отношение «$\leqslant$» на $X \times L$ удовлетворяет следующему условию: для $(a, \alpha), (b, \beta) \in X \times L$ справедливо $(a, \alpha) \leqslant (b, \beta)$ тогда и только тогда, когда $a \subseteq b$, $\alpha \leqslant \beta$.

Решетка уровней целостности — аналог *решетки многоуровневой безопасности*, в которой вместо *уровней конфиденциальности* и *неиерархических категорий конфиденциальности* используются соответственно *уровни целостности* и неиерархические категории целостности.

Роль —

1) заранее определенная совокупность правил, устанавливающих допустимое взаимодействие между *пользователем* и КС (на основе [2]);

2) совокупность *прав доступа* к *сущностям*.

Роль авторизованная пользователя (учетной записи пользователя, субъекта) — *роль*, которую потенциально могут получить функционирующие от имени *пользователя сессии* (*субъект-сессии*).

Роль административная — *роль*, обладающая *правами доступа*, позволяющими изменять параметры *ролевого управления доступом*, например множества *авторизованных ролей пользователей*, множества прав доступа ролей, *иерархию ролей*.

Роль текущая — роль, которой обладает *сессия* (*субъект*, *субъект-сессия*) в некотором *состоянии системы*.

Свойство безопасности $*$-свойство (свойство «звезда») — основное свойство безопасности моделей *систем с мандатным управлением доступом*, построенных на основе *классической модели Белла — ЛаПадулы*, задающее условия предоставления доступов *субъектов* к *сущностям* (*объектам*), направленные на предотвращение возможности реализации *запрещенных информационных потоков по памяти* от сущностей с высоким *уровнем конфиденциальности* к сущностям с низким уровнем конфиденциальности.

Свойство безопасности [*ds*-свойство] (свойство дискреционной безопасности) — свойство безопасности, задающее *дискреционное управление доступом* в рамках моделей *систем с мандатным управлением доступом*, построенных на основе *классической модели Белла — ЛаПадулы*.

Свойство безопасности [*ss*-свойство] («простое» свойство безопасности) — основное свойство безопасности моделей *систем с мандатным управлением доступом*, построенных на основе *классической модели Белла — ЛаПадулы*, задающее условия предоставления доступов *субъектов* к *сущностям* (*объектам*), направленные на обеспечение возможности предоставления *доступа* на чтение субъекта к сущности только в случае, когда *уровень доступа субъекта* не ниже *уровня конфиденциальности сущности*.

Связность [*tg*-связность] в модели *Take-Grant* — две вершины-*субъекта* *tg*-связны в *графе доступов*, когда они соединены *tg-путем*.

Связность [*own*-связность] в базовой ДП-модели — две вершины-*субъекта* *own*-связны в *графе прав доступа*, *доступов и информационных потоков* (описыва-

ющем *состояние системы* в рамках *базовой ДП-модели*), когда они соединены *output-путем*.

Сессия — см. субъект.

Система — специфическое воплощение информационной технологии с конкретным назначением и условиями эксплуатации [2].

Система в рамках ДП-моделей — автомат, каждое состояние которого задается *графом прав доступа, доступов и информационных потоков* (включая *функцию иерархии сущностей*) и элементами, специфичными для конкретных *ДП-моделей*, а *функция переходов — правилами преобразования состояний*.

Система в рамках модели Белла — ЛаПадулы —

1) автомат, каждое *состояние* которого задается множеством текущих *доступов субъектов* к *объектам* (*сущностям*), *матрицей доступов* (только в *классической модели Белла — ЛаПадулы*), *функциями уровней доступа субъектов*, *текущих уровней доступа субъектов* (только в *классической модели Белла — ЛаПадулы*) и *уровней конфиденциальности объектов*; *функция переходов* задается либо множеством действий системы (в *классической модели Белла — ЛаПадулы*), либо явно;

2) в *классической модели Белла — ЛаПадулы* множество всех возможных *траекторий* с заданным начальным *состоянием*, на каждой из которых переход из состояния в состояние осуществляется в соответствии с заданным множеством действий системы.

Система в рамках модели Биба — автомат, каждое *состояние* которого задается множеством текущих *доступов субъектов* к *объектам* (*сущностям*), *функциями уровней целостности субъектов*, *текущих уровней целостности* и *уровней целостности объектов*; *функция переходов* задается явно.

Система в рамках модели СВС — автомат, для которого задано начальное *состояние* и *функция переходов*, сопоставляющая каждому текущему состоянию системы, *идентификатору пользователя* (инициатора запроса) и запросу к *системе* последующее состояние системы.

Система в рамках модели ТМД — автомат, каждое состояние которого задается *матрицей доступов* и функцией *типов объектов*, *функция переходов — командами*.

Система в рамках модели ТМД монотонная (МТМД) — *система ТМД*, в *командах* которой отсутствуют *немонотонные примитивные операторы* вида «удалить»... и «уничтожить»...

Система в рамках модели ТМД монотонная в канонической форме — *система МТМД*, в которой *команды*, содержащие *примитивные операторы* вида «создать»..., не содержат условий и примитивных операторов вида «внести»...

Система в рамках модели ТМД монотонная ациклическая (АМТМД) — *система МТМД*, *граф создания* которой не содержит циклов.

Система в рамках модели ТМД монотонная циклическая — *система МТМД*, *граф создания* которой содержит хотя бы один цикл.

Система в рамках модели ТМД тернарная — *система ТМД*, каждая *команда* которой имеет не более трех *параметров*.

Система в рамках модели ХРУ — автомат, каждое состояние которого задается *матрицей доступов*; *функция переходов — командами*.

Система в рамках модели ХРУ монооперационная — *система* в рамках *модели ХРУ*, в каждой *команде* которой содержится один *примитивный оператор*.

Система в рамках формальной модели — заданный в рамках *формальной модели управления доступом* и *информационными потоками* автомат.

Система в рамках базовой ролевой модели (*RBAC*) — заданный в рамках *базовой ролевой модели* (*RBAC*) автомат, каждое состояние которого описывается *иерархией ролей*, *функциями авторизованных ролей пользователей*, *прав доступа ролей* и *текущих ролей сессий*; *функция переходов* задается явно.

Система в рамках модели *Take-Grant* классической — автомат, каждое состояние которого задается *графом доступов*, *функция переходов — де-юре правилами преобразования графов доступов*.

Система в рамках модели *Take-Grant* расширенной — автомат, каждое состояние которого задается *графом доступов и информационных потоков*, *функция переходов — де-юре* и *де-факто правилами преобразования графов доступов*.

Состояние системы — состояние автомата, задающего *систему* в рамках *формальной модели управления доступом* и *информационными потоками*.

Состояние системы безопасное — в рамках моделей КС с *мандатным управлением доступом состояние*, в котором все *доступы субъектов* к *сущностям* обладают $*$*-свойством* и *ss-свойством* (или их аналогами), дополнительно в *классической модели Белла — ЛаПадулы* обладают *ds-свойством*.

Состояние системы в рамках ДП-моделей — *граф прав доступа, доступов и информационных потоков* (включая *функцию иерархии сущностей*), а также элементы, специфичные для конкретных *ДП-моделей*.

Состояние системы в рамках классической модели *Take-Grant* — *граф доступов*.

Состояние системы в рамках модели Белла — ЛаПадулы — множество текущих *доступов субъектов* к *объектам* (*сущностям*), *матрица доступов* (только в *классической модели Белла — ЛаПадулы*), *функции уровней доступа субъектов*, *текущих уровней доступа субъектов* (только в *классической модели Белла — ЛаПадулы*) и *уровней конфиденциальности объектов*.

Состояние системы в рамках модели Биба — множество текущих *доступов субъектов* к *объектам* (*сущностям*), *функции уровней целостности субъектов*, *текущих уровней целостности субъектов* и *уровней целостности объектов*.

Состояние системы в рамках модели СВС — задается функциями *идентификаторов пользователей* (сопоставляет каждому идентификатору соответствующего ему *пользователя*), *ссылок на сущности* (сопоставляет каждой ссылке *сущность*, на которую она указывает) и входов пользователей (ставит в соответствие каждому идентификатору пользователя сущность-«устройство вывода», с которой вход в систему осуществил пользователь с данным идентификатором). При этом в каждом состоянии считаются заданными все другие элементы *модели СВС* (функции и множества).

Состояние системы в рамках модели ТМД — *матрица доступов* и *функция типов объектов*.

Состояние системы в рамках модели ХРУ — *матрица доступов*.

Состояние системы в рамках базовой ролевой модели (*RBAC*) — задается *иерархией ролей* и *функциями авторизованных ролей пользователей*, *прав доступа ролей* и *текущих ролей сессий*.

Состояние системы в рамках расширенной модели *Take-Grant* — *граф доступов и информационных потоков*.

Состояние системы в рамках модели ХРУ или ТМД, безопасное относительно права доступа *r* —

1) *состояние системы* в рамках *модели ХРУ* или *ТМД*, из которого невозможен переход системы в такое состояние, в котором возможна *утечка права доступа r*;

2) состояние системы в рамках модели ХРУ или *ТМД*, из которого невозможен переход системы в состояние, в котором право доступа r появляется в ячейке *матрицы доступов*, до этого r не содержавшей.

Ссылка на сущность косвенная — ссылка на *сущность*, являющуюся частью *контейнера*, через последовательность двух и более ссылок на сущности, в которой только первая ссылка есть *непосредственная ссылка*.

Ссылка на сущность непосредственная — ссылка на *сущность*, совпадающая с *идентификатором сущности*.

Субъект, активизирующий субъекта — *субъект*, в результате воздействия которого на *сущность-источник* в *системе* создается (активизируется) заданный субъект.

Субъект (субъект доступа, сессия, субъект-сессия) — *сущность*, которая инициирует выполнение операций (на основе [2]) или *правил преобразования состояний системы в рамках формальной модели*; действия субъекта регламентируются *политикой безопасности управления доступом* и*информационными потоками*.

Субъект доверенный —

1) *субъект системы в рамках формальной модели*, инициирующий выполнение *правил преобразования состояний*, реализация которых не приводит к нарушению в *системе* заданной *политики безопасности управления доступом* и *информационными потоками*. При моделировании реальных КС доверенным субъектам, как правило, соответствуют субъекты, реализующие механизмы безопасности или функционирующие от имени *доверенных* (привилегированных) *пользователей*;

2) в рамках *классической модели Белла — ЛаПадулы* субъект, которому разрешено нарушать $*$-*свойство безопасности*.

Субъект (субъект-сессия), доверенный и корректный в смысле целостности относительно сущности — *доверенный субъект*, не реализующий *информационный поток по памяти* к данной *сущности* от любой сущности с *уровнем целостности* ниже, чем у данной сущности.

Субъект (субъект-сессия), доверенный и корректный относительно информационных потоков по времени — *доверенный субъект*, не участвующий в реализации *информационных потоков по времени*.

Субъект, доверенный и корректный параметрически относительно сущности — *доверенный субъект*, не реализующий *информационный поток по памяти* к данной *сущности* (не являющейся доверенным субъектом) от любой сущности, *параметрически ассоциированной* с любым доверенным субъектом. При этом всегда каждый доверенный субъект корректен относительно другого доверенного субъекта (как сущности).

Субъект (субъект-сессия), доверенный и корректный параметрически относительно доверенного субъекта и сущности — *доверенный субъект*, не реализующий *информационный поток по памяти* к данной *сущности* от любой сущности, *параметрически ассоциированной* со вторым доверенным субъектом.

Субъект (субъект-сессия), доверенный и корректный функционально — *доверенный субъект*, во множество *функционально ассоциированных сущностей* которого не входят *недоверенные субъекты*.

Субъект, доверенный и корректный функционально относительно сущности — *доверенный субъект*, не реализующий *информационный поток по памяти* от данной *сущности* (не являющейся доверенным субъектом) к любой сущности, *функционально ассоциированной* с любым доверенным субъектом. При этом всегда каждый

доверенный субъект корректен относительно другого доверенного субъекта (как сущности).

Субъект (субъект-сессия), доверенный и корректный функционально относительно доверенного субъекта и сущности — *доверенный субъект*, не реализующий *информационный поток по памяти* от данной *сущности* к любой сущности, *функционально ассоциированной* со вторым доверенным субъектом.

Субъект недоверенный — *субъект системы в рамках формальной модели*, инициирующий выполнение любых заданных в *системе правил преобразования состояний*. При моделировании реальных КС недоверенным субъектам, как правило, соответствуют субъекты, функционирующие от имени *нарушителя* или *недоверенных* (непривилегированных) *пользователей*.

Субъекты, попарно корректные в смысле изолированной программной среды — множество *субъектов*, для каждой пары s и s' которых выполняется условие: в любом *состоянии системы* отсутствует *информационный поток по памяти* между любыми *сущностями* e и e', *функционально ассоциированными* соответственно с субъектами s и s' (на основе [7]).

Субъекты, попарно корректные абсолютно в смысле изолированной программной среды — множество *субъектов попарно корректных в смысле изолированной программной среды*, для каждой пары которых множества *функционально ассоциированных* с ними *сущностей* не имеют пересечения (на основе [7]).

Сущности, ассоциированные параметрически с субъектом — множество *сущностей*, содержащих *данные*, позволяющие идентифицировать вид преобразования данных, реализуемого *субъектом*.

Сущности, ассоциированные параметрически с учетной записью пользователя — множество *сущностей*, реализация от каждой из которых *информационного потока по памяти* к некоторому *субъекту* (*субъект-сессии*) позволяет ему создать субъекта от имени *данной учетной записи пользователя*.

Сущности, ассоциированные параметрически с ролью — множество *сущностей*, реализация от каждой из которых *информационного потока по памяти* к некоторому *субъекту* (*субъект-сессии*) является необходимым для получения или удаления им данной *роли* из множества его *текущих ролей*.

Сущность — *объект* или *контейнер*.

Сущность (объект), ассоциированная функционально с субъектом — *сущность*, *данные* в которой влияют на вид преобразования данных, реализуемого *субъектом*. Всегда субъект как сущность функционально ассоциирован сам с собой.

Сущность (объект)-источник при порождении субъекта — *сущность*, в результате воздействия на которую некоторым *субъектом* (*активизирующим субъектом*) в *системе* создается новый субъект.

Тип сущности — атрибут *сущности*, используемый при реализации, как правило, *дискреционного управления доступом*, как аналог *права доступа* (применяется в *моделях ТМД*, *СВС* и др., а также в некоторых ОС, например, ОС семейства *Linux* с пакетом безопасности *SELinux*).

Тип параметра команды дочерний/родительский — в рамках *модели ТМД тип дочернего/родительского параметра команды*.

Траектория (история) системы — конечная последовательность *состояний системы*, при этом на ней все переходы из состояния в состояние осуществлены в соответствии с заданными в системе *правилами преобразования состояний*.

Траектория системы без кооперации доверенных и недоверенных субъектов для передачи прав доступа — *траектория системы* в рамках *дискреционных* и *мандатных ДП-моделей*, при реализации которой используются *монотонные правила преобразования состояний* и *доверенные субъекты* не дают *недоверенным субъектам права доступа* к *сущностям* и не берут права доступа к сущностям.

Траектория системы без кооперации доверенных и недоверенных субъект-сессий для передачи прав доступа — *траектория системы* в рамках *ролевых ДП-моделей*, при реализации которой используются только *монотонные правила преобразования состояний* и *доверенные субъект-сессии* не берут *роли* во множество *текущих ролей*, не дают другим ролям *права доступа* к *сущностям*, не получают *доступ владения* к субъект-сессиям.

Траектория системы без кооперации доверенных и недоверенных субъектов для передачи прав доступа и реализации информационных потоков — в рамках *дискреционных* и *мандатных ДП-моделей траектория системы без кооперации доверенных и недоверенных субъектов для передачи прав доступа*, при реализации которой в случае инициирования *доверенными субъектами* применения *правил преобразования состояний* не создаются *информационные потоки по времени*.

Траектория системы блокирующих доступов доверенных субъектов — в рамках *дискреционных* и *мандатных ДП-моделей траектория системы без кооперации доверенных и недоверенных субъектов для передачи прав доступа*, при реализации которой все *доступы доверенных субъектов* являются *блокирующими* (*информационные потоки по времени*).

Траектория системы простая в рамках ролевых ДП-моделей — *траектория без кооперации доверенных и недоверенных субъект-сессий для передачи прав доступа*, при реализации которой *субъект-сессии* не получают *доступа владения* к субъект-сессиям с использованием *информационных потоков по памяти* к *сущностям, функционально ассоциированным*, или от сущностей, *параметрически ассоциированных* с этими субъект-сессиями.

Угроза безопасности информации — совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации [3].

Угроза доступности информации — потенциально возможное несанкционированное блокирование *доступа* к информации.

Угроза конфиденциальности информации — потенциально возможное нарушении *субъектами* установленных *политикой безопасности управления доступом* ограничений на *доступ* к информации.

Угроза раскрытия параметров КС — потенциально возможное несанкционированное выявление параметров, функций и свойств системы защиты КС.

Угроза целостности информации — потенциально возможное несанкционированное изменение информации *субъектами*.

Управление доступом — реализация в КС *политики безопасности управления доступом*.

Управление доступом дискреционное — *управление доступом*, соответствующее следующим требованиям: все *сущности* (в том числе *субъекты*) должны быть *идентифицированы*, т. е. каждой сущности должен быть присвоен уникальный *идентификатор*, задана *матрица доступов*, при этом субъект обладает *правом доступа* к сущности в том и только в том случае, когда в ячейке матрицы доступов, соответствующей субъекту и сущности, содержится данное право доступа.

Управление доступом мандатное — *управление доступом*, соответствующее следующим требованиям: все *сущности* должны быть *идентифицированы*; задана *решетка уровней конфиденциальности*; каждой сущности присвоен *уровень конфиденциальности*, задающий установленные ограничения на доступ к данной сущности; каждому *субъекту* системы присвоен *уровень доступа*, задающий уровень полномочий данного субъекта; субъект может получить *доступ* к сущности только в случае, когда уровень доступа субъекта позволяет предоставить ему данный доступ к сущности с заданным уровнем конфиденциальности и реализация доступа не приведет к возникновению *запрещенных информационных потоков* от сущностей с высоким уровнем конфиденциальности к сущностям с низким уровнем конфиденциальности.

Управление доступом ролевое — *управление доступом*, соответствующее следующим требованиям: все *сущности* должны быть *идентифицированы*; задано множество *ролей*, каждой из которых ставится в соответствие некоторое множество *прав доступа* к сущностям; каждый *субъект* (*сессия*, *субъект-сессия*) обладает некоторым множеством разрешенных (*авторизованных*) для данного субъекта ролей; субъект обладает правом доступа к сущности в случае, когда он обладает *текущей ролью* (принадлежащей множеству авторизованных ролей субъекта), которой соответствует множество прав доступа, содержащее данное право доступа к данной сущности.

Управление информационными потоками — реализация в КС *политики безопасности информационных потоков*.

Уровень доступа пользователя — элемент *решетки многоуровневой безопасности*, задающий максимальный *уровень конфиденциальности сущностей*, к которым функционирующие от имени *пользователя субъекты* могут получать *доступ* (как правило, на чтение).

Уровень доступа субъекта — элемент *решетки многоуровневой безопасности*, задающий максимальный *уровень конфиденциальности сущностей*, к которым *субъект* может получать *доступ* (как правило, на чтение).

Уровень доступа субъекта текущий — элемент *решетки многоуровневой безопасности*, задаваемый с целью предотвращения *запрещенных информационных потоков по памяти* от *сущностей* с высоким *уровнем конфиденциальности* к сущностям с низким уровнем конфиденциальности в зависимости от текущих (в некотором *состоянии системы*) *доступов субъекта* к *сущностям*. Всегда не превосходит *уровня доступа субъекта*.

Уровень конфиденциальности информации (данных) — элемент *решетки многоуровневой безопасности*, характеризующий *конфиденциальность информации*.

Уровень конфиденциальности сущности (объекта) — элемент *решетки многоуровневой безопасности*, соответствующий *уровню конфиденциальности данных*, содержащихся в *сущности*.

Уровень целостности информации — элемент *решетки уровней целостности*, характеризующий *целостность информации*.

Уровень целостности пользователя (учетной записи пользователя) — элемент *решетки уровней целостности*, задающий максимальный *уровень целостности сущностей*, к которым функционирующие от имени *пользователя субъекты* могут получать *доступ* на модификацию (запись, удаление и др.).

Уровень целостности роли — элемент *решетки уровней целостности*, задающий максимальный *уровень целостности сущностей*, к которым данная *роль* может обладать *правами доступа* владения или на модификацию (запись, удаление и др.).

Уровень целостности субъекта — элемент *решетки уровней целостности*, задающий максимальный *уровень целостности сущностей*, к которым *субъект* может получать *доступ* на модификацию (запись, удаление и др.).

Уровень целостности субъекта текущий — элемент *решетки уровней целостности*, задаваемый с целью предотвращения *запрещенных информационных потоков по памяти* от *сущностей* с низким *уровнем целостности* к сущностям с высоким уровнем целостности в зависимости от текущих (в некотором *состоянии системы*) *доступов субъекта* к сущностям. Всегда не превосходит *уровня целостности субъекта*.

Уровень целостности сущности (объекта) — элемент *решетки уровней целостности*, соответствующий *уровню целостности данных*, содержащихся в *сущности*.

Утечка права доступа (права доступа роли) — переход КС в *состояние*, в котором *субъект* получает *право доступа* к *сущности*, запрещенное априорно заданной *политикой безопасности управления доступом* и *информационными потоками*.

Утечка права доступа r в рамках модели ХРУ — переход *системы* в рамках *модели ХРУ* из некоторого *состояния* в последующее состояние в результате применения некоторой *команды*, содержащей *примитивный оператор*, вносящий *право доступа* r в ячейку *матрицы доступов*, до этого r не содержавшую.

Учетная запись пользователя — *идентификатор пользователя* и множество *параметрически ассоциированных* с ним *сущностей*.

Фактическое возможное действие субъекта (субъект-сессии) — действие (применение *правила преобразования состояния системы*), которое *субъект* может инициировать либо сам (при наличии у него соответствующих *текущих прав доступа*, *текущих ролей* и *административных ролей*), либо от имени некоторого другого субъекта, *доступом владения* к которому обладает первый субъект.

Фактическая роль/административная роль/доступ/уровень целостности субъекта (субъект-сессии) — *текущая роль/административная роль/доступ/уровень целостности* либо самого *субъекта*, либо некоторого другого субъекта, *доступом владения* к которому обладает первый субъект.

Фактическое право доступа субъекта (субъект-сессии) — *право доступа* либо самого *субъекта* (или его *текущей роли*), либо некоторого другого субъекта (или его *текущей роли*), *доступом владения* к которому обладает первый субъект.

Формальная модель — модель, заданная на математическом или ином другом *формализованном* языке.

Формальный — выраженный на языке с ограниченным синтаксисом и определенной семантикой, основанной на установившихся математических понятиях [2].

Функция авторизованных ролей пользователей — функция, задающая для каждого *пользователя* множество *ролей*, которые потенциально могут получить функционирующие от его имени *сессии* (*субъект-сессии*).

Функция администрирования иерархии ролей — в рамках *модели администрирования ролевого управления доступом* ($ARBAC$) функция, задающая для каждой административной *роли* интервал ролей, в пределах которого она позволяет изменять *иерархию ролей*.

Функция администрирования множеств авторизованных ролей пользователей — в рамках *модели администрирования ролевого управления доступом* ($ARBAC$) функция, задающая для каждой административной *роли* множество ролей,

которые с ее использованием могут быть включены или удалены из множества *авторизованных ролей пользователя* при выполнении заданных *предварительных условий*.

Функция администрирования прав доступа ролей — в рамках моделей КС с *ролевым управлением доступом* функция, задающая для каждой административной *роли* множество ролей, для которых с ее использованием разрешено включать или удалять *права доступа* из множеств прав доступа этих ролей (дополнительно в рамках *модели администрирования ролевого управления доступом ARBAC* требуется выполнение предварительных условий).

Функция иерархии ролей (административных ролей) — функция, задающая для каждой *роли* (*административной роли*) роли, которые непосредственно подчинены ей в *иерархии ролей*.

Функция иерархии сущностей — функция, задающая для каждой *сущности* сущности, которые непосредственно подчинены ей в *иерархии сущностей*.

Функция переходов системы — функция, задающая в рамках модели *системы* правила ее перехода из *состояния* в состояние.

Функция переходов системы безопасная —

1) в рамках *интерпретации «безопасность переходов» модели Белла — ЛаПадулы функция переходов системы*, обладающая $*$*-свойством* и *ss-свойством* для *функции переходов*;

2) в рамках *модели СВС функция переходов системы*, безопасная во всех смыслах, заданных в данной модели.

Функция переходов системы, безопасная в смысле администрирования —

1) в рамках *интерпретации «безопасность переходов» модели Белла — ЛаПадулы функция переходов системы*, разрешающая инициировать переход *системы* из *состояния* в состояние, в результате которого происходит изменение для некоторого *субъекта* его *уровня доступа* или для некоторого *объекта* (*сущности*) его *уровня конфиденциальности* только специально заданному для данных субъекта или объекта множеству субъектов;

2) заданная в рамках *модели СВС функция переходов системы*, запрещающая выполнение запросов *пользователей* к *системе*, которые не обладают *ролью*, разрешающей им изменять множества *авторизованных ролей пользователей*, *уровни доступа пользователей* или максимальные *уровни конфиденциальности информации*, выводимой на сущностях-«устройствах вывода».

Функция переходов системы, безопасная в смысле базовой теоремы безопасности — заданная в рамках *модели СВС функция переходов системы*, запрещающая выполнение запросов к *системе*, по которым она осуществляет переходы в небезопасные *состояния*.

Функция переходов системы, безопасная в смысле доступов к контейнерам с атрибутом *CCR* — заданная в рамках *модели СВС функция переходов системы*, запрещающая выполнение запросов *пользователей* к *системе*, которые приводят к *потенциальной модификации сущности с сущностью-источником*, находящейся в *контейнере* со значением `true` *атрибута способа доступа к содержимому контейнера* (*CCR*), обладающем *уровнем конфиденциальности* выше, чем *уровень доступа пользователя*.

Функция переходов системы, безопасная в смысле доступов к сущностям — заданная в рамках *модели СВС функция переходов системы*, запрещающая выполнение запросов к *системе*, по которым она осуществляет переходы в *состояния*, не удовлетворяющие требованиям *дискреционного управления доступом*.

Функция переходов системы, безопасная в смысле доступов по косвенной ссылке — заданная в рамках *модели CBC функция переходов системы*, запрещающая выполнение запросов *пользователей* к *системе*, которые приводят к получению *непосредственной ссылки на сущность*, находящуюся в *контейнере* со значением `true` *атрибута способа доступа к содержимому контейнера* (*CCR*), обладающем *уровнем конфиденциальности* выше, чем *уровень доступа пользователя*.

Функция переходов системы, безопасная в смысле модификации сущностей — заданная в рамках *модели CBC функция переходов системы*, запрещающая выполнение запросов к *системе*, которые приводят к *потенциальной модификации сущности*-приемника, обладающей *уровнем конфиденциальности* ниже, чем уровень конфиденциальности *сущности*-источника.

Функция пользователей сессий (субъект-сессий) — функция, задающая для каждой *сессии* (*субъект-сессии*) *пользователя*, от имени которого она функционирует.

Функция прав доступа ролей — функция, задающая для каждой *роли* множество *прав доступа* к *сущностям* (*объектам*), которыми она обладает.

Функция типов объектов в модели ТМД — функция, задающая в каждом состоянии *системы ТМД* для каждого *объекта* (или *субъекта*) его *тип*.

Функция текущих уровней доступа субъектов (пользователей) — функция, задающая в рамках *моделей систем* с *мандатным управлением доступом* для каждого *субъекта* его *текущий уровень доступа*.

Функция текущих уровней целостности субъектов (субъект-сессий) — функция, задающая в рамках *моделей систем* с *мандатным контролем целостности* для каждого *субъекта* его *текущий уровень целостности*.

Функция текущих ролей сессий (субъект-сессий) — функция, задающая для каждой *сессии* (*субъект-сессии*) в каждом *состоянии системы* множество *ролей*, которыми она обладает. Всегда для каждой сессии данное множество является подмножеством множества *авторизованных ролей пользователя*, от имени которого она функционирует.

Функция уровней доступа субъектов (пользователей) — функция, являющаяся одним из основных элементов *моделей систем* с *мандатным управлением доступом* и задающая для каждого *субъекта* его *уровень доступа*.

Функция уровней конфиденциальности сущностей (объектов) — функция, являющаяся одним из основных элементов *моделей систем* с *мандатным управлением доступом* и задающая для каждой *сущности* ее *уровень конфиденциальности*.

Функция уровней целостности ролей — функция, являющаяся элементом *ролевых ДП-моделей* и задающая для каждой *роли* ее *уровень целостности*.

Функция уровней целостности субъектов (субъект-сессий, пользователей) — функция, являющаяся одним из основных элементов *моделей систем* с *мандатным контролем целостности* и задающая для каждого *субъекта* его *уровень целостности*.

Функция уровней целостности сущностей (объектов) — функция, являющаяся одним из основных элементов *моделей систем* с *мандатным контролем целостности* и задающая для каждой *сущности* ее *уровень целостности*.

Целостность информации — состояние информации, при котором отсутствует любое ее изменение, либо изменение осуществляется только преднамеренно *субъектами*, имеющими на него право [3].

ЛИТЕРАТУРА

1. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных // Методические материалы ФСТЭК. 2008.
2. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий // Руководящий документ. ГОСТ Р ИСО/МЭК 15408-2002.
3. Защита информации. Основные термины и определения // Национальный стандарт Российской Федерации. ГОСТ Р 50922-2006.
4. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов // Национальный стандарт Российской Федерации. ГОСТ Р 53113.1-2008, ГОСТ Р 53113.2-2009.
5. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации // Гостехкомиссия России. Руководящий документ. 1992.
6. Техническая защита информации. Основные термины и определения // Рекомендации по стандартизации. Р 50.1.056-2005.
7. *Щербаков А. Ю.* Современная компьютерная безопасность. Теоретические основы. Практические аспекты. Учеб. пособие. М.: Книжный мир, 2009. 352 с.
8. *Девянин П. Н.* Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учеб. пособие для вузов. М.: Горячая линия — Телеком, 2011. 320 с.
9. *Носов В. А.* Основы теории алгоритмов и анализа их сложности. Курс лекций. М.: МГУ, 1992. 140 с.