Информационные технологии

ПРОТОТИП СИСТЕМЫ ВЫЯВЛЕНИЯ И АНАЛИЗА НЕТИПИЧНЫХ СОСТОЯНИЙ В ФУНКЦИОНИРОВАНИИ СЕТЕВОЙ ИНФРАСТРУКТУРЫ
THE PROTOTYPE OF SYSTEM OF DETECTION AND ANALYSIS OF ATYPICAL STATES IN THE FUNCTIONING OF THE NETWORK INFRASTRUCTURE

Г.В. Бабенко
G.V. Babenko
Администрация Губернатора Астраханской области
Astrakhan region Governor's administration

The most important attribute of our time is the global information integration, based on the construction of computer networks using the Internet.

Today, large amounts of data are transmitted using network technologies, so the important point in the information security is the security of networking computer systems.

This paper presents a prototype of the system analysis and control the flow of information networking based on the principle of detecting abnormalities in the functioning of the components of the network infrastructure

Важнейшим атрибутом нашего времени является глобальная информационная интеграция, основанная на построении компьютерных сетей масштаба предприятия и их объединении посредством сети Internet.

Большие объемы данных передаются с использованием сетевых технологий, поэтому важным моментом в защите информации является обеспечение безопасности, именно, сетевого взаимодействия компьютерных систем.

По требованиям безопасности сегодня в компьютерных сетях применяются системы антивирусного контроля, системы обнаружения атак и вторжений, либо аналогичные им по функциональному назначению и возможностям.

Существующие системы защиты в большинстве своем используют для распознавания атак сетевой или системный подход [3]. В том и другом случае эти системы осуществляют поиск известных разработчикам сигнатур атак, в качестве которых используются специфические шаблоны враждебных действий.

Исходя из этого, необходимым условием обеспечения безопасности компьютерной системы является использование подсистем обнаружения подозрительных аспектов в функционировании системы, которые позволяют своевременно определять инциденты информационной безопасности и реагировать на них, не имея четких сигнатурных описаний. Для разработки системы выявления и анализа таких состояний необходимо скомпилировать в единую модель принцип модульности, а так же сетевой и системный подход при определении нарушений

безопасности информации в компьютерной сети с использованием компонентонезависимых методов анализа информации, что значительно увеличит надежность системы и обеспечит корректность результатов анализа.

Функциональная схема системы

При создании прототипа системы была выбрана схема, реализующая принцип модульности систем [2]. Данная схема предоставляет неограниченные возможности развития и адаптации к изменяющимся параметрам среды, позволяя изменять функционал системы под определенные требования, при дальнейшем ее совершенствовании и модернизации (рис. 1).

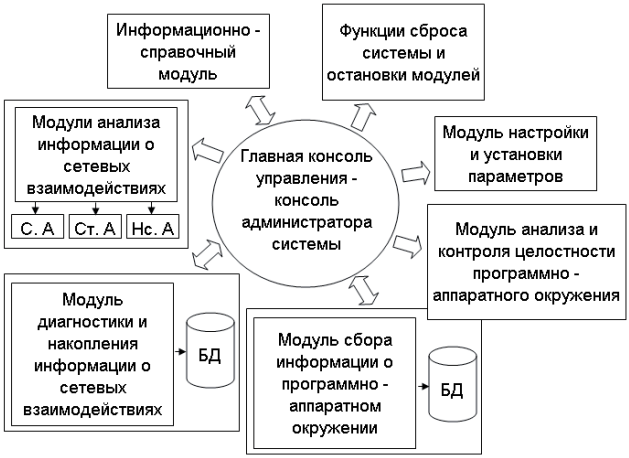

Рис 1. Модульно-блочная схема прототипа системы

Основным связующим блоком является главная консоль управления – ядро системы, являющееся центральной частью системы, обеспечивающее координированный доступ к ресурсам сети и ее компонентам: внешнему аппаратному и программному обеспечению, диагностической информации, информации о сетевых взаимодействиях и т.д. Обмен информацией и управление идет, в основном, через ядро системы. Основные блоки имеют двухстороннюю связь с ядром системы, при которой передача информации осуществляется одновременно или поочередно в обоих направлениях, что в свою очередь повышает оперативность приятия мер администратором системы, а так же увеличивает информативность о состоянии среды.

В комплексе данную схему реализации системы, возможно, обозначить модульным ядром, с применением статических методов загрузки модулей [4].

Определим основные и вспомогательные модули системы.

Основные модули непосредственно обрабатывают, хранят, производят анализ поступающей информации и принимают решения, основываясь на заранее определенных параметрах системы. По своему функциональному назначению к

основным модулям относятся:

- Модули анализа информации о сетевых взаимодействиях: статистический, сигнатурный, нейросетевой [5].
- Модуль диагностики и накопления данных: база данных структурированной информации.
- Модуль сбора информации о программно-аппаратной среде.
- Модуль анализа и контроля целостности программно-аппаратного окружения.
- Модуль настройки и установки параметров.

Соответственно дополнительные модули обеспечивают информационную поддержку администратора системы, а так же обладают возможностью возврата системы к настройкам по умолчанию и освобождению вычислительных ресурсов используемых системой анализа: остановка служб и приложений, при появлении такой необходимости или в случае некорректной работы одного из модулей системы.

Важной особенностью в системе анализа является реализация рекурсивной функции в процессе модернизации и последующего анализа информации, поступающей на сенсоры системы. Тем самым обеспечивается возможность адаптации системы к изменяющимся условиям работы сети, подразумевающая динамическую модификацию конфигурационной информации, успешно прошедшей процесс анализа (рис. 2).

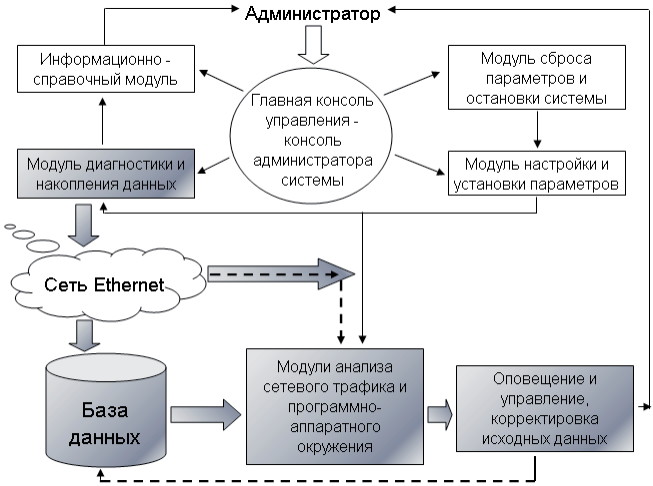

Рис 2. Технологический процесс прототипа системы

Система взаимодействует с двумя внешними сущностями: администратором и сетью.

Администратор непосредственно осуществляет управление системой до

установки режима функционирования. В системе предусмотрены автоматизированный и автоматический режимы.

При автоматизированном режиме администратор получает оповещения и рекомендации по устранению инцидентов информационной безопасности. Далее администратор принимает решение об уровне угрозы и вырабатывает меры по реагированию.

В автоматическом режиме система сама решает, какие меры принимать по устранению неполадок в функционировании сети, и составляет отчеты о действиях системы.

Сеть является непосредственным источником информации, поступающей в блоки анализа. Информация разделена на два независимых класса: сетевой трафик, классы WMI, предоставляющие информацию о программно-аппаратном окружении и сетевых взаимодействиях [7]. Для каждого из классов существует собственное хранилище данных, содержащее основные характеристики собранной информации.

Исходя из предложенного технологического процесса, в системе анализа необходимо наличие возможности обработки информации, поступающей непосредственно с сетевых интерфейсов.

Для решения этой задачи была разработана схема обработки поступающей на сенсоры информации (рис. 3).

Рис 3. Схема обработки информации

Важной особенностью технологии обработки поступающей на сенсоры системы информации является наличие доменной структуры и стандарта IPv4 в сетевой адресации. Обработку информации необходимо разделить на несколько этапов:

1. Первичный сбор и накопление конфигураций.
2. Анализ и модернизация конфигурации, управление и оповещение.

На начальном этапе система непрерывно производит сбор необходимой

информации на определенном временном отрезке либо до управляющей команды администратора. Полученные данные структурируются, фильтруются и классифицируются. Данный процесс позволяет извлечь важную информацию, необходимую для выявления отклонений в функционировании сети и сократить общий объем обрабатываемых данных. Структурированная информация в соответствии со своим классом попадает в соответствующие хранилища данных для хранения и последующего анализа. Одновременно, начиная с первого этапа, происходит отображение информации о сетевых взаимодействиях и изменениях в программно-аппаратном окружении.

На последующих этапах обработки производится извлечение необходимых показателей из баз данных, четко характеризующих изменяющиеся параметры сети. Информация анализируется по указанным выше методам и в случае обнаружения отклонений, система информирует администратора или же сама предпринимает действия по устранению, согласно встроенным функциям.

Если отклонения не обнаружены система перезаписывает конфигурационную информацию, при условии, что существует необходимость модернизации шаблона.

Внедрение в инфраструктуру сети

Для решения задачи внедрения системы в реальную или же заранее спроектированную виртуальную сетевую инфраструктуру были разработаны несколько подходов реализации (рис. 5):

- Автономная система.
- Система с применением сетевых агентов.
- Комбинированная система.

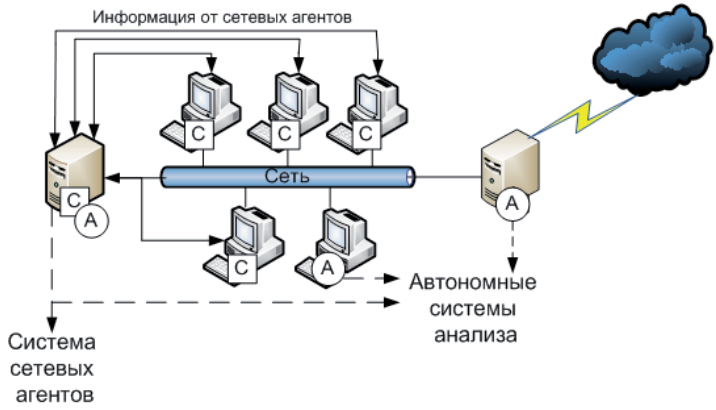

Рис 5. Схема внедрения

Автономная система основана на централизованной архитектуре [6]. Она устанавливается на центральном узле и анализирует информацию в подведом-

ственном сетевом сегменте. Отсутствие агентов не позволяет данному продукту отслеживать все события в компьютерной сети.

В автономной системе информационная база хранится на накопителях объекта анализа, результаты анализа отображаются так же на данной системе, без передачи по каналам связи. Данный тип систем является изолированным по отношению к возможностям комплексного анализа состояния безопасности в компьютерной сети, без применения дополнительных организационных мер. Данная схема внедрения в основном пригодна для применения на компонентах сети, отвечающих за предоставление конкретных услуг и функциональных возможностей: почтовый сервер, сервер приложений, ftp-сервер т.д.

Система сетевых агентов имеет децентрализованную или распределенную архитектуру. Сетевой агент устанавливается в полностью автономной операционной среде, например, на компьютере удаленного пользователя либо на одном из узлов корпоративной сети передачи данных: сервере Active Directory, прокси-сервере и т.д. [1]. Обнаружив нетипичное состояние в функционировании сети на удаленной машине, агент выдаст предупреждение непосредственно на ее экран. Если же аналогичное событие, по нарушению безопасности информации, окажется зафиксировано в ином узле корпоративной сети, сообщение о попытке несанкционированного доступа будет передано другому приложению, содержащему средства сетевого мониторинга - серверу администрирования, установленному на конкретном сетевом узле: рабочей станции или сервере, определенном под соответствующие функциональные возможности. Данный узел сети собирает и сопоставляет информацию, поступающую от разных, подчиненных ему агентов, и это дает ему возможность оперативно выявлять события, угрожающие безопасности сети.

При наличии двух и более сетевых интерфейсов (аппаратных компонентах) система может использоваться как в сетевом, так и в автономном режиме, при соответствующих настройках, что значительно повышает возможность по определению инцидентов информационной безопасности.

Заключение

В развитии систем обнаружения нарушений безопасности существует несколько подходов к разработке. Традиционный подход заключается в создании средств защиты, препятствующих реализации угроз типа нарушения целостности, конфиденциальности и отказа в обслуживании.

Система анализа и контроля потоков информации сетевого взаимодействия основана на принципе обнаружения отклонений в функционировании компонентов инфраструктуры сети, что позволяет данной системе идентифицировать угрозы безопасности информации, не обнаруживаемые традиционными средствами защиты.

С применением данной системы, процедура выявления инцидентов информационной безопасности может быть представлена в виде циклического процесса, реализуемого автоматизированной системой и действий администратора по работе с ней.

Наиболее важными задачами, которые должен решать администратор в процессе использования системы, являются:

- анализ результатов работы системы по выявлению нарушений в среде;
- своевременный контроль актуальности и модификации конфигураций.

Система является инструментом, позволяющим администратору управлять процессом выявления изменений в функционировании компьютерной сети.

Литература:

1. Андрончик А. Н., Богданов В. В., Домуховский Н. А., Коллеров А. С., Синадский Н. И., Хорьков Д. А., Щербаков М. Ю. Защита информации в компьютерных сетях. Практический курс: учебное пособие / А. Н. Андрончик, В. В. Богданов, Н. А. Домуховский, А. С. Коллеров, Н. И. Синадский, Д. А. Хорьков, М. Ю. Щербаков; под ред. Н. И. Синадского. Екатеринбург: УГТУ-УПИ, 2008. 248 с.

2. Биячуев Т.А. / под ред. Л.Г.Осовецкого Безопасность корпоративных сетей. – СПб: СПб ГУ ИТМО, 2004.- 161 с.

3. Гришина Н.В. Организация комплексной системы защиты информации. – М.: Гелиос АРВ, 2007. – 256 с.

4. Лукацкий, А. В. Обнаружение атак – 2-е изд., перераб. и доп. / А. В. Лукацкий. – СПб: БХВ-Петербург, 2003. – 608 с.

5. Осовский С. Нейронные сети для обработки информации / Пер. с польского И.Д. Рудинского. – М.: Финансы и статистика, 2002. – 344 с.

6. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства / Шаньгин В.Ф. - М.: ДМК Пресс, 2008 – 544 с.

7. Яремчук С. А. Защита вашего компьютера.- СПб.: Питер, 2008. – 288 с.

УДК 004.91

СОВРЕМЕННОЕ СОДЕРЖАНИЕ ДИСЦИПЛИНЫ «ИНФОРМАТИКА» ПРЕИМУЩЕСТВА ЭЛЕКТРОННОГО РЕСУРСА «ИНФОРМАТИКА»
CURRENT CONTENTS OF DISCIPLINE, «COMPUTER SCIENCE» ADVANTAGES OF ELECTRONIC RESOURCES «INFORMATION»

Я. Ю. Гришин
Ia. Iu. Grishin
Ульяновский Государственный Педагогический Университет
Ulyunovsk State Pedagogical University

This article provides an analysis of textbooks used in schools for teaching science: A brief description of each of them and concludes that substantial lines of these books.

Also discusses the advantages of using electronic aids to the usual textbooks, including an overview of electronic resources developed by the author.