УДК 004.652.4

05.00.00 Технические науки

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ ЭКСПЕРТНЫХ СИСТЕМ ДЛЯ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Кучер Виктор Алексеевич
к.т.н.

Магомадов Алексей Сайпудинович
д.т.н.

Чигликова Надежда Дмитриевна
к.т.н

Дьяченко Роман Александрович
д.т.н
Кубанский государственный технологический университет, Краснодар, Россия

Статья посвящена применению технологии экспертных систем в целях контроля правильности работы программных средств и баз данных. Отмечается, что главными вопросами управления безопасностью в критических информационных системах является процесс наблюдения и сбора информации в вычислительной среде. Результаты наблюдения должны оцениваться и обрабатываться экспертом по безопасности, а затем фиксироваться в базе знаний экспертных систем. Один из возможных вариантов управления безопасностью распределенной вычислительной сети – создание машины безопасности. Она позволит обеспечить: минимальное время реакции системы на внешние возмущения; достоверность аудита, защищенного *S*-интерфейсом и независимость процесса принятия решения от состояния контролируемых элементов информационных систем. После того, как агент полностью выработал свой ресурс, он уничтожается и заменяется новым. Такой механизм старения обеспечивает защиту агента от изучения и от внешних атак

Ключевые слова: КРИТИЧЕСКИЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ, БАЗЫ ДАННЫХ, ЭКСПЕРТНАЯ СИСТЕМА, ПРОГРАММНЫЕ АГЕНТЫ, МАШИНА БЕЗОПАСНОСТИ

UDC 004.652.4

Technical sciences

USING TECHNOLOGIES OF EXPERT SYSTEMS FOR SECURITY IN INFORMATION SYSTEMS

Kucher Victor Alekseevich
Cand.Tech.Sci.

Magomadov Alexei Saipudinovich
Dr.Sci.Tech.

Chiglikova Nadezhda Dmitrievna
Cand.Tech.Sci.

Dyachenko Roman Aleksandrovich
Dr.Sci.Tech.
Kuban State Technological University, Krasnodar, Russia

The article is devoted to the expert systems technology using to monitor the correct operation of the software and databases. It is noted that the main issues of security management in critical information systems is a process of observation and collection of information in a computing environment. Observation results should be evaluated and processed by an expert on security and then recorded in the database of expert systems. One of the possible options for security management of distributed computing network - creating a security machine. It will ensure: minimum response time to external perturbations; the accuracy of the audit protected by S-interface and independent decision-making process of the state of the controlled elements of information systems. After that, the agent is completely worn out; it is destroyed and replaced by a new one. This aging mechanism protects agent from analyzing and from external attacks

Keywords: CRITICAL INFORMATION SYSTEMS, DATA BASES, EXPERT SYSTEM, PROGRAM AGENT, SECURITY MACHINE

Известно, что одна из наиболее сложных проблем в информатизации современного общества является необходимость обеспечения безопасности применения информационных технологий

(ИТ), программных средств (ПС) и баз данных (БД) для обработки конфиденциальной информации, циркулирующей в информационных системах (ИС) критических объектов. Отметим также, что к таким объектам относятся атомные станции, военные объекты, экологически опасные производства, объекты транспорта, связи и др.

Среди различных способов защиты информации в таких ИС выделяется система с контролем правильности работы ПС и БД с учетом ограничений, накладываемых на приложения технологией, а также с учетом организации вычислительного процесса.

Следует отметить, что в настоящее время одним из перспективных направлений обеспечения безопасности критических ИС и контроля правильности работы ПС, БД является применение технологии экспертных систем (ЭС).

Из публикаций [1-3] известно, что значительная часть ИС имеет сетевую распределенную иерархическую структуру. Ее вычислительная среда задается набором состояний, переходы между которыми определяются изменениями потребления существующих в ней информационных ресурсов. При этом в каждый фиксированный момент времени состояние вычислительной среды ИС характеризуется множеством активных процессов, связями между ними и потребляемой информацией этими процессами. Если ИС детерминирована (имеют место повторяющиеся процессы), то становится возможным применение технологии ЭС в задачах обеспечения безопасности информации.

Основным вопросом при решении этих задач является разработка рациональной схемы управления процессами, обеспечивающими эту безопасность. Под управлением безопасностью будем понимать процесс

целенаправленного воздействия на ИС, в результате которого ИС должна выполнять поставленную перед ней цель в условиях противодействия внутреннего и внешнего злоумышленника. Задача управления безопасностью ИС может быть задана четверкой:

$$<X, I, M\text{пр}, C\text{у}> ,$$

где X – управляющее воздействие на ИС; *I* –информация состояния элементов ИС; *M*пр – механизм принятия решения, реализующий алгоритм управления для достижения заданной цели управления *C*у. Элементы *X, I, M*пр зависят от объекта управления и, конечно же, они определяются при наличии модели объекта.

Первостепенными вопросами управления безопасностью в критических ИС являются процесс наблюдения и сбора информации за вычислительной средой. К ним же относятся контроль выполнения процессов на рабочих станциях, средствах телекоммуникации, подключенных программных и аппаратных средств защиты. Результаты наблюдения должны оцениваться и обрабатываться экспертом по безопасности, а затем фиксироваться в базе знаний ЭС.

Режим системы наблюдения и контроля разделяется на два этапа: первый – накопление информации для обучения и сам процесс обучения базы знаний, второй – работа системы на базе полученных знаний, и оценка правильности работы вычислительных процессов.

Наблюдения и сбор информации о состоянии объектов ИС осуществляется программными агентами, встраиваемыми в интерфейсы операционных систем, средств телекоммуникаций и другого оборудования. По результатам работы агентов формируется аудит, который анализируется и обрабатывается ЭС. ЭС по аудиту

устанавливает соответствие поведенческой модели системы допустимой модели, заявленной в политике безопасности по требованиям безопасности ИС. Все случаи несоответствия предъявляются эксперту для принятия решения. При этом, если пропущенное решение оказалось правильным, то ЭС может дообучаться, а ее база знаний корректироваться.

В публикациях по безопасности ИТ [4,5] выделяют две концептуальные схемы управления информационными системами:

1) Используются агенты наделенными элементами интеллекта, выполняющие некоторые функции ЭС, связанные с первоначальным анализом и логическим выводом по данным аудита.

2) Используются последовательные агенты, выполняющие только фиксацию и передачу событий о состоянии вычислительной среды для принятия решения.

Первая схема содержит существенный недостаток с учетом фактора информационной безопасности. В этом случае механизм принятия решения *М*пр находится в одной среде с контролируемыми ПС и БД. Он может быть подвержен нападению со стороны злоумышленника как извне ИС, так и изнутри системы через программное обеспечение. В результате такого нападения управляющие воздействия *X* будут неадекватными состоянию ИС.

Вторая схема значительно безопаснее, так как механизм принятия решения *М*пр изолирован от ПС. Однако при такой схеме актуальным становится вопрос достоверности аудита, поступающего от агента.

И в первом и во втором случае недостатки агентов могут быть значительно уменьшены. Необходимо организовать передачу информации между агентами отдельной выделенной машиной через *Security* интерфейс (*S*-интерфейс). Такую машину можно назвать машиной безопасности (МБ).

Схема управления безопасностью, описанная выше для распределенной вычислительной сети, показана на рисунке 1. МБ будет присутствовать в каждой локальной вычислительной сети (ЛВС). Она имеет выход во внешние сети, что значительно повышает скорость обмена аудитом от каждого элемента ЛВС.

Реализация МБ на практике позволяет обеспечить:

1. Минимальное время реакции системы на внешние возмущения.
2. Достоверность аудита, защищенного *S*-интерфейсом.
3. Независимость процесса принятия решения от состояния контролируемых элементов ИС.

Сигналы обработки аудита с каждой МБ поступают на МБ администратора безопасности (рабочее место эксперта), который по результатам изучения аудита может дообучить базу знаний ЭС, заменить скомпрометированного агента на одном из контролируемых устройств.

Разумеется, в описанной схеме должны быть предусмотрены мероприятия для защиты самого агента: защита кода агента, распределение его по диску рабочей станции, контроль целостности резидентной части агента, запрещение всех процедур обмена

информацией с кодом агента и аудитом и др.

Должен вестись также учет всех сеансов работы агентов и истории их старения. Агент стареет быстрее при фактах несанкционированного доступа (НСД) к ресурсам технологического процесса. Каждое событие НСД или событие, требующее внимания эксперта для его уточнения и квалификации, имеют свои оценки. Эти события накапливаются.

После того, как агент полностью выработал свой ресурс, он уничтожается и заменяется новым. Такой механизм старения обеспечивает защиту агента от изучения и от внешних атак. Чем больше накопленный уровень нештатных ситуаций на станции, тем больше вероятность того, что агент будет подвержен злонамеренному воздействию и тем быстрее он должен быть заменен.

В течение определенного интервала времени в результате работы описанной ЭС может быть накоплено достаточное количество инцидентов, которые должны быть использованы экспертом для дообучения базы знаний ЭС. Таким образом, это дает возможность в случае возникновения внештатных ситуаций добиться приемлемого для практического использования времени реакции системы.

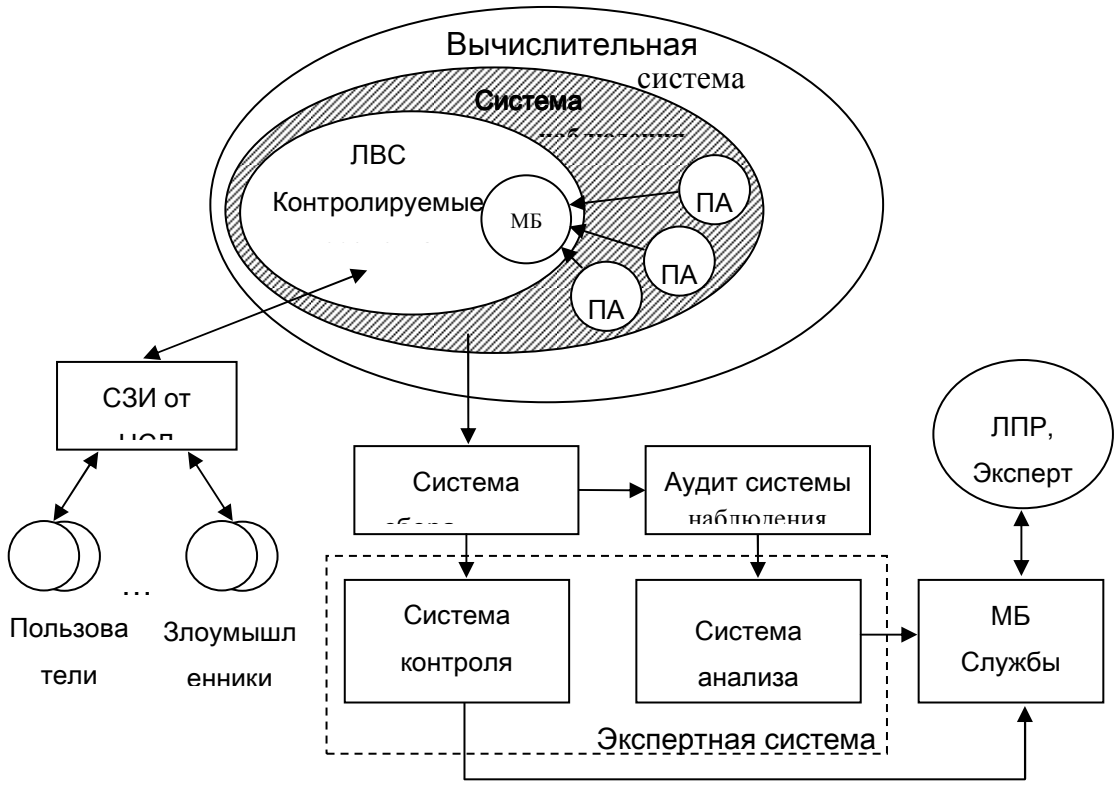

Рисунок 1 – Схема организации управления безопасностью в распределенной вычислительной среде

Литература

1. Андрианов В.В., Овчаров А.С., Пучков В.Г. «Возможности применения технологии экспертных систем в приложениях безопасности» //Специальная техника средств связи. Серия системы, сети и технические средства конфиденциальной связи». Пенза: ПНИЭИ, 1997, С. 17-21.
2. Гук М. Аппаратные средства локальных сетей. Энциклопедия. СПб., 2002 С. 457-469.
3. Брайдо В.Л. Вычислительные системы, сети и телекоммуникации. СПБ., 2002, С. 625-644.
4. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. СПБ., 2002, С. 583-630.
5. Ухлинов Л.П. Управление безопасностью информации в автоматизированных системах. М., 1996, С. 29-39.

References

1. Andrianov V.V., Ovcharov A.S., Puchkov V.G. «Vozmozhnosti primenenija tehnologii jekspertnyh sistem v prilozhenijah bezopasnosti» //Special'naja tehnika

sredstv svjazi. Serija sistemy, seti i tehnicheskie sredstva konfidencial'noj svjazi». Penza: PNIJeI, 1997, S. 17-21.

2. Guk M. Apparatnye sredstva lokal'nyh setej. Jenciklopedija. SPb., 2002 S. 457-469.
3. Brajdo V.L. Vychislitel'nye sistemy, seti i telekommunikacii. SPB., 2002, S. 625-644.
4. Olifer V.G., Olifer N.A. Komp'juternye seti. Principy, tehnologii, protokoly. SPB., 2002, S. 583-630.
5. Uhlinov L.P. Upravlenie bezopasnost'ju informacii v avtomatizirovannyh sistemah. M., 1996, S. 29-39.