УДК 004.04

В.Е. Мухин, А.Н. Волокита

Разработка и реализация политики безопасности в распределенных компьютерных системах

Рассмотрены общие принципы построения и основные элементы модели политики безопасности компьютерных систем, определены потенциальные угрозы их безопасности, сформулирован и обоснован основной принцип политики безопасного администрирования.

The general principles of the design and the basic elements of the security policy of computer systems are described. The potential threats to their security are defined, the main principles of the policy of the safe administrating is formulated and substantiated.

Розглянуто загальні принципи побудови та основні елементи моделі політики безпеки комп'ютерних систем, визначено потенційні загрози їх безпеці, сформульовано і обгрунтовано основний принцип політики безпечного адміністрування.

Введение. Построение эффективной системы защиты информации в распределенных компьютерных системах (РКС) требует реализации комплексного подхода, важнейший элемент которого – формирование и реализация политики безопасности.

Политика безопасности представляет собой набор правил и нормативных документов, определяющих реализацию административных и программно-аппаратных механизмов защиты информации в РКС. Сформированная политика безопасности позволяет выбрать конкретные средства для ее обеспечения, представляя собой активный компонент защиты, включающий в себя предварительный анализ возможных угроз безопасности, правила поведения легальных субъектов РКС и принципы выбора механизмов для предотвращения несанкционированного доступа нарушителей.

Однако в процессе реализации политики безопасности возникают *следующие задачи*: определение базовых принципов формирования политики безопасности, разработка механизмов поддержки, анализа и контроля политики безопасности, а также формализация правил политики безопасности, в частности, правил управления доступом субъектов к объектам компьютерных систем. Выделим в качестве основной задачи вопрос формализации политики безопасности и разработаем соответствующую модель политики безопасного управления доступом в распределенных компьютерных системах.

Общие принципы построения политики безопасности распределенных компьютерных систем

Главная задача при формировании политики безопасности распределенных компьютерных систем – определение правил защиты ресурсов, т.е. информационных активов РКС.

В целом политика безопасности РКС характеризуется следующим [1–3]:

- содержит концепцию, включающую в себя цели, основные направления и принципы действий в сфере информационной безопасности;
- учитывает нормативно-правовые требования, а также требования владельцев информации по обеспечению ее безопасности;
- согласуется со стратегией управления рисками безопасности в РКС, для которых она разрабатывается и поддерживается;
- устанавливает критерии оценки рисков безопасности;
- утверждается администратором безопасности и руководством организации, владеющей РКС.

Изначально политика безопасности строится с учетом рисков безопасности, существующих в РКС. Далее определяется стратегия защиты, составляется программа обеспечения информационной безопасности и устанавливаются правила, определяющие конфигурацию сис-

тем защиты, а также действия администратора безопасности и пользователей РКС в штатных условиях и в случае непредвиденных обстоятельств, например, при атаках злоумышленников [4].

Таким образом, политика безопасности выполняет две основные функции, определяя:

- права и полномочия легальных субъектов в РКС;
- правила защиты ресурсов РКС.

Политика безопасности представляется в комплексе документов, отражающих все основные требования к обеспечению защиты информации в РКС [1], а также определяет способы имплементации системы безопасности и правила настройки параметров распределенных компьютерных систем. При этом определяются требуемые механизмы защиты информации в РКС, устанавливается порядок реагирования в случае нештатных ситуаций. При возникновении инцидентов, связанных с нарушением безопасности или сбоем в работе системы, политика безопасности устанавливает порядок действий, направленных на устранение последствий.

Таким образом, политика информационной безопасности РКС основывается на обобщенных строго формализованных правилах, процедурах и требованиях:

– использование сертифицированного оборудования и программного обеспечения;

– установление процедур допуска субъектов к ресурсам РКС;

– установление правил защиты ресурсов;

– определение правил доступа субъектов к объектам РКС и т.д.

Существенная функция политики безопасности – четкое разграничение прав субъектов РКС по отношению к объектам: все легальные субъекты должны четко знать границы своих прав, а также права других субъектов–участников РКС по отношению к объектам, владельцами которых они являются.

В целом политика безопасности определяет действия администраторов РКС и легальных субъектов при инсталляции и использовании средств защиты информации, а также в процессе обработки и передачи информации в РКС.

Выделяются три основные раздела политики безопасности [5]:

– имеет четко определенную задачу, обосновывающую необходимость применения и преимущества процедур, реализующих данную политику (цель);

– содержит раздел, описывающий конкретную сферу ее применения, например, она применяется ко всем компьютерным системам и сетям или лишь к отдельным сегментам РКС (область);

– определяются действия администратора безопасности, который должен знать все требования политики безопасности в конкретной РКС (ответственность).

Разработка политики безопасности предполагает реализацию ряда предварительных шагов:

- выявление угроз для ресурсов РКС;
- анализ потенциально уязвимых ресурсов РКС;
- оценку рисков безопасности для конкретных РКС.

Общий жизненный цикл политики безопасности включает в себя следующие основные этапы:

- проведение предварительного анализа состояния информационной безопасности РКС;
- разработку политики безопасности;
- внедрение разработанной политики безопасности;
- анализ реализации политики безопасности и выполнение действий по ее дальнейшему совершенствованию.

Основные элементы политики безопасности

Согласно требованиям современных стандартов в области безопасности [5, 6], политика безопасности должна включать в себя следующие элементы:

- назначение уровня допуска субъектов к ресурсам РКС;
- управление доступом субъектов к объектам РКС;
- поддержку безопасности использования объектов.

Рассмотрим особенности каждого из перечисленных элементов.

Назначение уровней допуска субъектов к объектам РКС

Для разграничения уровней допуска субъектов к объектам им назначаются метки безопасности. Метка субъекта описывает уровень его допуска к объектам, метка объекта – степень секретности содержащейся в нем информации. Метки безопасности состоят из двух частей – уровня секретности и списка категорий. Уровни секретности, установленные в системе, формируют упорядоченное множество, которое может быть следующим:

- совершенно секретно;
- секретно;
- конфиденциально;
- открытая информация.

Категории образуют неупорядоченный набор, описывающий предметную область, к которой относятся данные. Механизм категорий позволяет разделить информацию по сегментам, что повышает защищенность объектов. Так, субъект не может получить доступ к сегментам «чужих» категорий, даже если уровень его допуска – «совершенно секретно».

Управление доступом субъектов к объектам РКС

С учетом политики безопасности оно разделяется на *мандатное* и *меточное* управление.

Мандатное управление доступом – это метод управления доступом к объектам, основаный на учете личности субъекта или группы, в которую входит субъект. Специфика мандатного управления состоит в том, что некоторое лицо (администратор безопасности или владелец объекта) предоставляет другим субъектам права доступа (мандат) к объекту. Текущее состояние прав доступа при мандатном управлении описывается матрицей доступа, в строках которой перечислены субъекты, а в столбцах – объекты РКС. В позициях, расположенных на пересечении строк и столбцов, записываются права доступа, предоставленные субъекту i по отношению к объекту j, например: R-чтение, W-запись, E-выполнение, T-разрешение на передачу прав другим субъектам и т.д. Однако ввиду того, что данная матрица весьма велика по объему хранимых данных и разрежена, т.е. большинство позиций в ней пусты или нулевые, в практических приложениях в РКС используется более компактное представление матрицы доступа, основанное на структурировании прав субъектов (владелец/группа/ прочие) либо на механизме списков управления доступом, т.е. на разбиении матрицы по столбцам, когда для каждого объекта перечисляются субъекты вместе с их правами доступа.

В большинстве РКС реализуется именно мандатное управление доступом. Главное его достоинство – адаптивность, главные недостатки – децентрализация управления ввиду сложности централизованного контроля, а также отделение мандатов от данных, что позволяет копировать секретную информацию в общедоступные файлы [7].

Меточное управление доступом базируется на сопоставлении меток безопасности субъекта и объекта. После того, как установлены метки безопасности субъектов и объектов, фиксируются соответствующие права доступа субъектов к объектам.

Для эффективной реализации меточного механизма управления доступом необходимо обеспечить целостность меток. Во-первых, не должно быть субъектов и объектов без меток, иначе возникнут легко используемые «дыры». Во-вторых, при любых операциях с данными метки должны быть корректными, в особенности это относится к экспорту и импорту данных. Так, при передаче файла по каналу связи должна передаваться и ассоциированная с ним метка, причем в таком виде, чтобы удаленная система могла ее идентифицировать, несмотря на возможные различия в уровнях секретности и наборе категорий.

Одним из средств обеспечения целостности меток безопасности является разделение ресурсов РКС на многоуровневые и одноуровневые. На многоуровневых ресурсах может храниться информация разных уровней секретности, одноуровневые ресурсы представляют собой частный случай многоуровневых, когда допустимый диапазон состоит из одного уровня. На основании анализа уровня ресурса принимается решение о записи на него информа-

ции с определенной меткой. Например, запрещено печатать совершенно секретную информацию на сетевом принтере с уровнем допуска «конфиденциально».

Метки безопасности, ассоциируемые с субъектами, более динамичны, чем метки объектов. Субъект может в течение сеанса работы с системой изменять свою метку, не выходя за предопределенный для него диапазон допуска. В частности, он может преднамеренно снижать уровень своего допуска для уменьшения вероятности совершения непреднамеренных ошибок, реализуя принцип минимизации привилегий.

Субъект может читать информацию из объекта только в том случае, если уровень секретности субъекта не ниже чем у объекта, а все категории, перечисленные в метке безопасности объекта, присутствуют в метке субъекта, т.е. метка субъекта «доминирует» над меткой объекта. Субъект может записывать информацию в объект только в том случае, если метка безопасности объекта «доминирует» над меткой субъекта. В частности, субъект с уровнем допуска «конфиденциально» может писать в «секретные» файлы, но не может – в «открытые», т.е. уровень секретности информации не должен понижаться.

Меточное управление доступом эффективно реализуется в РКС с повышенным уровнем безопасности. Независимо от практического использования, меточное управление – удобный методологический базис для начальной классификации информации и распределения прав доступа. На практике мандатное и меточное управление доступом может сочетаться в рамках одной РКС, что позволяет использовать преимущества обоих подходов.

Безопасность использования объектов – дополнение средств управления доступом, предохраняющее от случайного или преднамеренного получения доступа к секретной информации. Безопасность использования должна гарантироваться для областей оперативной памяти (в частности, для буферов с образами экрана, расшифрованными паролями и т.п.), для дисковых блоков и других хранилищ данных в РКС.

Ввиду того что информация о субъектах также представляет собой объект, необходимо обеспечить безопасность этих данных. Когда пользователь теряет права доступа к ресурсам РКС, его следует не только лишить возможности входа в систему, но также запретить ему доступ ко всем объектам, иначе новый пользователь сможет получить ранее использовавшийся идентификатор и все права своего предшественника [8].

Контроль

Механизм контроля является дополнением к правилам управления доступа субъектов к объектам. Цель контроля – отслеживание действий субъектов и состояния объектов в любой момент их нахождения в РКС. Средства контроля делятся на три категории:

- идентификация и аутентификация;
- предоставление защищенного канала связи;
- анализ действий субъектов.

Рассмотрим эти категории.

Идентификация и аутентификация

Каждый пользователь, прежде чем получить доступ к РКС должен идентифицировать себя, т.е. ввести свое имя (*login*) при входе в систему. В свою очередь система должна его аутентифицировать – проверить его подлинность и подтвердить, что он тот, за кого себя выдает. Простейшее средство проверки подлинности – пароль, но могут использоваться и более сложные механизмы, такие как личные карточки, биометрические устройства и т.д.

Идентификация и аутентификация – первый и важнейший этап обеспечения информационной безопасности, поскольку без идентификации пользователей невозможно протоколировать их действия.

Предоставление защищенного канала связи

Защищенный канал связывает пользователя непосредственно с ресурсами РКС, минуя другие, потенциально опасные компоненты системы. Цель предоставления защищенного канала связи – обеспечить пользователю подтверждение подлинности РКС, с которой он взаимодействует.

Достаточно легко реализовать защищенный канал связи в том случае, если используется

неинтеллектуальный терминал – при условии защищенности линии связи между терминалом и системой достаточно реализовать специальный протокол взаимодействия. Если же пользователь работает с интеллектуальным терминалом, персональным компьютером или рабочей станцией, задача обеспечения защищенного канала связи значительно усложняется [9].

Анализ действий субъектов

Данный анализ связан с действиями субъектов (событиями), относящимися к безопасности системы. К числу таких событий относятся: вход в систему (*login*); выход из системы (*logout*); операции с файлами (открыть, закрыть, переименовать, удалить); обращение к удаленным ресурсам РКС; смена привилегий или других атрибутов безопасности (прав доступа, уровня допуска пользователя и т.п.).

Полный перечень событий в РКС, подлежащих регистрации и анализу, зависит от выбора политики безопасности и от специфики самой РКС.

Если фиксировать все события, связанные с безопасностью РКС, то объем регистрационной информации будет увеличиваться и эффективный анализ этих данных станет невозможным. Поэтому часто реализуется механизм выборочного мониторинга как действий пользователей (например, отслеживаются только подозрительные субъекты), так и событий безопасности.

Мониторинг позволяет следить за пользователями и реконструировать прошедшие события, он также важен как профилактическое средство, поскольку субъекты могут воздержаться от нарушений безопасности, зная, что их действия фиксируются. Реконструкция событий позволяет проанализировать случаи нарушений безопасности, выяснить их причины, оценить размеры ущерба и принять меры по недопущению подобных нарушений в будущем.

При мониторинге событий фиксируется следующая информация:

- дата и время события;
- идентификатор субъекта – инициатора действия;
- тип события;
- результат действия субъекта;
- идентификаторы используемых объектов (например, открываемых или удаляемых файлов);
- метки безопасности субъектов и объектов события;
- изменения, внесенные в регистрационные записи по безопасности (например, новая метка безопасности объекта).

Отметим важность не только сбора информации, но и ее регулярного и целенаправленного анализа, т.е. гарантированности.

Гарантированность – это степень уверенности, с которой можно утверждать, что для реализации политики безопасности в РКС выбран подходящий набор средств и что каждое из этих средств корректно выполняет свои функции.

Выделяются два вида гарантированности – операционная и технологическая. Операционная гарантированность относится к архитектурным и реализационным аспектам системы, а технологическая – к методам построения и сопровождения системы.

Операционная гарантированность включает в себя проверку следующих элементов: архитектура системы, целостность системы, защищенность каналов передачи информации, эффективность администрирования безопасности, надежность восстановления системы после сбоев.

Операционная гарантированность позволяет убедиться в том, что архитектура РКС и ее реализация действительно соответствует избранной политике безопасности. Архитектура системы должна способствовать реализации мер безопасности и поддерживать их. Примеры подобных архитектурных решений в рамках аппаратуры и операционной системы РКС – разделение команд по уровням привилегированности, защита различных процессов от взаимного влияния при выделении каждому своего виртуального пространства, особая защита ядра операционной системы.

Технологическая гарантированность охватывает весь жизненный цикл РКС, т.е. периоды проектирования, реализации, тестирования и сопровождения. Все перечисленные действия должны выполняться в соответствии с установленными требованиями, чтобы обезопа-

ситься от несанкционированного доступа к информации и нелегальных «закладок» в программное обеспечение и аппаратуру РКС.

Важный аспект технологической гарантированности – тестирование. Тестированию подлежат как собственно механизмы безопасности, так и пользовательский интерфейс к ним. Тесты должны подтвердить, что защитные механизмы функционируют в соответствии со своим описанием и что не существует доступных способов обхода или разрушения защиты, а также продемонстрировать действенность средств управления доступом, защищенность регистрационной и аутентификационной информации.

Модель политики безопасности распределенных компьютерных систем

Рассмотрим и формализуем один из аспектов политики безопасности, связанный с управлением доступом субъектов к объектам РКС на основе использования математической модели. Фактически, рассмотрим формализацию политики безопасного администрирования РКС.

Для формализации представления модели введем следующие обозначения:

$ND = \{nd_i\}$ – множество узлов РКС, которое включает в себя сервера и рабочие станции, $SR = \{sr_i\}$ – подмножество серверов (маршрутизаторов) доменов РКС, $WS = \{ws_i\}$ – подмножество рабочих станций, при этом: $SR \cup WS = ND$, $SR \cap WS = \varnothing$.

$U = \{u_i\}$ – множество субъектов РКС;

$A(u,ws)$ – функция, определяющая для субъектов $\{u_i\}$ множество рабочих станций $\{ws_i\}$, к которым они имеют доступ локально или по сетевым коммуникационным каналам;

$M(u,ws)$ – функция, определяющая для субъектов $\{u_i\}$ множество рабочих станций $\{ws_i\}$, на которых они могут размещать и модифицировать свои ресурсы: файлы, данные или процессы от своего имени;

$R(u,ws)$ – функция, определяющая множество прав субъектов $\{u_i\}$ на рабочих станциях $\{ws_i\}$;

R_{wsj} – множество прав субъектов U по отношению к рабочей станции ws_j, таких как читать, модифицировать информацию, запускать процессы, администрировать операционную систему и т.д.

После инсталляции система безопасности РКС характеризуется следующим образом:

• множества *ND, SR, WS* и $R(u,ws)$ являются постоянными во времени. Регистрация субъектов, установление их прав в системе, а также функции серверов и рабочих станций в РКС определяются администратором системы перед допуском субъектов к РКС;

• изначально субъекты РКС не имеют своих ресурсов на рабочих станциях, т.е. для каждого $\{u_i\}$:

$$M(u,ws) = \varnothing; \qquad (1)$$

• легальный (зарегистрированный) субъект u_i рабочей станции ws_j обладает правами $R(u_i,ws_j)$ по доступу к ней.

• если у субъекта u_i некоторые специальные права по доступу к определенной рабочей станции ws_j, например: R_1 = «Отладка», R_2 = «Инсталляция драйверов» и т.д., то он может получить полные права доступа R_{wsj} к ресурсам данной рабочей станции, т.е:

$$\{R_1,R_2,...,R_n\} \cap R(u_i,ws_j) \neq \varnothing) => R_{wsj}. \qquad (2)$$

Доверенными субъектами рабочей станции ws_j являются такие субъекты u_i, для которых изначально заданы права $R(u_i,ws_j)$. Множество доверенных субъектов рабочей станции ws_j обозначим как U_{wsj}. Остальные субъекты из множества $U \backslash U_{wsj}$ для данной рабочей станции являются *недоверенными*.

Итак, узел nd_2 *непосредственно подчинен* узлу nd_1, если выполняется одно из следующих условий:

– nd_1 – сервер (маршрутизатор) домена, nd_2 – рабочая станция этого домена;

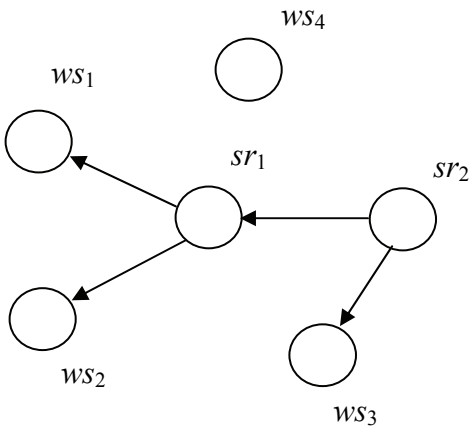
– nd_1 – сервер первого домена, nd_2 – сервер второго домена, который доверяет первому.

Таким образом, построим для РКС ориентированный граф подчиненности $G(N, L)$ узлов в РКС. В данном графе N – множество вершин (узлов); L – множество ребер.

Всем зарегистрированным узлам (серверам и рабочим станциям) РКС в графе $G(N, L)$ соответствует вершина, в которую входит только одно ребро и не выходит ни одного ребра в незарегистрированные узлы (вершины). Если узел не является членом данного домена, то в графе $G(N, L)$ ему соответствует изолированная вер-

шина. При этом $(nd_1, nd_2) \in L$ тогда и только тогда, если узел nd_2 непосредственно подчинен узлу nd_1, а узел nd_2 подчинен узлу nd_1 ($nd_1 \rightarrow nd_2$) тогда и только тогда, когда в графе $G(N, L)$ существует ориентированный путь от nd_1 до nd_2.

Покажем фрагмент графа подчиненности $G(N, L)$ узлов в РКС на рисунке.



Граф $G(N, L)$ подчиненности узлов в домене РКС

В данном графе: ws_1, ws_2 – рабочие станции первого домена; ws_3 – рабочая станция второго домена; ws_4 – рабочая станция – не член домена; sr_1 – сервер первого домена; sr_2 – сервер второго домена, которому доверяет первый сервер. Тогда

$$\{(sr_1, ws_1), (sr_1, ws_2), (sr_2, ws_3), (sr_2, sr_1)\} \in L .$$

В результате, наличие у субъекта u_i прав на рабочей станции ws_i определяет соответствующие права на рабочих станциях, подчиненных ей, т.е. для всех $ws_i \rightarrow ws_j$:

$$R(u_i, ws_i) => R(u_i, ws_j) . \quad (3)$$

Определим потенциальные угрозы РКС в рамках политики безопасного администрирования с использованием введенных выше параметров.

Угроза 1. Если субъект u_i может разместить ресурсы на рабочей станции ws_j, то существует угроза получения им полных прав доступа к данной рабочей станции, т.е.:

$$\{M(u_i, ws_j), R(u_i, ws_j) \neq \neq R_{wsj}\} => R(u_i, ws_j) = R_{wsj} . \quad (4)$$

Угроза 2. Обращение субъекта u_i к ресурсам рабочей станции ws_j содержит угрозу перехвата его прав доступа другим субъектом u_{i+1}, который имеет свои ресурсы на этой рабочей станции, т.е.:

$$\{A(u_i, ws_j): M(u_{i+1}, ws_j), R(u_{i+1}, ws_j) \neq R_{wsj}\} => R(u_{i+1}, ws_j) = R_{wsj} . \quad (5)$$

Отметим, что в РКС не все легальные субъекты являются доверенными по отношению к конкретной рабочей станции. Таким образом, необходимо учесть, что потенциально существует недоверенный субъект рабочей станции, который может разместить на ней свои ресурсы и реализовать угрозу 2.

Сформулируем **основной принцип** политики безопасного администрирования РКС с использованием введенных обозначений:

РКС удовлетворяет требованиям безопасного администрирования тогда и только тогда, когда выполняются условия 1, 2, 3 и 4.

Условие 1. При размещении субъектом u_i своих ресурсов на рабочей станции ws_i, необходимо, что бы он не имел возможности получения всех прав доступа к другой рабочей станции системы ws_j, т.е.:

$$\{M(u_i, ws_i), R(u_i, ws_i) = = R_{wsi}\} \neq > R(u_i, ws_j) = R_{wsj} . \quad (6)$$

Условие 2. При обращении субъекта u_i к рабочей станции ws_i другие субъекты u_j не должны получить права доступа к другой рабочей станции ws_j РКС, в том числе и к той, права доступа к которой он имеет (ws_i), т.е.:

$$\{A(u_i, ws_i), R(u_i, ws_i) = R_{wsi}\} \neq > \neq > \{R(u_j, ws_i) = R_{wsi} \,\&\, R(u_j, ws_j) = R_{wsj}\} . \quad (7)$$

Проверка условий 1 и 2 требует рассмотрения всех вариантов функционирования системы, что, в общем случае, представляет собой *NP*-полную задачу. Однако в практических приложениях достаточно отслеживать лишь те варианты, которые фактически реализуются в РКС.

Условие 3. Субъект u_i имеет возможность разместить свой ресурс на рабочей станции ws_j только в двух случаях:

- данной рабочей станции не подчинена ни одна другая рабочая станция;
- субъект является доверенным субъектом всех рабочих станций, подчиненных данной, т.е.:

$$\{(ws_j \nrightarrow ws_k), M(u_i, ws_j)\} \cup \{(ws_j \rightarrow ws_k), M(u_i, \forall\ ws_k)\} => M(u_i, ws_j). \quad (8)$$

Условие 4. Субъект u_i имеет возможность обратиться к рабочей станции ws_j только в том

случае, если все рабочие станции ws_k, доверенным субъектом которых он является, подчинены данной рабочей станции, т.е.:

$$\{(ws_j \rightarrow \forall\, ws_k), A(u_i, \forall\, ws_k)\} => A(u_i, ws_j). \quad (9)$$

Доказательства. Докажем необходимость выполнения условий 1, 2, 3 и 4 для безопасного администрирования РКС. Доказательство выполним методом от противного.

Вначале докажем, что условие 1 выполняется тогда и только тогда, когда выполняется условие 3. Докажем *необходимость* выполнения условия 3 для выполнения условия 1.

Пусть существует субъект u_i с правами $M(u_i,ws_j)$, для которого не выполняется условие 3, т.е. существует ws_k такая, что $ws_k \neq ws_j$, и при $ws_j \rightarrow ws_k$, субъект $u_i \notin U_{wsk}$, т.е. не имеет прав $M(u_i,ws_k)$.

Из определения угрозы 1 следует, что для субъекта u_i существует возможность получения прав $R(u_i,ws_j) = R_{wsj}$ к рабочей станции ws_j. Из (3) следует, что при наличии у субъекта u_i прав R_{wsj} при условии $ws_j \rightarrow ws_k$, он может получить права: $R(u_i,ws_k) = R_{wsk}$. Соответственно, если субъект u_i имеет права R_{wsk}, то как следствие, он также имеет право $M(u_i,ws_k)$. Таким образом, мы пришли к противоречию, что подтверждает необходимость выполнения условия 3 для выполнения условия 1.

Докажем *достаточность* выполнения условия 3 для выполнения условия 1.

Пусть имеются ws_j, ws_k, такие, что $ws_j \neq ws_k$, для которых не выполняется условие 1, т.е. $\{M(u_i,ws_j),\ R(u_i,ws_j) = R_{wsi}\} => R\ (u_i,ws_k) = R_{wsk}$. Таким образом, размещение субъектом u_i своих ресурсов на рабочей станции ws_j было использовано им для получения всех прав на рабочей станции ws_k. Поскольку $ws_j \neq ws_k$, то из (3) следует, что это возможно лишь в случае: $ws_j \rightarrow ws_k$, т.е. рабочая станция ws_j имеет в качестве подчиненных все рабочие станции ws_k, что противоречит условию 3, так как субъект u_i не является доверенным субъектом всех рабочих станций ws_k. Таким образом, выполнение условия 3 достаточно для выполнения условия 1.

Докажем, что условие 2 выполняется тогда и только тогда, когда выполняется условие 4.

Вначале докажем *необходимость* выполнения условия 4 для выполнения условия 2.

Пусть существует субъект u_i с правами $A(u_i,ws_j)$ по отношению к рабочей станции ws_j, для которого не выполняется условие 4, т.е. существует рабочая станция ws_k по отношению к которой субъект u_i в результате получает права $A(u_i,ws_k)$, но при этом $ws_j \not\rightarrow ws_k$.

Предположим, что существует субъект u_j с правами $R(u_j,ws_k) = R_{wsk}$. Тогда из условий 1 и 2, определения угрозы 2 и (5) следует, что субъект u_j имеет права $M(u_j,ws_k)$, но при $ws_j \not\rightarrow ws_k$ он не может иметь прав R_{wsk}, т.е. $R(u_j,ws_k) \neq R_{wsk}$, что противоречит приведенному выше предположению. Таким образом, условие 2 не выполняется ввиду того, что обращение субъекта u_i к рабочей станции ws_j не может быть использовано субъектом u_j для получения полных прав доступа на рабочей станции ws_k и выполнение условия 4 необходимо для выполнения условия 2.

Докажем *достаточность* выполнения условия 4 для выполнения условия 2.

Пусть существуют субъекты u_i, u_j и рабочие станции ws_j, ws_k такие, что $ws_j \neq ws_k$, для которых не выполняется условие 2, т.е.: имеются права $R(u_i,ws_j) = R_{wsj,}$, $R(u_j,ws_k) = R_{wsk}$, при этом реализовалась угроза 2 и обращение субъекта u_i к рабочей станции ws_j использовано субъектом u_j для получения всех прав доступа на рабочей станции ws_k. Но в соответствии с условиями 1 и 2 и определением угрозы 2: $R(u_j,ws_k) \neq R_{wsk}$ и, следовательно, с учетом (3) в этом случае: $ws_j \not\rightarrow ws_k$. Таким образом, полные права доступа $R(u_j,ws_k) = R_{wsk}$ к рабочей станции ws_k субъектом u_j могут быть получены в результате его простого обращения к рабочей станции ws_k или от другого недоверенного субъекта u_{j+1}, который несанкционированно получил соответствующие права доступа. Но в защищенной РКС не существует недоверенных субъектов, которые обладают полными правами доступа на какомлибо узле. Следовательно, в этом случае должно выполняться условие подчиненности $ws_j \rightarrow \rightarrow ws_k$, и тогда условие 4, наоборот, не выполняется, и подтверждается предположение о том, что выполнение условия 4 достаточно для выполнения условия 2.

Окончание на стр. 93.

Таким образом, предложенная модель позволяет формально определить правила доступа субъектов к объектам РКС, описать угрозы безопасности РКС и определить принципы и условия безопасного администрирования РКС.

Заключение. Наличие научно-обоснованной и формализованной политики безопасности – обязательное условие комплексной защиты распределенных компьютерных систем.

Предложенный элемент политики безопасности – модель безопасного администрирования доступа субъектов к объектам РКС – позволяет формализовать важный компонент системы защиты информации. Для эффективного внедрения разработанной политики информационной безопасности на основе предложенной модели дополнительно выполняются следующие мероприятия: корректировка стратегии и основных положений политики безопасности на всех ее уровнях; постоянное совершенствование системы реагирования на инциденты; повышение эффективности методов и средств аудита информационной безопасности.

1. *Шаньгин В.Ф.* Информационная безопасность компьютерных систем и сетей. – М.: ФОРУМ: ИНФРА–М, 2008. – 416 с.
2. *Barman S.* Writing Information Security Policies. – Boston: New Riders, 2002. – 342 p.
3. *Девянин П.Н.* Модели безопасности компьютерных систем. – М.: Академия, 2005. – 143 с.
4. *Галатенко В.А.* Основы информационной безопасности. – М.: УИТ, 2003. – 277 с.
5. *ISO*/*IEC* 27001:2005. «Information technology. Security techniques. Information security management systems. Requirements», 18 Oct. 2005. – 44 p.
6. *Peltier T.R.*. Information Security Policies. Procedures and Standards: Guideline for Effective Information Security Management. – Boca Raton: Auerbach Publ., 2002. – 176 p.
7. *Wood C.C.* Information Security Policies Made Easy. – Houston, Texas, USA: Pentasafe Security Technologies Inc., 2002. – 84 p.
8. *Application* of formal methods to the analysis of web-services security / L. Tobarra, D. Cazorle, F. Cuartero et al. // 2nd Intern. Workshop on Web Services and Formal Methods (WS-FM'05), Versailles, France, Sept. 2005. – P. 215–229.
9. *An Advisor* for Web Services Security Policies / K. Bhagavan, C. Fournet, A.D. Gordon et al. // Proc. of ACM Workshop on Secure Web Services (SWS'05), Fairfax, Virginia, USA, Nov. 2005. – P. 197–206.

Поступила 15.01.2010
Тел. для справок: (044) 406-8650 (Киев)
E-mail: *mukhin@comsys.ntu-kpi.kiev.ua*, *drang@ukr.net*