КОМП'ЮТЕРНІ ЗАСОБИ, МЕРЕЖІ ТА СИСТЕМИ

УДК 681.324

Н.И. АЛИШОВ, М.И. ОГУРЦОВ, Ю.Н. ХАНЕНКО

АРХИТЕКТУРА РАСПРЕДЕЛЕННОЙ ПРОАКТИВНОЙ СИСТЕМЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Предлагается парадигма построения подсистемы защиты информации, основанной на принципе предупреждения возможных угроз и неисправностей – проактивном подходе. При этом на основе проведенного анализа и оценки существующих систем защиты разработан агентный принцип создания системы безопасности, позволяющий ей выполнять свои функции автономно, без вмешательства оператора. Защита интерфейсов, протоколов и услуг каждого уровня системы обработки информации даёт возможность дистанцироваться от конкретных типов угроз.

Введение. Вопросу безопасности телекоммуникационных сетей и систем посвящено множество статей, научных работ и исследований. Однако в этих работах мало уделяется внимания глобальным задачам построения систем защиты. В основном авторы концентрируются на решении какой-то конкретной проблемы или борьбе с отдельными уязвимостями [1–3]. Большинство работ по данной тематике посвящено оценке и анализу рисков, разработке модели нарушителя [4–6]. Полной и законченной теории создания систем безопасности информации на данный момент, к сожалению, не существует.

Только незначительная часть разработок в области компьютерных сетей направлена на проектирование систем, изначально являющихся защищёнными от достаточно большого множества как внешних, так и внутренних угроз [7]. Подобные системы называются проактивными (проактивный сервис, в основном, ориентирован не на устранение, а на предупреждение неисправностей и представляет собой совокупность стратегических мероприятий, которые должны обеспечить оптимальную и бесперебойную работу сети с учетом политики безопасности). Из разработок в области создания проактивных систем наиболее известны такие, как Virtual Private Net-works, Sunscreen, Kerberos и др. [8]. Проактивные системы опираются на семь базовых принципов [9]: связь с физическим миром; «глубокие» сетевые взаимодействия; макрообработка; функционирование в условиях неопределенности; предвидение; персонификация; замкнутый цикл управления.

Ориентация на системы, в которых человек не выполняет управляющую функцию, или на полностью автоматические системы – общая цель проактивных компьютерных систем организации безопасности корпоративных информационных ресурсов.

Анализ большого количества систем (проактивных и реактивных) показывает, что отсутствует системный подход к созданию средств защиты информационных ресурсов, следствием чего является неэффективность и ненадёжность существующих систем безопасности, нерациональное использование доступных ресурсов. В данной работе сделана попытка разработать концепцию и архитектуру системы, способной в фоновом режиме противостоять внутренним и внешним угрозам.

Представляется целесообразным прежде всего разработать чёткую классификацию систем безопасности и вычислительных систем вообще. Достаточно удобной, всеохватывающей, простой и универсальной является классификация систем с точки зрения их распределённости – централизованные и распределённые системы. Под распределённой вычислительной системой (РВС) понимают организационно-техническую систему, реализующую информационную технологию по принципу распределения информационных ресурсов, включая данные, средства для их обработки (аппаратные и программные), процессы и сведения о пользователях. Основным свойством РВС является её интеллектуальность – как системы в целом, так и её взаимодействующих между собой частей. Все компьютерные сети можно считать распределёнными вычислительными системами, однако следует различать физическую и логическую распределённость систем, а также распределённость в различных слоях функционирования, в том числе и в слое безопасности. Например, система Kerberos – централизованная с точки зрения архитектуры, но если рассматривать её на слое безопасности, игнорируя архитектуру, то очевидно, что она является распределённой – в защите от любой атаки принимают участие не только атакуемый элемент, но и другие элементы системы (KDC). Эталонная семиуровневая модель взаимодействия компьютерных систем – архитектура OSI – предопределяет распределённость созданных на её основе систем [10]. Возможны любые комбинации архитектурных и логических распределённости и централизованности различных вычислительных сетей.

Основные функции любой вычислительной системы – ввод/вывод, преобразование, хранение и передача информации. В распределённых системах это организуется только через межклиентное сетевое взаимодействие, что усложняет их защиту и достижение безопасности информационных ресурсов (состояние, при котором обеспечивается выполнение функций обработки данных, взаимодействия и защиты или самозащиты). Таким образом, в РВС защита тоже должна быть распределённой.

Постановка задачи. Базовая модель функционирования распределённых систем – эталонная модель взаимодействия открытых систем (ВОС), сутью которой являются семь уровней с набором протоколов, услуг и интерфейсов (возможны ещё и компоненты), при этом каждый уровень имеет свои услуги, прото-

колы, интерфейсы и компоненты [11]. Используя эти уровни, можно реализовать работу любых программных надстроек, и именно через эти услуги, интерфейсы и протоколы злоумышленникам удаётся нанести системе ущерб, ведь, фактически, иного пути для атаки на телекоммуникационную систему не существует. Следовательно, угрозы конфиденциальности, целостности и доступности интерфейсов, протоколов и услуг являются наиболее обобщённым видом угроз, и универсальность проектируемых систем защиты может быть основана именно на этой не конкретной, а обобщённой угрозе. Для подобной системы не будет иметь значения, какие конкретно атаки организуются на телекоммуникационную систему – они априори будут неэффективны.

С другой стороны, нельзя загружать сетевой трафик, нужен компромисс, поэтому предлагается в каждый уровень инкапсулировать интеллектуальные агенты безопасности, функционирование которых, как правило, происходит в фоновом режиме [12].

Наилучшей организацией архитектуры подсистемы безопасности, использующей семиуровневую модель ВОС, является глубоко распределённая система защиты информации (эшелонированная защита). По аналогии с моделью ВОС она строится многоуровневой, для всех элементов системы каждый уровень имеет свои услуги, интерфейсы и протоколы (рис. 1). Он будет взаимодействовать с выше- и нижерасположенными уровнями, как и в модели ВОС, а также с компонентами однорангового уровня систем безопасности других защищаемых объектов.

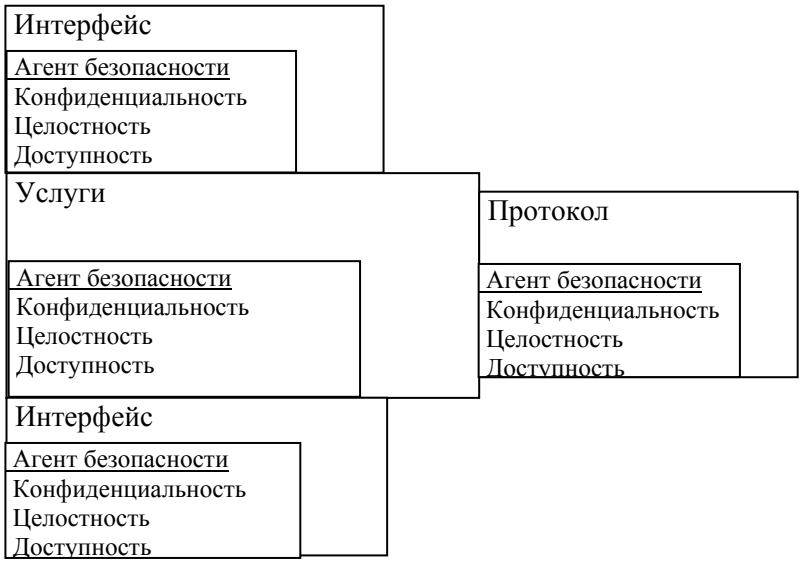

РИС. 1. Атомарный компонент подсистемы безопасности информации

Методы решения задачи. Угрозы существуют на всех уровнях модели ВОС, а, следовательно, лишь абстрагировавшись от конкретных типов угроз, обеспечивая защиту интерфейсов, протоколов и услуг каждого уровня, можно обезопасить систему. Подобное решение может стать одним из лучших в обеспечении безопасности сетевого периметра.

Рассмотрим, что означают конфиденциальность, целостность и доступность для интерфейсов, протоколов и услуг. Каждый протокол имеет свои особенности, но в любом случае должен обеспечивать взаимодействие как минимум двух объектов (в этом его концептуальное отличие от алгоритма – чёткой последовательности операций, приводящей к выполнению поставленной задачи из достаточно большого класса однотипных задач, но без взаимодействия). Следовательно, для всех протоколов обобщающим является их предназначение – обеспечение взаимодействия, и агент безопасности в данном случае ответственен за конфиденциальность, целостность и доступность этого взаимодействия. Интерфейсов также существует много, они представляют собой правила доступа к услугам. Следовательно, общим для них будет обеспечение конфиденциальности, целостности и доступности правил доступа к услугам. Основной функцией всех услуг является предоставление кому-либо каких-либо ресурсов (в том числе и возможностей). Тут обеспечение безопасности – это защита ресурса от неправомерного доступа и/или использования, от подмены либо повреждения/уничтожения.

За основу подсистемы безопасности целесообразно выбрать агентную технологию. Каждый агент будет действовать с учётом реальной ситуации на подотчётном ему участке (мониторинг в фоновом режиме). При этом он является интеллектуальным, способным действовать независимо от других агентов, хотя и связанным с ними. Если возникло нарушение безопасности, которое можно разрешить на месте, то оно будет немедленно исправлено агентом безопасности, без его связи с другими агентами либо с контролирующим центром (полное разветвление служб безопасности). Под агентом тут подразумевается сущность, обладающая способностью к формулированию целей, обучению, планированию и принятию решений в окружении, которое динамично изменяется. Назначение агентов – упростить и улучшить взаимодействие пользователей со сложными программными системами в слабоструктурированной динамично изменяющейся распределенной среде путем адаптации к особенностям конкретного пользователя. Агент, в отличие от традиционных программ, способен не только взаимодействовать с этой средой, получая от неё информацию через свои сенсоры, влияя на среду с помощью своих эффекторов, но и изменять свое поведение, обучаясь на собственном опыте.

Для реализации своих функций агент должен обладать, по крайней мере, четырьмя возможностями [13]:

- поддерживать взаимодействие с окружающей средой, получая от нее информацию и реагируя на эту информацию своими действиями;
- проявлять собственную инициативу;

• посылать и получать сообщения от других агентов;

• действовать без вмешательства извне.

Как правило, агентов не программируют для выполнения конкретной работы, а обучают на примерах. Агенты, имеющие высокий уровень интеллектуальности, способны самостоятельно учиться на собственном опыте.

Основные свойства программного агента:

• *автономность* – агент выполняет значительную часть своей работы автономно, не взаимодействуя с человеком или другими агентами;

• *коммуникабельность* – агент умеет общаться с пользователем, получая от него задачу и предоставляя результаты;

• *адаптивность поведения* – в процессе общения с пользователем агент умеет настраиваться на его личные привычки и методы работы;

• *рациональность поведения* – агент своими действиями должен продвигаться к решению поставленной задачи и не выполнять действия, препятствующие этому процессу. Если агент на основе своих знаний считает, что определенное действие приблизит его к поставленной цели, то он может выполнить это действие. Но это действие может и не привести его к цели, если информация, на основе которой агент принял решение, была неверной или неполной. Таким образом, решение агента о целесообразности выполнения действий зависит от имеющейся информации и средств ее обработки;

• *восприимчивость* – агент, который находится в информационной среде, воспринимает определенным образом изменения окружающей среды и может реагировать на эти изменения;

• *проактивность* – агент должен не только выполнять текущую задачу, но и собирать при этом потенциально полезную для пользователя информацию, накапливая ее в своей базе данных.

Если проблема не может быть разрешена агентом, обнаружившим её, необходимая информация будет немедленно передана тем компонентам системы защиты, которые способны исправить ситуацию. Такой подход позволит сократить трафик, используемый для обеспечения безопасности, но при этом общий уровень защиты телекоммуникационной системы повысится, так как каждая услуга, интерфейс, протокол и, возможно, компонент каждого уровня эталонной модели ВОС будут защищены собственными агентами безопасности с учётом их индивидуальных специфических особенностей. Одни инкапсулированные компоненты в фоновом режиме будут контролировать целостность системы, другие – следить за соблюдением порядка доступа, правильностью проверки подлинности абонентов системы, обеспечивать конфиденциальность передаваемой по сетевым коммуникациям информации. Конечно, некоторая часть аппаратных мощностей при этом будет расходоваться на их функционирование, но это малая цена за построение максимально защищённой информационно-телекоммуникационной системы.

Использование в системе безопасности агентов, работа которых основана на принципе проактивности, минимизирует возможности злоумышленников, при

этом уменьшая нагрузку на администратора безопасности. Дополнительный эффект даст ранее предложенная инкапсуляция агентов на каждом уровне модели OSI (рис. 2).

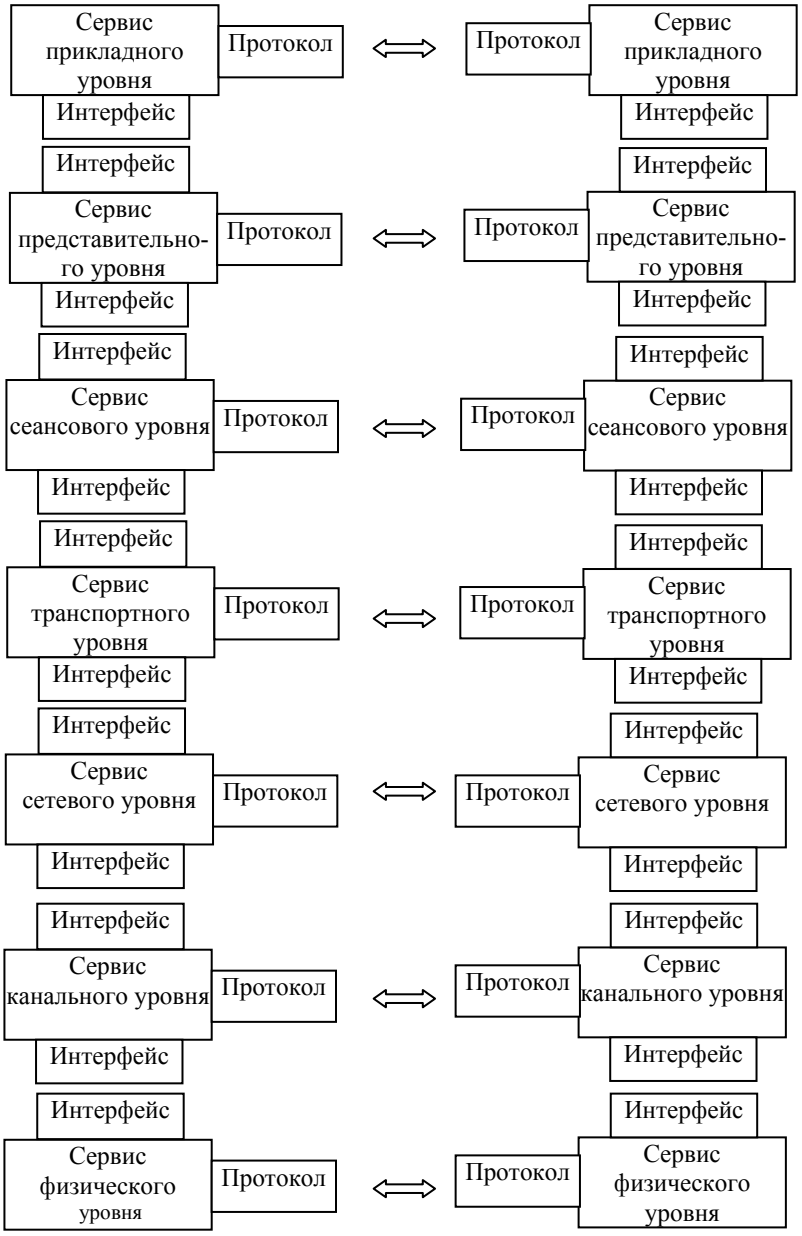

РИС. 2. Инкапсуляция агентов безопасности на каждом уровне модели ВОС

Рассмотрим особенности построения предлагаемой системы безопасности.

1. Отдельные элементы данной системы уже существуют. Это доказывают примеры систем безопасности, приведенные в первой части статьи. Кроме того, проактивно защищённые системы используются, например, в банковском деле – при банковских переводах через телекоммуникационные сети общего назначения (Internet).

2. Система должна быть распределённой, т. е. реализующей информационную технологию на основании распределения информационных ресурсов. РВС включает данные, средства для их обработки, активные компоненты. Информационными ресурсами РВС являются обрабатываемые данные, программное обеспечение, информационные составляющие аппаратного обеспечения и сведения о пользователях, сюда же следует включать различные агенты, в том числе агенты безопасности. Политика безопасности – множество правил, контролирующих порядок обработки информации, взаимодействия подсистем и обеспечения защиты, – определяет безопасность РВС и архитектуру системы защиты. При этом распределённость РВС ведёт к росту уязвимости её информационных ресурсов и расширению множества угроз безопасности. С точки зрения агентного подхода угрозы безопасности также следует считать агентами либо мультиагентными системами (при распределённой угрозе), абстрагируясь от дестабилизирующих факторов различной природы (аппаратных, программных, пользовательских и др.).

3. Безопасность РВС – такое состояние информационной мультиагентной среды, при котором в условиях влияния дестабилизирующих факторов (угроз безопасности) обеспечивается выполнение функций обработки данных, межагентного взаимодействия и защиты (самозащиты). Защита – неотъемлемое, внутреннее свойство РВС. Система состоит из компонентов (интеллектуальных подсистем), реализующих общую политику безопасности (рис. 3). Организация безопасности включает функции, агенты и механизмы безопасности (агенты реализуют функции посредством механизмов).

4. РВС – многоуровневая самоподобная система; каждый её компонент представляет собой многокомпонентную систему, и так далее, вплоть до минимальной системной ячейки – концептуальной единицы (атомарного компонента) [14]. Структура системы безопасности совпадает со структурой РВС. Результатом является декомпозиция политики безопасности, её функций и механизмов, критериев оценки состояния отдельных агентов и всей мультиагентной среды (в реальном времени). При этом устанавливается строгая иерархия управления безопасностью.

Система программно независима. Более того, с точки зрения архитектуры агенты, обеспечивающие конфиденциальность, целостность и доступность услуги, интерфейса, протокола одного уровня, аналогичны подобным агентам всех других уровней (см. рис. 2). Они будут обеспечивать защиту непрерывно, с момента возникновения телекоммуникационной системы и в течение всего её дальнейшего жизненного пути в реальном режиме времени. В центре системы находится центральный узел обеспечения безопасности, связанный со всеми

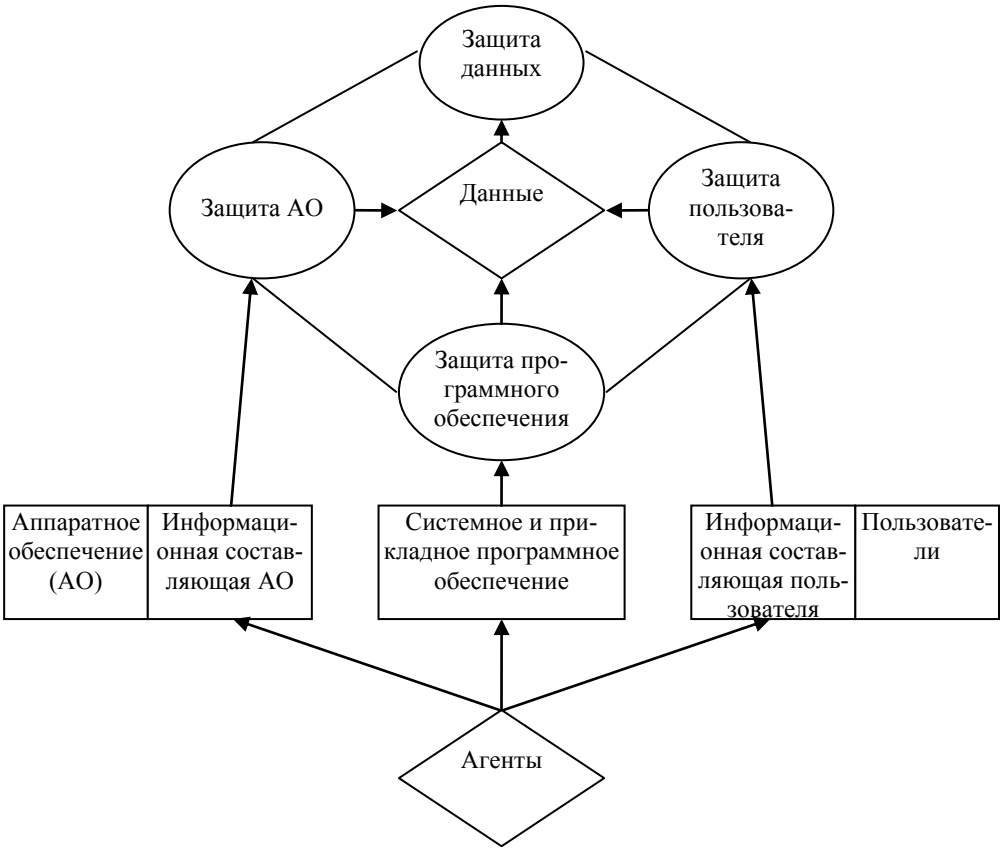

РИС. 3**.** Мультиагентная модель защищённой вычислительной системы

агентами (не постоянно, только при изменении параметров либо при необходимости вмешательства) (рис. 4). При этом именно узлы сети и её коммуникации являются сутью системы безопасности.

Заключение. Несомненно, системы безопасности, в которых реализован предлагаемый подход, сначала будут крайне дорогими. С другой стороны, для сетей, где циркулирует более ценная, чем аппаратное и программное обеспечение телекоммуникационной системы, информация (например, секретная или совершенно секретная, разглашение которой может нанести серьёзный ущерб государству, обществу, юридическим либо физическим лицам), их применение будет оправдано. Вместе с тем очевидно, что данный подход значительно более выгоден как с экономической точки зрения, так и с точки зрения простого и прозрачного администрирования, изменения структуры и собственно безопасности. Предлагаемая мультиагентная распределённая система безопасности является интеллектуальной, физически однородной, корпоративной (самоорганизующейся), самоподобной, легко поддающейся интеграции и дифференциации. Соз-

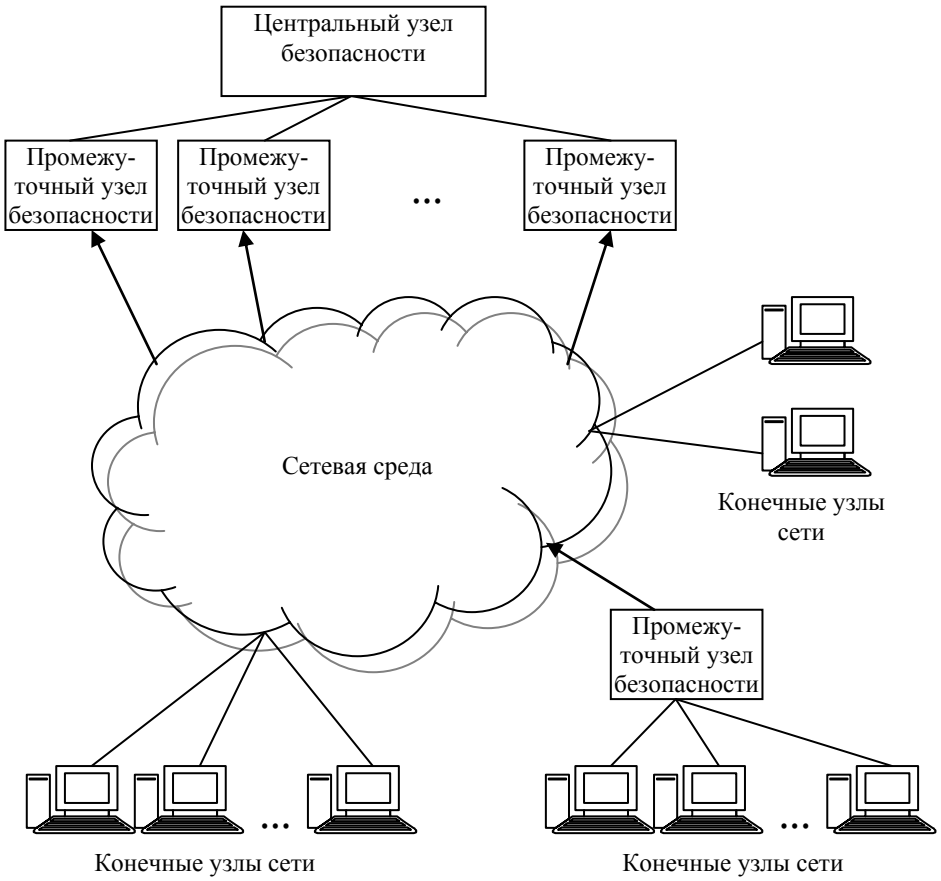

РИС. 4. Архитектура распределённой проактивной системы безопасности

дание такой проактивной системы требует вложения значительных средств, но в дальнейшем эти вложения минимизируются. При этом очевидно, что уровень защищённости на всём жизненном пути проактивной системы превышает уровень безопасности реактивной.

1. *Александров А.* Грамотная защита информационных потоков. – http://www.bytemag.ru/Article.asp?ID=2640
2. *Зорин В.* Архитектура защищенного портала – http://www.bytemag.ru/ Artcle.asp?ID=2449
3. *Гриняев С.* Ставка на особо защищенные информационные системы. – http://www.bytemag.ru/Article.asp?ID=836
4. *Компьютерные* сети и сетевые технологии: Пер. с англ. / М. Спортак, Ф. Паппас, Р. Пит и др – Киев.: ООО «ТИД «ДС», 2002. – 736 с.
5. *Хорошко В.А., Чекатков А.А.* Методы и средства защиты информации. – Киев.: Юниор, 2003. – 504 с.

6. *Домарев В.В.* Безопасность информационных технологий. Методология создания систем защиты. – К.: ООО «ТИД «ДС», 2001. – 688 с.
7. *Лукацкий А.* Сетевая контрразведка: как обнаружить сканирование узлов и портов. – http://www.bytemag.ru/Article.asp?ID=251
8. *Рассел Кей.* Kerberos. Computerworld, № 30/2000 12.08.2000 – http://www.osp.admin.tomsk.ru/cw/2000/30/index.htm
9. *Рой Вонт, Тревор Перинг, Дэвид Тенненхаус*. Адаптивные и проактивные компьютерные системы // Открытые системы. – 2003. – № 10 – http://www.osp.ru/os/2003/ 10/010.htm
10. *Олифер В.Г., Олифер Н.А.* Компьютерные сети. Принципы, технологии, протоколы. – СПб.: Питер, 2002. – 672 с.
11. *Дей Д.Д., Зиммерман Ю.* Эталонная модель взаимосвязи открытых систем (ВОС) // ТИИЭР. – 1983. – **71**, № 12. – С. 8–16.
12. *Алишов Н.И.* Архитектура подсистемы защиты информации телекоммуникационной системы передачи информации // Перспективные средства вычислительной техники и информатики. – Киев: Ин-т кибернетики им. В.М. Глушкова НАН Украины, 1999. – С. 141–147.
13. *Клышинский Э.С.* Некоторые аспекты построения агентных систем. – http://pmg.org.ru/russian/
14. *Алишов Н.И.* Организации безопасности информационных ресурсов в системах телекоммуникаций // Тр. IV Междунар. науч.-техн. конф. по телекоммуникациям "Телеком-99". – Одесса , 1999. – С. 112–115.

Получено 26.04.2005