УДК 614.2

С.К. Варлатая, М.В. Шаханова

Анализ методов описания политики безопасности при разработке информационно-безопасных технологий

Проанализированы методы описания политики безопасности при разработке информационно-безопасных технологий построения вычислительных систем. Политика безопасности может быть разработана и описана с использованием формального и неформального метода. Выявлены достоинства и недостатки каждого из методов. Определены требования, предъявляемые к моделям безопасности.
Ключевые слова: политика безопасности, формальное и неформальное описание политики безопасности, модель безопасности.

Основой для организации процесса разработки информационно-безопасных технологий защиты информации является политика безопасности. Политику безопасности необходимо сформулировать для того, чтобы определить, от каких именно угроз и каким образом защищается информация в вычислительной системе.

Под политикой безопасности понимается набор правовых, организационных и технических мер по защите информации. Политика безопасности должна быть оформлена в виде специального документа (или комплекта документов), с которым должны быть ознакомлены все пользователи системы.

С одной стороны, политика безопасности информирует пользователей о том, как правильно эксплуатировать систему, с другой – определяет множество механизмов безопасности, которые должны существовать в вычислительной системе.

Политика безопасности вычислительной системы при разработке информационно-безопасных технологий может состоять из множества частных политик, направленных на конкретные аспекты защиты информации.

Политика безопасности может быть представлена на трех уровнях рассмотрения. При этом на каждом уровне рассмотрения описываются различные аспекты разработки политики безопасности [3].

На первом уровне разработка политики безопасности осуществляется руководством организации, для которой разрабатываются информационно-безопасные технологии. Здесь формируется так называемая «информационная политика безопасности». На этом уровне политика безопасности выражается в самых общих терминах. Объектом рассмотрения на данном уровне являются информация и процедуры управления, принятые в организации.

На втором уровне политика безопасности, сформулированная руководством организации, обычно раскрывается инженерами безопасности, имеющими более глубокие знания о вычислительном процессе, чем управляющие структуры организации. Объектом рассмотрения политики безопасности становятся пользователи системы, для которых система представляется как множество программ, выполняющих операции над вычислительными ресурсами. На этом уровне реализуются положения информационной политики безопасности организации при разработке информационно-безопасных технологий. Кроме того, здесь определяются непосредственно политика разграничения доступа и вспомогательные политики безопасности.

И наконец, на третьем уровне политика безопасности, определенная инженерами безопасности, непосредственно реализуется разработчиками информационно-безопасных технологий. Объектом политики безопасности являются процессы в системе, а вычислительная система рассматривается как множество сервисов, предоставляемых компонентами системы пользователям. На данном уровне идентифицируются компоненты, ответственные за обработку запросов пользователей [2].

Нужно отметить, что при уточнении политики безопасности в процессе ее разработки необходимо обеспечивать корректность реализации требований высокого уровня на более низком уровне рассмотрения. На каждом последующем уровне не должно создаваться новых политик безопасности, не описанных на предыдущем уровне, а все политики безопасности информационно-безопасных технологий, определенные на верхнем уровне, должны быть реализованы на нижнем уровне.

При разработке политики безопасности информационно-безопасных технологий следует руководствоваться следующими правилами:

1) Каждая операция, специфицированная политикой безопасности высокого уровня, должна поддерживаться политикой безопасности низкого уровня.

2) Ни одна из операций, разрешенных политикой безопасности низкого уровня, не должна быть забыта при описании политики безопасности высокого уровня.

Аргументация о соответствии интерпретаций политики безопасности на различных уровнях рассмотрения, так же как и само описание политики безопасности, может быть выражено с использованием следующих методов описания:

1. Естественный язык. К недостаткам данного способа относятся противоречивость и различные интерпретации положений политики безопасности. В связи с возможными противоречиями, вызванными неформальностью метода, в описании политики безопасности должны быть четко определены попытки нарушения безопасности.

2. Математическое формальное описание (на основе соответствующей математической модели). Уменьшает противоречивость естественного языка, позволяет использовать средства верификации политики безопасности. К недостаткам данного метода можно отнести сложность описания, что сужает круг людей, понимающих политику безопасности, понижая вероятность того, что политика безопасности будет корректно реализована.

3. Нематематическое формальное описание. Промежуточное решение, наследующее достоинства и недостатки описания с использованием естественного языка и математического формального описания.

Таким образом, политика безопасности может быть разработана и описана с использованием как формального, так и неформального метода.

Для неформальных способов описания политик при разработке информационно-безопасных технологий разграничения доступа широкое распространение получило описание правил доступа субъектов к объектам в виде таблиц, наглядно представляющих правила доступа. Обычно такие таблицы подразумевают, что субъекты, объекты и типы доступа для данной системы определены. Это позволяет составить таблицу в виде одной колонки для различных типов доступа, определенных в системе, и другой колонки, описывающей правила, регламентирующие доступ субъектов к объектам [4].

Описание поддерживающих политик безопасности целесообразно выполнять в форме списков, определяющих соответствующие требования.

Рассмотрим описание политики разграничения доступа некоторой организации при разработке информационно-безопасных технологий. На уровне управления организации описание политики разграничения доступа может быть сделано в следующей форме: «Информация при обработке и хранении должна быть защищена от неавторизованного раскрытия и модификации».

Для того чтобы сформулировать политику в форме высокоуровневых спецификаций разграничения доступа, необходимо описать свойства субъектов и объектов организации, а также возможные операции субъектов системы над объектами. Субъектов в системе можно охарактеризовать с помощью следующих понятий [5].

1. Степень доверия к субъекту – используется при доступе субъектов к информации с учетом классификации информационных ресурсов.

2. Необходимость доступа субъекта – атрибут указывает, что пользователь должен иметь доступ к информационному ресурсу.

3. Роль, исполняемая субъектом, – используется при описании функций пользователя системы и соответствующих полномочий этого пользователя.

4. Группы, к которым относится субъект, – используется при группировании пользователей с одинаковыми привилегиями.

В свою очередь, у объектов могут быть следующие характеристики:

1. Метка чувствительности объекта – используется при классификации информационных ресурсов. Корректная классификация ресурсов обеспечивает максимальную стоимость информации для организации. В данном примере вся информация, создаваемая пользователем, должна иметь одну из следующих категорий: «конфиденциальная», «для служебного пользования», «свободно доступная».

2. Идентификатор объекта – может использоваться для определения источника информации или ее владельца.

3. Метки и атрибуты объекта, используемые дискреционной политикой доступа (списки контроля доступа, биты защиты и др.).

В качестве основных операций, выполняемых субъектами системы над объектами, можно выделить следующие:

1) создание объектов и задание атрибутов доступа к ним; в том числе классификация объектов;

2) периодическая корректировка классификации объектов; классификация информационных ресурсов с течением времени уменьшается (конфиденциальная информация может стать информацией для служебного пользования, а информация для служебного пользования может со временем стать общедоступной); если пользователь, создающий информацию, знает дату корректировки классификации информации, он может сделать метку «Конфиденциальная до ...»;

3) уничтожение объектов;

4) чтение информации из объектов;

5) запись информации в объекты;

6) копирование объектов.

При описании ограничений на операции можно учитывать следующие внешние условия [2]:

1. Расположение – разрешение доступа может базироваться на положении (например, пользователь может получить доступ к некоторому информационному ресурсу только из офиса).

2. Время – разрешение доступа может базироваться на времени (например, пользователь может получить доступ к некоторому информационному ресурсу только в определенное время).

3. Другие условия.

Преимуществом такого способа представления политики безопасности является то, что она гораздо легче для понимания пользователями, чем формальное описание, так как для ее понимания не требуется специальных математических знаний. Это снижает вероятность атак на вычислительную систему по причине ее некорректной эксплуатации вследствие непонимания принципов разработки системы.

Основным недостатком неформального описания политики безопасности системы является то, что при такой форме представления правил доступа в системе гораздо легче допустить логические ошибки при проектировании системы и ее эксплуатации, приводящие к нарушению безопасности системы. Особенно это справедливо для политик безопасности нетривиальных систем, подобных распределенным вычислительным системам.

Необходимо отметить, что неформально могут быть описаны не только политики, но и модели безопасности. Примером неформального описания модели безопасности может служить модель Кларка–Вилсона.

Требование формального описания характерно для систем, область применения которых критична. В частности, можно отметить тот факт, что для защищенных выделительных систем высокой степени надежности необходимы формальное предоставление и формальный анализ системы. Практическое значение применения формальных методов при анализе систем заключается в возможности анализа всех реакций сложной программной системы.

В основе формального описания политики безопасности при разработке информационно-безопасных технологий лежит модель безопасности, или модель защиты. Примером формального описания модели безопасности может служить модель Белла и Лападула.

В соответствии с [1] модель защиты (безопасности) есть абстрактное (формализованное или неформализованное) описание комплекса программно-технических средств и (или) организационных мер защиты от несанкционированного доступа.

К модели безопасности должны предъявляться требования, общие для всех моделей: адекватность; способность к предсказанию; общность.

Для автоматизации процесса доказательства свойств системы используются так называемые «доказатели теорем» – программное обеспечение, проводящее формальную дедукцию на основе комбинации эвристик и непосредственного поиска. Другим видом программного обеспечения, используемого при формальном анализе систем, являются «контроллеры доказательств» – программы, предоставляющие пользователю возможность проводить последовательность шагов в процессе логических выводов о свойствах системы, но проверяющие корректность каждого шага. Естественно, самыми эффективными средствами формального анализа являются средства, сочетающие в себе свойства двух приведенных выше видов программного обеспечения.

Преимуществом формального описания является отсутствие противоречий в политике безопасности и возможность теоретического доказательства безопасности системы при соблюдении всех условий политики безопасности при разработке информационно-безопасных технологий.

С другой стороны, применение формальных методов для анализа систем, содержащих программное обеспечение, имеет недостаток, присущий всем методам моделирования: формальные методы имеют дело не с самой системой, а с ее моделью, которая может не отражать реальность или отражать ее неадекватно. Данная проблема может возникнуть вследствие использования модели, учитывающей не все факторы, оказывающие влияние на реальную систему. С другой стороны, излишняя подробность описания системы ведет к резкому росту временных затрат на проведение формального анализа и к неэффективности применения данного метода.

Таким образом, возникает задача корректного выбора уровня абстракции в описании модели безопасности. Под уровнем абстракции понимается множество требований к реальной системе, которые должны найти свое отражение в модели для адекватного отображения моделируемой системы [2].

Исходя из опыта работ в области безопасности с использованием формальных методов, существуют недостатки использования формальных методов и выявлены следующие проблемы:

1. Неразрешимость некоторых проблем безопасности с использованием формальных методов.

2. Использование формальных методов при разработке систем может привести к появлению систем, практическое использование которых весьма неудобно.

3. Использование формальных методов при разработке систем приводит к дорогостоящим и отнимающим много времени проектам.

4. Многие нарушения безопасности происходят вследствие некорректного использования пользователями компьютерных систем; даже в том случае, если в основу разработки системы заложена самая стойкая модель безопасности и устранены все каналы утечки информации, безопасность системы может быть нарушена в результате использования слабого пароля, оставленной слабости или ошибки реализации.

5. Модели безопасности часто не обеспечивают безопасности реальной системы; безопасность обеспечивается только в рамках формальной модели, которая часто бывает упрощенной; любой выход за пределы модели влечет нарушение безопасности.

Литература

1. Бурков В.Н. Модели и механизмы управления безопасностью / В.Н. Бурков, Е.В. Грацианский, С.И. Дзюбко, А.В. Щепкин. – М.: СИНТЕГ, 2001. – 160 с.

2. Корт С.С. Теоретические основы защиты информации: учеб. пособие / С.С. Корт. – М.: Гелиос АРВ, 2004. – 240 с.

3. Соколов А.В. Защита информации в распределенных корпоративных сетях и системах / А.В. Соколов, В.Ф. Шаньгин. – М.: ДМК Пресс, 2002. – 656 с.

4. Оценка безопасности информационных технологий. Общие критерии / А.П. Трубачев, М.Ю. Долинин, М.Т. Кобзарь и др. – М.: СИП РИА, 2002. – 356 с.

5. Шаханова М.В. Современные технологии информационной безопасности: учеб. пособие / М.В. Шаханова. – Владивосток: Изд-во ДВГТУ, 2007. – 217 с.

Варлатая Светлана Климентьевна
Канд. техн. наук, профессор, декан ФИКТ Дальневосточного Государственного Технического Университета (ДВПИ им. В.В. Куйбышева), г. Владивосток

Шаханова Марина Владимировна
Ст. преп. кафедры ЭКТ Дальневосточного Государственного Технического Университета (ДВПИ им. В.В. Куйбышева), г. Владивосток
Тел.: (4-232) 20-72-38, 8-914-735-70-19
Эл. адрес: marinavl2007@yandex.ru

S.K. Varlatay, M.V. Shakhanova

The analysis of methods of the description of the security policy by working out of information-safe tehnologies

In the present article methods of the description of a security policy are analysed by working out of information-safe technologies of construction of computing systems. The security policy can be developed and described with use formal and with use of an informal method. Merits and demerits of each of methods are revealed. The requirements shown to models of safety are defined.
Keywords: a security policy, the formal and informal description of a security policy, safety model.