УДК 681.3

ОПРЕДЕЛЕНИЕ ПОЛИТИК СЕТЕВОГО ДОСТУПА

А. Б. ДЕМУСЬКОВ
Гомельский государственный университет им. Ф. Скорины, Республика Беларусь

Одной из политик информационной безопасности предприятия является и политика сетевого доступа [1, 3].

Как показывает опыт, имеется два вида политики сетевого доступа, которые влияют на проектирование, установку и использование систем защиты, таких как брандмауэр. Политика верхнего уровня является концептуальной и она определяет:

– доступ к каким сервисам будет разрешен или явно запрещен из защищаемой сети;

– как эти сервисы будут использоваться;

– при каких условиях будет делаться исключение и политика не будет соблюдаться.

Политика нижнего уровня описывает, как система защиты должна на самом деле ограничивать доступ и фильтровать сервисы, которые указаны в политике верхнего уровня.

Существует ряд вариантов этой политики, которые можно реализовать:

– запрет доступа извне;

– неограниченный доступ в Internet;

– ограниченный входящий доступ;

– ограниченный выходящий доступ [3].

Политика проектирования брандмауэра [2, 3] как средства защиты в основном определяет политику сетевого доступа: чем строже политика проектирования брандмауэра, тем более строгой будет и политика сетевого доступа. Поэтому, прежде всего, нужно определиться с политикой проектирования брандмауэра.

Она специфична для конкретного брандмауэра. Нельзя разрабатывать эту политику, не понимая такие вопросы, как возможности и ограничения брандмауэра, угрозы и уязвимые места, связанные с TCP/IP. Как правило, реализуется одна из двух базовых политик:

– разрешить доступ для сервиса, если он явно не запрещен;

– запретить доступ для сервиса, если он явно не разрешен.

Брандмауэр, который реализует первую политику, пропускает все сервисы в сеть по умолчанию, если только этот сервис не был явно указан в политике управления доступом как запрещенный. Брандмауэр, который реализует вторую политику, по умолчанию запрещает все сервисы, но пропускает те, которые указаны в списке разрешенных сервисов. Вторая политика следует классической модели доступа, используемой во всех областях информационной безопасности.

Первая политика менее желательна, так как она предоставляет больше способов обойти брандмауэр, например, пользователи могут получить доступ к новым сервисам, не запрещаемым политикой (или даже не указанных в политике), или запустить запрещенные сервисы на нестандартных портах TCP/UDP, которые не запрещены политикой. Определенные сервисы, такие как X Windows , FTP, ARCHIE и RPC, сложно фильтровать, и для них лучше подходит брандмауэр, реализующий первую политику. Вторая политика строже и безопаснее, но ее тяжелее реализовать и она может повлиять на работу пользователей в том отношении, что ряд сервисов, такие, как описанные выше, могут оказаться блокированными или использование их будет ограничено.

Политика доступа к сервисам – самый важный компонент из четырех, описанных выше. Остальные три компонента используются для реализации политики. И, как отмечалось выше, политика доступа к сервисам должна отражать общую политику безопасности организации [2]. Эффективность системы брандмауэра при защите сети зависит от типа используемой реализации, от правильности процедур работы с ним, и от политики доступа к сервисам.

Теперь рассмотрим политику аутентификации удалённых пользователей.

Удаленные пользователи – это те пользователи, которые устанавливают соединения с внутренними системами откуда-либо из Internet. В любом случае для всех таких соединений должны использоваться меры усиленной аутентификации брандмауэра перед предоставлением доступа к внутренним системам. В политике должно быть указано, что удаленные пользователи не могут по-

лучать доступ к системам с помощью неавторизованных модемов. Не должно быть исключений для этого правила, так как даже один перехваченный пароль или один неконтролируемый модем может открыть «проход» в обход брандмауэра.

Такая политика имеет и недостатки:

– необходимо обучать пользователей пользоваться средствами усиленной аутентификации;

– расход средств на устройства аутентификации пользователей и администрирование удаленного доступа.

Но будет ещё большей глупостью установить брандмауэр и не контролировать удаленный доступ.

Помимо соединений через модемы политика должна регламентировать использование соединений с помощью протоколов SLIP и PPP. Пользователи могут использовать их для создания новых сетевых соединений внутри защищенной сети. Такое соединение потенциально является способом обхода брандмауэра, и может оказаться даже более опасным, чем коммутируемое соединение.

И наконец, для достижения положительных результатов от применения рассмотренных политик сетевого доступа необходимо, чтобы эти политики были не только декларированы, а доведены пользователю и наглядны. Политика организации – это средство довести позицию руководства в отношении компьютерной безопасности и явно указать, что оно ожидает от сотрудников, действий в тех или иных ситуациях и регистрации своих действий.

Для того чтобы быть эффективной, политика должна быть согласована с другими существующими законами, приказами и общими задачами организации. Она также должна быть интегрирована и согласована с другими политиками предприятия (например, политикой по приему на работу).

Список литературы

1 **Герасименко, В. А.** Основы защиты информации / В. А. Герасименко, А. А. Малюк. – М. : МИФИ, 1997. – 537 с.

2 Проблемы информационной безопасности в системе высшей школы : сб. науч. тр. X всероссийская науч. конф. – М. : МИФИ, 2003. – 256 с.

3 **Демуськов, А. Б.** Политики информационной безопасности предприятий / А. Б. Демуськов, В. А. Короткевич, Л. И. Короткевич // Известия Гомельского государственного университета им. Ф. Скорины. – 2003. – № 4 (19).

УДК 004.052.32+681.518.5

МОДЕЛИРОВАНИЕ РАБОТЫ САМОДВОЙСТВЕННЫХ КОМБИНАЦИОННЫХ УСТРОЙСТВ В УСЛОВИЯХ ВОЗНИКНОВЕНИЯ ОДИНОЧНЫХ КОНСТАНТНЫХ НЕИСПРАВНОСТЕЙ

Д. В. ЕФАНОВ, Т. С. ПОГОДИНА
Российский университет транспорта (МИИТ), г. Москва

При разработке и конструировании управляющих вычислительных комплексов применяются разнообразные методы обеспечения надежности и безопасности функционирования, так или иначе подразумевающие внесение в них избыточности (временно́й, информационной, структурной) по определенным принципам [1]. Важным является не только обеспечение выполнения объектом заданного управляющего алгоритма, но и возможности сохранения им таких свойств, как контролепригодность, самопроверяемость, отказоустойчивость, живучесть. В особенности это важно при использовании вычислительных комплексов в критических системах, к которым относятся и разнообразные системы управления, применяемые на транспорте [2].

Исследования [3–5] показывают, что достаточно большой класс контролепригодных устройств и систем образуют самодвойственные объекты автоматики и вычислительной техники. Свойство самодвойственности представления сигналов в них позволяет непрерывно контролировать их исправность при наличии временно́го ресурса для проведения процедур по тестированию. Вполне понятно, что не любое устройство является самодвойственным, однако существуют способы преобразования структур любых устройств к самодвойственному виду [3]. Таким образом, класс самодвойственных контролепригодных устройств является перспективным в решении задачи синтеза высоконадежной системы управления любым ответственным технологическим процессом.