ГОСУДАРСТВЕННЫЙ КОМИТЕТ СВЯЗИ, ИНФОРМАТИЗАЦИИ И ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ РЕСПУБЛИКИ УЗБЕКИСТАН

Ташкентский университет информационных технологий

Кафедра "Информационная безопасность"

Допустить к защите

Зав. кафедрой _____
_____

" _____ "_____ 20___ г.

Выпускная квалификационная работа

на тему: "ОРГАНИЗАЦИЯ И ПРИМЕНЕНИЕ ТЕХНОЛОГИИ АКТИВНОГО АУДИТА"

Выпускник: _____ **Бойкулов Х. С.**

Руководитель: _____ **Кучкаров Т.А.**

Рецензент _____ **Парсиев С. С.**

Консультант
по БЖД _____ **Кодиров Ф.М.**

Ташкент 2013 г.

ГОСУДАРСТВЕННЫЙ КОМИТЕТ СВЯЗИ, ИНФОРМАТИЗАЦИИ И ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ РЕСПУБЛИКИ УЗБЕКИСТАН

Ташкентский университет информационных технологий

Факультет_____ Кафедра____ _____

Направление (специальность) _____
_____

"УТВЕРЖДАЮ"
Зав. кафедрой _____
_____

" __ " _____ 2013 г., протокол №__

Задание

на выпускную квалификационную работу

_____ *Бойкулову Хамдаму Суюновичу* _____
(фамилия, имя, отчество)

Тема работы: *"Организация и применение технологии активного аудита"*
_____

Утверждена приказом по университету от "__" _____ 20___ г. № ____ _____

1. Срок сдачи законченной работы *10.06.2013 г.*

Исходные данные к работе *Материалы полученные из интернета, из книг, из рефератов и технических документаций*
_____

2. Содержание расчетно-пояснительной записки (перечень подлежащих разработке вопросов) *1 Исследование методов и средств активного аудита. 2. Разработка алгоритма активного аудита информациионой системы. 3. Безопасность жизнедеятельности.*
_____

3. Перечень графического материала *Материалы презентации*
_____

4. Дата выдачи задания 20.01.13 г._____

Руководитель _____
(подпись)

Задание принял _____
(подпись)

5. Консультанты по отдельным разделам выпускной работы

Раздел	Ф.И.О. руководителя	Подпись, дата	
		Задание выдал	Задание получил
Обзорная и основная части	Кучкаров Т.А.		
БЖД	Кодиров Ф.М.		

8. График выполнения работы

№	Наименование раздела работы	Срок выполнения	Отметка руководителя о выполнении
1.	Исследование методов и средств активного аудита	29.02.2013	
2.	Разработка алгоритма активного аудита информационной системы	20.03.2013	
3.	Безопасность жизнедеятельности	25.05.2013	
4.	Подготовка презентационного материала	30.05.13	

Выпускник _____
_____ "____" _____2013 г.
(подпись)

Руководитель _____
_____ "____" _____2013 г.
(подпись)

Выпускная квалификационная работа посвящена исследованию нового сервиса безопасности – активному аудиту. В работе проанализированы методы проведения активного аудита, приведена различная архитектура активного аудита, требования к системам активного аудита, имеющиеся стандарты в этой области, примеры реализации систем активного аудита.

В работе приводится разработанный алгоритм активного аудита информационной системы на основе технологий искусственный иммунных систем. Рассмотрены вопросы безопасности жизнедеятельности: анализ условий труда, вопросы организации рабочего места, а также чрезвычайные ситуации.

Ушбу битирув малакавий иш ахборот хавфсизлигида янги сервис - актив аудитга бағишланган. Ишда актив аудит тизимлар таҳлил этилган, соҳага доир стандартлар ўрганиб чиқилган ва шу асосида ахборот тизимларини актив аудит ўтқазиш алгоритми ишлаб чиқилган.

Шунингдек хаёт фаолияти хавфсизлиги хам кўриб чиқилган.

The Subject exhaust qualification work is comparatively new service to safety - active audit. In work are analysed methods of the undertaking active audits, is brought different architecture active audit, requirements to system active audit, available standards in this area, examples to realization of the systems active audit.

The designed algorithm active audit information system happens to In work on base technology artificial systems.

The Considered questions to safety to vital activity: analysis of the conditions of the labour, questions to organizations worker place, as well as exceeding situations.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Развитие информационно-коммуникационных технологий (ИКТ) является одним из основных факторов благосостояния и экономического роста страны. Сегодня ИКТ становится одним из основных приоритетов государственной политики Узбекистана.

В Постановлении Президента Республики Узбекистан "О мерах по дальнейшему внедрению и развитию современных информационно-коммуникационных технологий. (Собрание законодательства Республики Узбекистан, 2012 г., № 13, ст. 139) одной из основных задачи является дальнейшее внедрение и развитие информационно-коммуникационных технологий [1].

Сегодня информационные системы (ИС) играют ключевую роль в обеспечении эффективности работы коммерческих и государственных предприятий. Повсеместное использование ИС для хранения, обработки и передачи информации делает актуальными проблемы их защиты, особенно учитывая глобальную тенденцию к росту числа информационных атак, приводящих к значительным финансовым и материальным потерям. Для эффективной защиты от атак компаниям необходима объективная оценка уровня безопасности ИС - именно для этих целей и применяется аудит безопасности.

В таких условиях системы информационной безопасности должны уметь противостоять многочисленным, разнообразным атакам, ведущимся изнутри и извне, атакам автоматизированным и скоординированным. Иногда нападение длится доли секунды; порой прощупывание слабостей ведется медленно и растягивается на часы, так что подозрительная активность практически незаметна. Целью злоумышленников может быть нарушение доступности, целостности или конфиденциальности.

Темой выпускной квалификационной работы является относительно новый сервис безопасности – активный аудит. Активный аудит направлен на выявление подозрительной (злоумышленной и/или аномальной) активности с целью оперативного принятия ответных мер. С этим сервисом связываются надежды на существенное повышение защищенности корпоративных информационных систем (может быть, потому, что недостаточность более традиционных механизмов, к сожалению, доказана практикой). В этом плане выбранная тема выпускной работы ***является весьма актуальной***.

Цель работы заключается в разработке алгоритма активного аудита, основанного на применении технологий искусственных иммунных систем.

Основными задачами работы являлись:

1. Анализ субъектов и объектов информационной системы на предмет проведения активного аудита.

2. Разработка алгоритма активного аудита ИС, основанного на применении технологий искусственных иммунных систем.

3. Разработка структуры системы активного аудита, которая включает в себя набор сенсоров для анализа и обработки информации о функционировании информационной системы.

Выпускная квалификационная работа состоит из введения, трех глав и заключения.

В ***обзорной части*** выпускной работы проанализированы методы проведения активного аудита, приведена различная архитектура активного аудита, требования к системам активного аудита, имеющиеся стандарты в этой области, примеры реализации систем активного аудита.

В ***основной части*** работы приводится разработанный алгоритм активного аудита информационной системы на основе технологий искусственный иммунных систем.

Рассмотрены вопросы ***безопасности жизнедеятельности***: анализ условий труда, вопросы организации рабочего места, а также чрезвычайные ситуации.

В разделе ***"Охрана труда и техника безопасности"*** рассмотрены вопросы безопасности жизнедеятельности: анализ условий труда, вопросы организации рабочего места, а также чрезвычайные ситуации.

1. ИССЛЕДОВАНИЕ МЕТОДОВ И СРЕДСТВ АКТИВНОГО АУДИТА

1.1. Активный аудит и его место среди других сервисов безопасности

Формула «защищать, обнаруживать, реагировать» (по-английски это звучит лучше: «protect, detect, react») является классической. Только эшелонированная, активная оборона, содержащая разнообразные элементы, дает шанс на успешное отражение угроз.

Назначение активного аудита - обнаруживать и реагировать. Как указывалось во введении, обнаружению подлежит подозрительная активность компонентов информационной системы (ИС) - от пользователей (внутренних и внешних) до программных систем и аппаратных устройств.

Подозрительную активность можно подразделить на злоумышленную и аномальную (нетипичную). Злоумышленная активность - это либо атаки, преследующие цель несанкционированного получения привилегий, либо действия, выполняемые в рамках имеющихся привилегий (возможно, полученных незаконно), но нарушающие политику безопасности. Последнее мы будем называть злоупотреблением полномочиями. Нетипичная активность может впрямую не нарушать политику безопасности, но, как правило, она является следствием либо некорректной (или сознательно измененной) работы аппаратуры или программ, либо действий злоумышленников, маскирующихся под легальных пользователей.

Активный аудит дополняет такие традиционные защитные механизмы, как идентификация/аутентификация и разграничение доступа. Подобное дополнение необходимо по двум причинам. Во-первых, существующие средства разграничения доступа не способны реализовать все требования политики безопасности, если последние имеют более сложный вид, чем разрешение/запрет атомарных операций с ресурсами. Развитая политика

безопасности может накладывать ограничения на суммарный объем прочитанной информации, запрещать доступ к ресурсу B, если ранее имел место доступ к ресурсу A, и т.п. Во-вторых, в самих защитных средствах есть ошибки и слабости, поэтому, помимо строительства заборов, приходится заботиться об отлавливании тех, кто смог через эти заборы перелезть.

Развитые системы активного аудита несут двойную нагрузку, образуя как первый, так и последний защитные рубежи (рис. 1.1). Первый рубеж предназначен для обнаружения атак и их оперативного пресечения. На последнем рубеже выявляются симптомы происходящих в данный момент или ранее случившихся нарушений политики безопасности, принимаются меры по пресечению нарушений и минимизации ущерба.

Рис. 1.1. Защитные рубежи, контролируемые системами активного аудита

И на первом, и на последнем рубеже, помимо активного аудита, присутствуют другие сервисы безопасности. К первому рубежу можно отнести сканеры безопасности, помогающие выявлять и устранять слабые места в защите. На последнем рубеже для обнаружения симптомов нарушений могут использоваться средства контроля целостности. Иногда их включают в репертуар систем активного аудита; мы, однако, не будем этого делать, считая контроль целостности отдельным сервисом.

Между сервисами безопасности существуют и другие связи. Так, активный аудит может опираться на традиционные механизмы протоколирования. В свою очередь, после выявления нарушения зачастую требуется просмотр ранее

накопленной регистрационной информации, оценить ущерб, понять, почему нарушение стало возможным, спланировать меры, исключающие повторение инцидента. Параллельно производится надежное восстановление первоначальной (то есть не измененной нарушителем) конфигурации.

Отдельным вопросом является взаимодействие систем активного аудита и управления. Активный аудит выполняет типичные управляющие функции анализ данных об активности в информационной системе, отображение текущей ситуации, автоматическое реагирование на подозрительную активность. Сходным образом функционирует, например, подсистема сетевого управления. Целесообразно интегрировать активный аудит и «общее» управление, в максимально возможной степени используя общие программно-технические и организационные решения. В эту интегрированную систему может быть включен и контроль целостности, а также агенты другой направленности, отслеживающие специфические аспекты поведения ИС (рис. 1.2).

С логической точки зрения можно считать, что существует центральная консоль управления, куда стекаются данные от систем активного аудита, контроля целостности, анализа защищенности, контроля систем и сетей по другим аспектам. На этой консоли в том или ином виде отображается текущая ситуация, с нее, автоматически или вручную, выдаются управляющие команды.

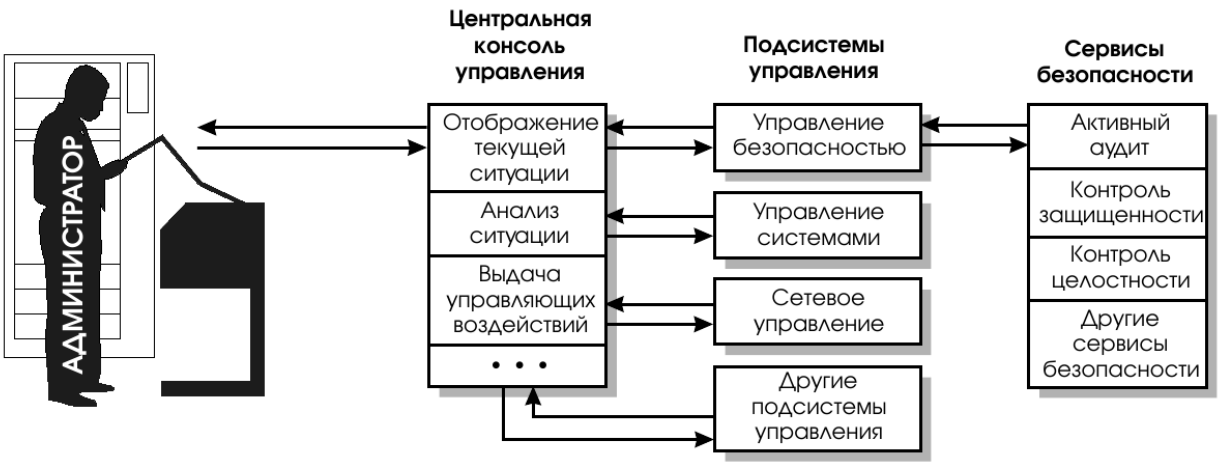


Рис. 1.2. Интеграция сервисов безопасности и системы управления

1.2. Методы проведения активного аудита

1.2.1. История развития аудита

Первые работы в области систем активного аудита относятся к началу 1980-х годов (см. [8]). До этого регистрационная информация обрабатывалась вручную (во всяком случае, без применения специального программного обеспечения) штатом аудиторов. Работа людей-аудиторов была тяжелой и неэффективной; очевидно, в наше время вдвойне наивно надеяться на то, что системный администратор (даже высококвалифицированный) без средств активного аудита сможет в режиме реального времени найти в регистрационных журналах подозрительные записи и принять адекватные меры противодействия.

Вполне понятно, что на первом этапе не было речи об анализе сетевой активности (самих сетей было не так много). Обрабатывались системные журналы, иногда с небольшой задержкой, чаще раз в сутки (тогда подобные задержки были вполне приемлемыми). Направление сетевой безопасности стало интенсивно развиваться примерно десять лет спустя в 1990-е годы и плоды этого развития мы наблюдаем сейчас, прежде всего, на примере межсетевых экранов.

При разработке систем активного аудита вставали как концептуальные, так и технические проблемы. По большому счету концептуальная проблема была одна: как выявлять подозрительную активность? Первоначально были предложены статистические методы, основанные на предположении о том, что злоумышленная активность всегда сопровождается какими-то аномалиями, изменением профиля поведения пользователей, программ или аппаратуры. Несколько позднее для нужд активного аудита стали применять экспертные системы, описывающие злоумышленную активность совокупностью правил.

Довольно быстро стало понятно, что два подхода - статистический и экспертный - хорошо дополняют друг друга и что с возникающими проблемами они могут справиться только вместе. Действительно, статистический подход хорош там, где существует понятие типичного поведения, а распределения измеряемых величин в нормальной ситуации остаются относительно стабильными. С другой стороны, экспертный подход плохо справляется с неизвестными атаками (равно как и с многочисленными вариациями известных атак).

Главной технической проблемой является проблема масштабируемости. Даже на одном хосте при числе пользователей порядка нескольких сотен объем регистрационной информации, генерируемой только операционной системой, измеряется гигабайтами или в лучшем случае сотнями мегабайт. Хранение и обработка подобных объемов - задача непростая. Несмотря на все сложности, интенсивность работ в области активного аудита нарастает. Это касается и коммерческих, и исследовательских проектов.

1.2.2. Архитектура систем активного аудита

У систем активного аудита целесообразно различать локальную и глобальную архитектуру. В рамках локальной архитектуры реализуются элементарные составляющие, которые затем могут быть объединены для обслуживания корпоративных систем.

Основные элементы локальной архитектуры и связи между ними показаны на рис. 1.3. Первичный сбор данных осуществляют агенты, называемые также сенсорами. Регистрационная информация может извлекаться из системных или прикладных журналов (технически несложно получать ее и напрямую от ядра ОС), либо добываться из сети с помощью соответствующих механизмов активного сетевого оборудования или путем

перехвата пакетов посредством установленной в режим мониторинга сетевой карты.

На уровне агентов (сенсоров) может выполняться фильтрация данных с целью уменьшения их объема. Это требует от агентов некоторого интеллекта, но зато разгружает остальные компоненты системы. Агенты передают информацию в центр распределения, который приводит ее к единому (стандартному для конкретной системы активного аудита) формату, возможно, осуществляет дальнейшую фильтрацию (редукцию), сохраняет в базе данных и направляет для анализа статистическому и экспертному компонентам.

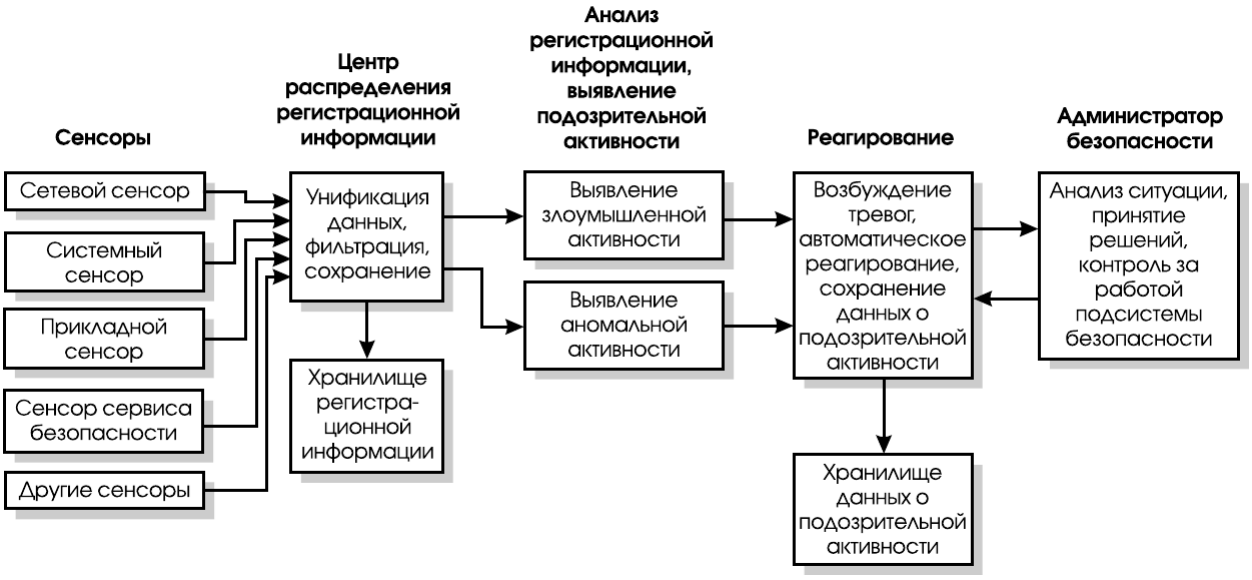


Рис. 1.3. Основные элементы локальной архитектуры систем активного аудита

Содержательный активный аудит начинается со статистического и экспертного компонентов. Если в процессе статистического или экспертного анализа выявляется подозрительная активность, соответствующее сообщение направляется решателю, который определяет, является ли тревога оправданной, и выбирает способ реагирования. Хорошая система активного аудита должна уметь внятно объяснить, почему она подняла тревогу, насколько серьезна ситуация и каковы рекомендуемые способы действия. Если выбор должен оставаться за человеком, то пусть он

сводится к нескольким элементам меню, а не к решению концептуальных проблем.

Глобальная архитектура подразумевает организацию одноранговых и разноранговых связей между локальными системами активного аудита (рис. 1.4). На одном уровне иерархии располагаются компоненты, анализирующие подозрительную активность с разных точек зрения. Например, на хосте могут располагаться подсистемы анализа поведения пользователей и приложений. Их может дополнять подсистема анализа сетевой активности. Когда один компонент обнаруживает что-то подозрительное, то во многих случаях целесообразно сообщить об этом соседям либо для принятия мер, либо для усиления внимания к определенным аспектам поведения системы.

Разноранговые связи используются для обобщения результатов анализа и получения целостной картины происходящего. Иногда у локального компонента недостаточно оснований для возбуждения тревоги, но «по совокупности» подозрительные ситуации могут быть объединены и совместно проанализированы, после чего порог подозрительности окажется превышенным. Целостная картина, возможно, позволит выявить скоординированные атаки на разные участки информационной системы и оценить ущерб в масштабе организации.

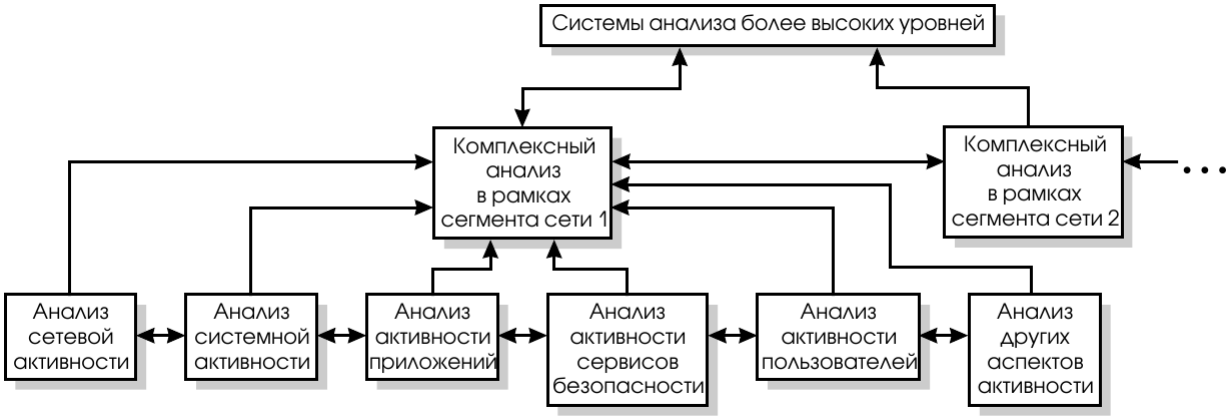


Рис. 1.4. Глобальная архитектура системы активного аудита.

К числу важнейших архитектурных относится вопрос о том, какую информацию и в каких масштабах собирать и анализировать. Первые системы активного аудита были однохостовыми. Затем появились многохостовые конфигурации. Прорыву в области коммерческих продуктов мы обязаны сетевым системам, анализировавшим исключительно сетевые пакеты. Наконец, в настоящее время, как и следовало ожидать, можно наблюдать конвергенцию архитектур, в результате чего рождаются комплексные системы, отслеживающие и анализирующие как компьютерную, так и сетевую регистрационную информацию (рис. 1.5).

Без понимания семантики защищаемых или анализируемых объектов обеспечение безопасности невозможно. Это понимание может быть выражено в процедурном (программы) или декларативном (описания) видах, но оно должно существовать. Декларативная семантика предпочтительнее, поскольку она позволяет без изменений применять программный продукт к различным объектам.

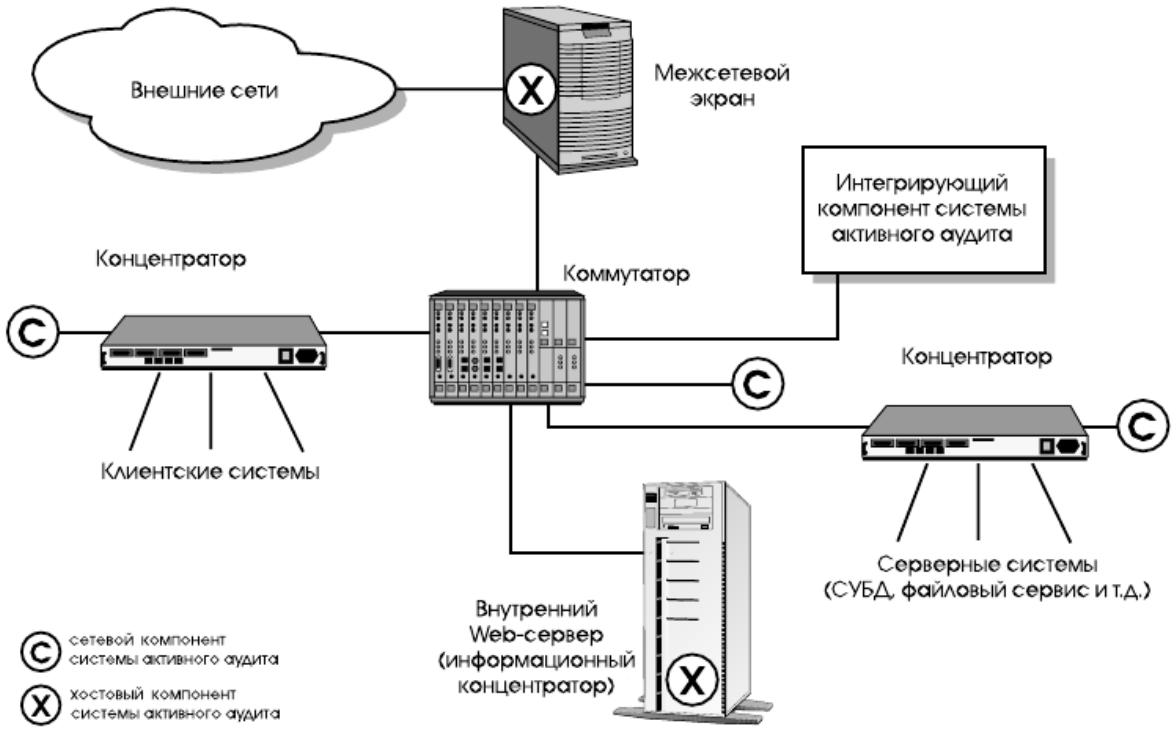


Рис. 1.5. Архитектура комплексной системы активного аудита

В статье [6] отмечалось, что современные информационные системы не готовы к эффективному управлению. В еще большей степени этот вывод применим к активному аудиту. Программные системы являются «неаудируемыми», нет ясных критериев, позволяющих отличить нормальное поведение от злоумышленного или аномального. В таких условиях наивно было бы ожидать, что установленные «поверх» средства выявления подозрительной активности сотворят чудо и отразят все атаки. Впрочем, вопрос "аудируемости" программных продуктов пока совершенно не исследован.

Традиционным является вопрос, где размещать сенсоры систем активного аудита. Столь же традиционный ответ гласит: «везде, где можно». Только анализ всех доступных источников информации позволит с достоверностью обнаруживать атаки и злоупотребления полномочиями и докапываться до их первопричин [11]. Если вернуться к трактовке информационной системы в виде совокупности сервисов, то средства обнаружения атак должны располагаться перед защищаемыми ресурсами (имея в виду направление движения запросов к сервисам), а средства выявления злоупотреблений полномочиями - на самих сервисах. Обнаружение аномальной активности полезно во всех упомянутых точках. Только при таком размещении сенсоров будет выполнен важнейший принцип невозможности обхода защитных средств. Кроме того, будет минимизировано число сенсоров, что в условиях сегментации сетей и применения коммутационных технологий также оказывается проблемой.

Для того, чтобы система активного аудита, особенно распределенная, была практически полезной, необходимо обеспечить целостность анализируемой и передаваемой информации, а также целостность самой программной системы и ее живучесть в условиях отказа или компрометации отдельных компонентов (зачастую атака направляется сначала на средства безопасности, а уже потом - на прикладные компоненты). Ясно, что это проблема всех распределенных систем, и для ее

решения служат сервисы взаимной аутентификации и контроля целостности (в том числе проверка подлинности источника данных).

1.2.3. Выявление злоумышленной активности

Под злоумышленной активностью мы понимаем как атаки (очевидно, противоречащие любой политике безопасности), так и действия, нарушающие политику безопасности конкретной организации путем злоупотребления имеющимися полномочиями. Разделение двух видов злоумышленной активности представляется нам целесообразным по той причине, что настройка на выявление атак может быть выполнена поставщиком системы активного аудита (атаки носят универсальный характер), в то время как политика безопасности (если, конечно, она есть) у каждой организации своя и настраиваться на нее заказчикам придется самим.

Для выявления злоумышленной активности пытались и пытаются использовать несколько универсальных технологий: *экспертные системы*, *нейронные сети*, *сопоставление с образцом*, *конечные автоматы* и т.п. Одной из первых и до сих пор самой употребительной остается *технология обнаружения сигнатур злоумышленных действий*. Идея состоит в том, чтобы каким-либо образом задать характеристики злоумышленного поведения (это и называется сигнатурами), а затем отслеживать поток событий в поисках соответствия с предопределенными образцами. Иногда сопоставление основывается на простом механизме регулярных выражений, известному всем по ОС Unix. В более серьезных разработках уже свыше десяти лет используются *экспертные системы*, опирающиеся на наборы правил, задающие более мощные языки.

Грубо можно считать, что экспертная система состоит из универсальной оболочки и наполнения в виде правил вывода, являющихся формализацией знаний о предметной области. В области активного аудита

чаще всего используется оболочка PBEST (Productionn Based Expert System Toolset) [15]. Ее мы и рассмотрим вместе с некоторыми сигнатурами атак, заимствованными из той же статьи [15].

```
rule [Bad_Login(#10;*):
  [e:event|   event_type   ==   login,
              return_code            ==
              'BAD_PASSWORD]
==>
  [+bad_login|      username      =
                 e.username,
                 hostname
                 e.hostname]
  [ |e]
  [!|printf("Bad login for user %s from host %s\n", e.username, e.hostname)]
]
```

Листинг 1. Пример правила на языке P-BEST

Каждое правило состоит из двух частей: условия применимости (называемого также *антецедентом*) и правой части - *консеквента*. Когда очередное событие в отслеживаемом потоке делает истинным условие применимости некоторого правила, говорят, что правило «зажигается». Если консеквент содержит какие-либо действия, они выполняются (или помещаются в поле зрения компонента, принимающего решения о реагировании на злоумышленную активность).

В состав P-BEST входит компилятор pbcc, транслирующий правила вывода в функции языка C. После компиляции может быть получена либо самостоятельная экспертная система, либо набор библиотек, которые можно подключить к более широкому окружению. Для нас существенно, что язык P-BEST достаточно прост и интуитивно ясен, поэтому в принципе пользователи сами могут описывать на нем новые атаки и иные злоумышленные действия. Компиляция (в противовес интерпретации) правил позволяет получить эффективное решение, пригодное для работы в реальном масштабе времени. В состав антецедентов и консеквентов могут

входить произвольные функции языка C. Это упрощает связь с окружением, программирование реакций и т.п.

Приведем пример простого правила, записанного на языке P-BEST (см. листинг 1). Оно обрабатывает неудачную попытку входа в систему. Предполагается, что ранее были описаны типы **event** и **bad_login** с соответствующими полями.

В первой строке, помимо названия правила, указан его приоритет (10), влияющий на порядок выполнения, а также дано разрешение на его многократное применение. Чтобы не случилось зацикливания, оператор «**[|e]**» в консеквенте удаляет факт **e** из базы фактов, но предварительно в эту базу добавляет факт **bad_login**, который затем можно использовать, например, для подсчета числа неудачных попыток входа. Наконец, конструкция «**!|**» позволяет выполнять функции языка C. Разумеется, в реальных системах реакция должна быть более изощренной.

В качестве реального примера использования языка P-BEST рассмотрим правило, идентифицирующее атаки посредством переполнения буфера, резервируемого для хранения параметров (см. листинг 2). Подобные атаки используют ошибки в программном обеспечении, связанные с проверкой корректности параметров (точнее, с отсутствием или недостаточностью таких проверок). Если подходящим образом задать слишком длинные параметры некоторым утилитам, выполняющимся от имени суперпользователя (таким, например, как **eject** или **fdformat** в Solaris 2.5), можно выполнить в привилегированном режиме произвольную команду.

Приведенное правило рассчитано на модуль регистрации/аудита BSM в ОС Solaris. Идея выявления атак посредством переполнения буфера основана на анализе длины аргументов системных вызовов группы exec. Оказывается, размер учетной записи о «зловредном» exec составляет не менее 500 байт, в то время как в нормальных случаях он практически никогда не превышает 400.

```
rule[BSM_LONG_SUID_EXEC(*):
  [+e:bsm_event]
  [?|e.header_event_type == AUE_EXEC ||
     e.header_event_type == AUE_EXECVE]
  [?|e.subject.euid != e.subject.ruid]
  [?|e.header_size > 'NORMAL_LENGTH]
==>
  [!|printf("ALERT: buffer overrun attack on command %s\n",
  e.header_command)]
]
```

Листинг 2. Пример правила, выявляющего атаки посредством переполнения буфера параметров

Таким образом, подход, основанный на выявлении сигнатур злоумышленных действий средствами экспертных систем, оказывается вполне работоспособным со всех точек зрения.

Самой сложной проблемой для сигнатурного подхода является обнаружение ранее неизвестных атак. Выше мы указывали, что новые угрозы появляются практически каждый день. Бороться с ними можно двумя способами.

Во-первых, можно регулярно обновлять набор сигнатур. Здесь, помимо полноты, критически важной является частота обновлений. Во-вторых, можно (и нужно) сочетать сигнатурный подход с методами выявления *аномальной активности.*

1.2.4. Выявление аномальной активности

Для выявления аномальной активности было предложено довольно много методов (см. [17]): *нейронные сети*, *экспертные системы*, *статистический подход*. В свою очередь, статистический подход (он является темой нашего рассмотрения) можно подразделить на кластерный и факторный анализ, а также дискриминантный (классификационный) анализ. Статистический анализ представляется нам наиболее

перспективным, отчасти «от противного», в силу недостатков, присущих другим подходам.

У нейронных сетей две основные проблемы:

- непонятность результатов: нейронная сеть принимает решение, но не объясняет, почему оно было принято;
- нехватка адекватного обучающего материала: невозможно создать базу всех типов аномалий.

Основной недостаток экспертных систем был указан выше - неумение выявлять (и, следовательно, отражать) неизвестные атаки.

У статистического подхода также есть проблемы:

- относительно высокая вероятность ложных тревог (нетипичность поведения не всегда означает злой умысел);
- плохая работа в случаях, когда действия пользователей не имеют определенного шаблона, когда с самого начала пользователи совершают злоумышленные действия, наконец, когда пользователь постепенно изменяет шаблон своего поведения в сторону злоумышленных действий.

Тем не менее, как показывает опыт, с этими проблемами можно бороться.

Выявление аномальной активности статистическими методами основывается на сравнении краткосрочного поведения с долгосрочным. Для этого измеряются значения некоторых параметров работы субъектов (пользователей, приложений, аппаратуры). Параметры могут отличаться по своей природе; можно выделить следующие группы:

- категориальные (измененные файлы, выполненные команды, номер порта и т.п.);
- числовые (процессорное время, объем памяти, количество просмотренных файлов, число переданных байт и т.п.);
- величины интенсивности (число событий в единицу времени);
- распределение событий (таких как доступ к файлам, вывод на печать и т.п.).

Алгоритмы анализа могут работать с разнородными значениями, а могут преобразовать все параметры к одному типу (например, разбив область значения на конечное число подобластей и рассматривая все параметры как категориальные).

Выбор измеряемых характеристик работы - очень важный момент. С одной стороны, недостаточное число фиксируемых параметров может привести к неполноте описания поведения субъекта и к большому числу пропуска атак; с другой стороны, слишком большое число отслеживаемых характеристик потребует слишком большого объема памяти и замедлит работу алгоритма анализа.

Измерения параметров накапливаются и преобразуются в профили - описания работы субъектов. Суть преобразования множества результатов измерения в профили - сжатие информации. В результате от каждого параметра должно остаться лишь несколько значений статистических функций, содержащих необходимые для анализирующего алгоритма данные. Для того, чтобы профили адекватно описывали поведение субъекта, необходимо отбрасывать старые значения параметров при пересчете значений статистических функций. Для этого, как правило, используется один из двух методов:

- *метод скользящих окон* – результаты измерений за некоторый промежуток времени (для долгосрочных профилей — несколько недель, для краткосрочных - несколько часов) сохраняются; при добавлении новых результатов старые отбрасываются. Основным недостатком метода скользящих окон является большой объем хранимой информации.
- *метод взвешенных сумм* - при вычислении значений статистических функций более старые данные входят с меньшими весами (как правило, новые значения функций вычисляются по рекуррентной формуле, и необходимость хранения большого количества информации отпадает). Основным недостатком метода является более низкое качество описания поведения субъекта, чем в методе скользящих окон.

Итак, долгосрочные профили содержат в себе информацию о поведении субъектов за последние несколько недель; обычно они пересчитываются раз в сутки, когда загрузка системы минимальна. Краткосрочные профили содержат информацию о поведении за последние несколько часов или даже минут; они пересчитываются при поступлении новых результатов измерений.

Статистический подход является предметом интенсивных исследований, но уже сейчас он обладает достаточной зрелостью, используется в академических и коммерческих разработках. Можно ожидать, что со временем его позиции будут укрепляться. Во всяком случае, системы активного аудита, в которых статистический компонент отсутствует, не могут претендовать на полноту защитных функций.

1.2.5. Реагирование на подозрительные действия

После того, как обнаружена сигнатура злоумышленного действия или нетипичная активность, необходимо выбрать достойный ответ. По многим соображениям удобно, чтобы компонент реагирования содержал собственную логику, фильтруя сигналы тревоги и сопоставляя сообщения, поступающие от подсистем анализа. Для активного аудита одинаково опасны как пропуск атак (это значит, что не обеспечивается должной защиты), так и большое количество ложных тревог (это значит, что активный аудит быстро отключат).

При выборе реакции особенно важно определить первопричину проблем. Для сетевых систем это особенно сложно в силу возможности подделки адресов в пакетах. Данный пример показывает, что сильнодействующие средства, пытающиеся воздействовать на злоумышленника, сами могут стать косвенным способом проведения атак.

С точки зрения быстрого реагирования, традиционные меры, связанные с информированием администратора, не особенно эффективны. Они хороши

в долгосрочном плане, для глобального анализа защищенности командой профессионалов. Здесь активный аудит смыкается с пассивным, обеспечивая сжатие регистрационной информации и представление ее в виде, удобном для человека.

Разумная реакция на подозрительные действия может включать увеличение степени детализации протоколов и активизацию средств контроля целостности. В принципе, это пассивные меры, но они помогут понять причины и ход развития нарушения, так что человеку будет проще выбрать «меру пресечения».

Вероятно, в перспективе нормой станет взаимодействие с системами, через которые поступает подозрительный сетевой трафик. Это поможет пресечению злоумышленной активности и прослеживанию нарушителя.

1.2.6. Требования к системам активного аудита

В этом пункте мы рассмотрим требования к системам активного аудита, существенные с точки зрения заказчиков.

На первое место следует поставить требование полноты. Это весьма емкое понятие, включающее в себя следующие аспекты:

- **полнота отслеживания информационных потоков к сервисам.** Активный аудит должен охватывать все потоки всех сервисов. Это означает, что система активного аудита должна содержать сетевые и системные сенсоры, анализировать информацию на всех уровнях - от сетевого до прикладного.
- **полнота спектра выявляемых атак и злоупотреблений полномочиями.** Данное требование означает не только то, что у системы должен быть достаточно мощный язык описания подозрительной активности (как атак, так и злоупотреблений полномочиями). Этот язык должен быть прост, чтобы заказчики могли производить настройку системы в соответствии со своей политикой безопасности.

- **достаточная производительность.** Система активного аудита должна справляться с пиковыми нагрузками защищаемых сервисов.

Пропуск даже одного сетевого пакета может дать злоумышленнику шанс на успешную атаку. Если известно, что система активного аудита обладает недостаточной производительностью, она может стать объектом атаки на доступность, на фоне которой будут развиваться другие виды нападения.

Помимо полноты, системы активного аудита должны удовлетворять следующим требованиям:

- **минимум ложных тревог**. В абсолютном выражении допустимо не более одной ложной тревоги в час. При интенсивных потоках данных между сервисами и их клиентами подобное требование оказывается весьма жестким. Пусть, например, в секунду по контролируемому каналу проходит 1000 пакетов. За час пакетов будет 3 600 000. Можно предположить, что почти все они не являются злоумышленными. И только один раз система активного аудита имеет право принять «своего» за «чужого», то есть вероятность ложной тревоги должна составлять в данном случае не более $3 * 10^{-7}$.

- **умение объяснять причину тревоги.** Выполнение этого требования во-первых, помогает отличить обоснованную тревогу от ложной, во-вторых, помогает определить первопричину инцидента, что важно для оценки его последствий и недопущения повторных нарушений. Даже если реагирование на нарушение производится в автоматическом режиме, должна оставаться возможность последующего разбора ситуации специалистами.

- **интеграция с системой управления и другими сервисами безопасности.** Интеграция с системой управления имеет две стороны. Во-первых, сами средства активного аудита должны управляться (устанавливаться, конфигурироваться, контролироваться) наравне с другими инфраструктурными сервисами. Во-вторых, активный аудит может (и должен) поставлять данные в общую базу данных управления.

- **наличие технической возможности удаленного мониторинга информационной системы**. Это спорное требование, поскольку не все организации захотят оказаться под чьим-то «колпаком». Однако, с технической точки зрения подобная мера вполне оправдана, поскольку большинство организаций не располагает квалифицированными специалистами по информационной безопасности. Отметим, впрочем, что удаленный мониторинг может быть использован и для бесспорных целей, таких как контроль из штаб-квартиры за работой удаленных отделений.

1.3. Стандарты в области активного аудита

Активный аудит - относительно новая область, однако, проблемы совместимости, согласованной работы различных систем, разумеется, уже дают о себе знать. Начинают формироваться стандарты, которые можно назвать внутренними. Они помогают взаимодействовать между собой компонентам систем активного аудита и системам в целом.

1.3.1. Обмен данными о подозрительной активности

Многие атаки на информационные системы носят распределенный характер. При этом разные средства активного аудита видят один и тот же инцидент с разных точек зрения. Несомненно, совместный, многоаспектный анализ полезен для прослеживания злоумышленников, определения причин и масштабов инцидентов.

Разделение информации о подозрительной активности является главным направлением работ недавно созданной в рамках Тематической группы по технологии Интернет (Internet Engineering Task Force, IETF). Рабочей группы по обнаружению вторжений ((Intrusion Detection Working Croup, IDWC).

В июне 1999 года появился первый проект группы — «Требования к формату обмена данными о подозрительной активности» [20]. Это «мета-стандарт», выдвигающий довольно общие требования к будущим рекомендациям группы; тем не менее, он представляет несомненный интерес.

Группе IDWC предстоит специфицировать формат и процедуры разделения данных между системами выявления подозрительной активности, реагирования и управления. Предполагается, что автоматизированные системы активного аудита будут использовать формат IDBF при формировании сообщений о подозрительной активности. На самом деле требования [20] разрабатывались, в первую очередь, в расчете на взаимодействие между анализирующим компонентом и компонентом реагирования, происходящее по протоколу TCP/IP.

IDBF должен поддерживать все механизмы обнаружения подозрительной активности. Он должен быть рассчитан на IPv6, содержать все необходимое для интернационализации/локализации, поддерживать фильтрацию и агрегирование сообщений компонентом реагирования, их надежную доставку (в том числе через межсетевой экран без внесения в конфигурацию последнего изменений, способных ослабить периметр безопасности).

Формат IDBF должен поддерживать взаимную аутентификацию общающихся сторон, неотказуемость от факта передачи, а также целостность и конфиденциальность потока сообщений.

В сообщениях формата IDBF должны содержаться дата и время подозрительных событий и, если возможно, дата и время атаки. Если анализатор сам принял ответные меры, в IDBF-сообщениях должна быть информация об этом. Если анализатор может оценить последствия зафиксированной атаки, он также обязан сообщить об этом.

Формат IDBF должен поддерживать информацию о производителе системы активного аудита, сгенерировавшей сообщение, а также расширения, специфичные для конкретной системы.

В сообщениях могут содержаться идентификаторы источника и цели атаки. Если атака имеет сетевой характер, в качестве идентификаторов могут использоваться IP-адреса.

1.3.2. Общий каркас систем активного аудита

Общий каркас систем активного аудита (Common Intrusion Detection Framework, CIDF, см. [21]) разрабатывается группой исследовательских организаций, финансируемых агентством DARPA и работающих в области выявления подозрительной активности.

Цель создания общего каркаса близка к исходным посылкам группы IDWC (см. предыдущий пункт) - обеспечить интероперабельность и разделение информации различными системами активного аудита и их компонентами, максимизировать повторное использование последних в различных контекстах. В сходстве целей нет ничего удивительного, поскольку именно участники группы CIDF стали инициаторами организации группы IDWC, хотя теперь последняя живет своей, вообще говоря, независимой жизнью.

В рамках CIDF разработан язык описания подозрительной активности и способ кодирования информации о подозрительных событиях. Язык приспособлен для описания по крайней мере трех видов сообщений:

- «сырой» информации о событиях (например, записей регистрационного журнала или сетевых пакетов);
- результатов анализа (таких как выявленные аномалии или атаки);
- рекомендованных реакций (прервать какую-либо активность или изменить конфигурацию защитных средств).

Кроме того, на языке могут быть описаны следующие сущности:

- связи между событиями (например, причинно-следственные);
- роли объектов в событиях (например, объект инициировал событие);
- свойства объектов;
- связи между объектами.

```
(Delete
     (Context
          (HostName
          'main.strange.com')  (Time
          '23:55:12 Aug 11 1999')
     )
     (Initi
     ator
          (UserName 'root')
     )
     (So
     urc
     e
          (FileName '/etc/passwd')
     )
)
```

Листинг 3. Пример S-выражения языка CIDF

По внешнему виду язык CIDF является лиспоподобным. Его основу составляют так называемые S-выражения, первым элементом которых должен быть семантический идентификатор, определяющий смысл последующих элементов. В статье [21] среди прочих приводится пример S-выражения, воспроизведенный нами на листинге 3 с небольшими изменениями.

Данное выражение означает, что в указанное время пользователь **root** удалил файл **/etc/passwd** на компьютере **main.strange.com**. Семантические идентификаторы задают действия (**Delete**) и роли (**Context**, **Initiator** и т.п.), выполняемые объектами. В результате становится понятно, что, кто, где и когда сделал.

Для организации взаимодействия между компонентами в каркасе CIDF предлагается использовать службу каталогов (LDAP). Компоненты регистрируются и афишируют виды выражений, которые они отправляют или воспринимают. Разумеется, в каталоге может быть и другая информация, например, сертификаты в стандарте X.509 и т.п.

1.4. Примеры систем активного аудита

Рассмотрим системы активного аудита, наиболее интересные с точки зрения архитектуры или реализованных в них идей. Тем, кто желает ознакомиться с перечнем и основными свойствами известных систем активного аудита, можно рекомендовать в качестве отправной точки аннотированный список [22], а также сборник ответов [16].

1.4.1. Система EMERALD

Система EMERALD (см., например, [23]) по сути является старейшей разработкой в области активного аудита, так как она вобрала в себя опыт более ранних систем - IDES и NIDES, созданных в Лаборатории информатики Стэнфордского исследовательского института.

EMERALD расшифровывается как Event Monitoring Enabling Responses to Anomalous Live Disturbances – мониторинг событий, допускающий реакцию на аномалии и нарушения. EMERALD включает в себя все компоненты и архитектурные решения, необходимые для систем активного аудита, оказываясь тем самым не только старейшей, но и самой полной разработкой как среди исследовательских, так и среди коммерческих систем.

Строго говоря, EMERALD является не готовым продуктом, а программной средой, которая строится по модульному принципу. Основным «кирпичиком» служит монитор (рис. 1.6).

Каждый монитор включает в себя компонент распознавания сигнатур злоумышленных действий, компонент выявления аномальной активности,

решатель, выбирающий способ реагирования на нарушения, а также описание контролируемого объекта. Каждый монитор настраивается по описанию и следит за своим объектом. Мониторы распределяются по информационной системе, образуя иерархию. Отметим, что контролируемые объекты могут иметь как системную, так и сетевую природу. Таким образом, совокупность мониторов может покрыть «всех и каждого».

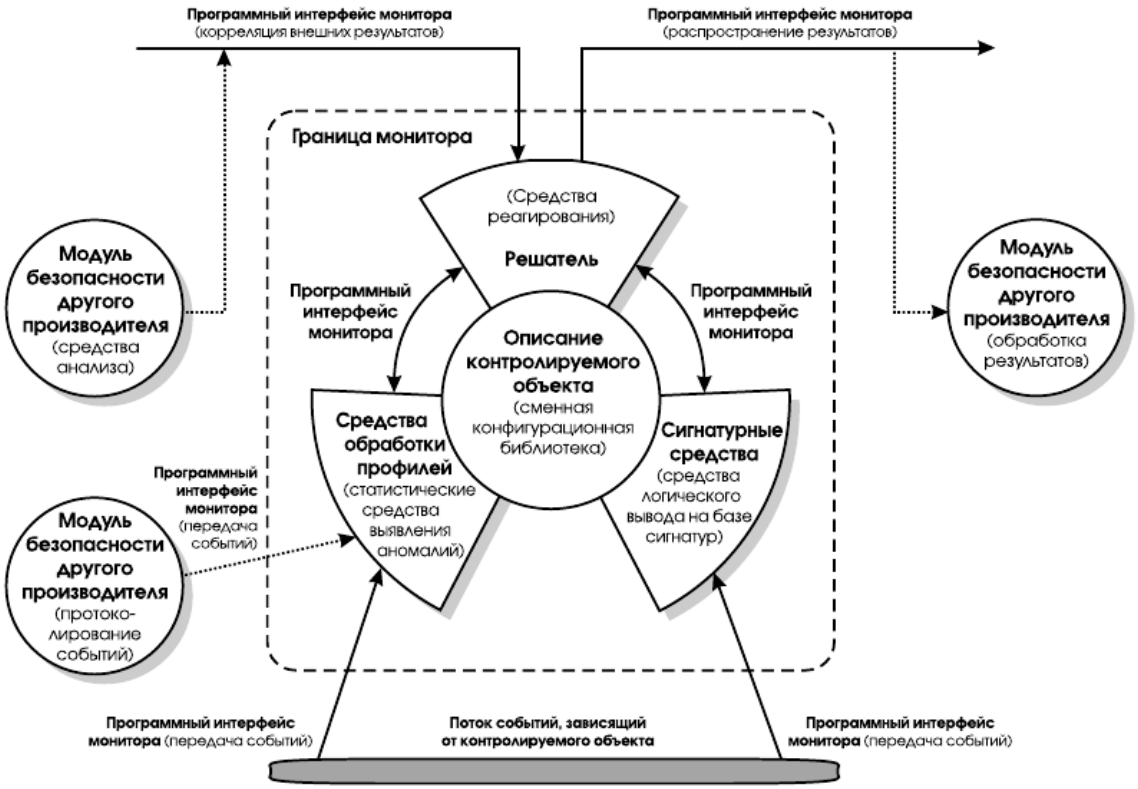


Рис. 1.6. Модуль системы EMERALD и его возможные связи

В общем случае мониторы системы EMERALD развертываются динамически, после чего в реальном времени контролируют поведение инфраструктурных и/или прикладных сервисов. Данные для анализа могут собираться как «пассивным» чтением регистрационных журналов или сетевых пакетов, так и с помощью активных проб. Результаты анализа могут направляться в асинхронном режиме другим мониторам.

По сути, в разделе «Методы проведения активного аудита» было рассмотрены архитектурные и реализационные решения, принятые в

системе EMERALD. Для распознавания сигнатур злоумышленных действий используется экспертная система P-BEST, а выявление аномальной активности основано на применении четырех классов величин (категориальных, непрерывных, показателей интенсивности, распределениях). Статистическому анализу подвергается поведение не пользователей, а сервисов. Профили сервисов существенно меньше и они гораздо стабильнее, чем у пользователей. В результате удалось заметно снизить ошибки первого и второго рода, то есть пропуск нарушений политики безопасности и возбуждение ложных тревог.

В среде EMERALD изначально существуют описания для элементов инфраструктуры (маршрутизаторы, межсетевые экраны) и прикладных сервисов (FTP, SMTP, HTTP и т.д.). Это означает, что, наряду с гибкостью и расширяемостью, EMERALD в достаточной степени удобен для быстрого развертывания в типичной информационной системе.

Одной из важнейших новаций системы EMERALD является корреляционный анализ сигналов тревоги, поступающих от разных мониторов. Такой анализ проводится по четырем категориям:

- выявление общих характеристик;
- исследование одного события с разных точек зрения;
- выявление связей между сигналами тревоги;
- выявление тренда (детерминированной составляющей).

По мнению разработчиков, результаты, полученные при создании системы EMERALD, выглядят обнадеживающими. EMERALD годится не только для активного аудита, но и для решения других задач информационной безопасности и управления (например, поддержания высокой доступности или анализа поведения сети). Иерархическая организация мониторов и корреляционный анализ помогают выявлять скоординированные, распределенные атаки. Система EMERALD производит очень сильное впечатление.

1.4.2. Система NFR

Система NFR (Network Flight Recorder), как и EMERALD, привлекает, прежде всего, архитектурной и технологической правильностью.

NFR относится к числу сетевых систем, существующих в виде свободно распространяемого инструментария и коммерчески «упакованного» продукта NFR Intrusion Detection Appliance. С внешней точки зрения NFR представляет собой либо одну станцию, осуществляющую мониторинг сегмента сети, к которому она подключена, либо совокупность таких станций с центральной управляющей консолью. Однако наиболее интересна не внешняя, а внутренняя архитектура NFR, превосходно описанная в статье [24].

Строго говоря, NFR — это нечто большее, чем система выявления подозрительной сетевой активности. Правильнее рассматривать ее как компонент сетевого управления, одним из аспектов которого является борьба с нарушениями политики безопасности (равно как и со сбоями и отказами оборудования и программного обеспечения).

Основные компоненты внутренней архитектуры NFR показаны на рис. 1.7. Один или несколько сетевых сенсоров ((packet suckers в терминологии NFR) поставляют данные решателю, который эти данные фильтрует, реассемблирует потоки, при обнаружении нарушений реагирует на них, а также передает информацию поддерживающему сервису для сохранения с последующей статистической обработкой и обслуживанием запросов. Поддерживающий сервис может также просматривать переданную ему информацию на предмет выявления сигнатур злоумышленных действий.

Разумеется, для всех стыков определены программные интерфейсы, так что возможна, например, смена или добавление сенсора или поддерживающего сервиса. "Отвязывание" поддерживающего сервиса от сбора и первичного анализа регистрационной информации позволяет

распределять нагрузку, чтобы сложная обработка не тормозила процессы, от которых требуется работа в реальном масштабе времени.

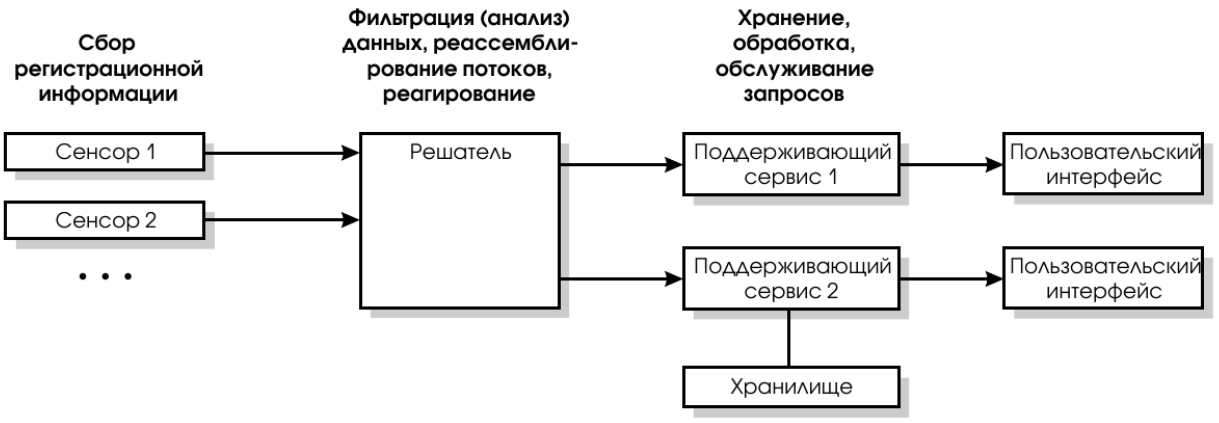


Рис. 1.7. Основные элементы архитектуры NFR

Ядром NFR является решатель, а основой решателя — язык описания фильтров, который называется N. Это универсальный язык программирования, содержащий переменные с областями видимости, списочные типы данных, управляющие структуры, процедуры. Кроме того, в N есть специфические типы данных, такие как IP-адрес. Любопытно отметить, что под значения разного рода счетчиков отводится по 64 разряда, что освобождает от проблем переполнения даже в больших сетях.

N - интерпретируемый язык. Программы, написанные на N, переводятся в байт-коды для простой стековой машины. Такие программы (и, следовательно, фильтры) оказываются весьма компактными. Что касается скорости интерпретации, то при достаточно высоком уровне базовых операций она оказывается не намного ниже, чем при выполнении скомпилированной программы. Кроме того, применяемый при интерпретации N-программ механизм ленивых вычислений позволяет избежать лишних операций, обычно сопутствующих проверке сложных условий.

В N заложены знания о структуре сетевых пакетов и протоколах более высоких уровней. Например, допустимы обращения вида ip.src, tcp.hdr или syslog.message.. Возможно и обращение к произвольным частям пакетов. В

принципе, на N можно написать интерпретатор любого прикладного протокола.

На листинге 4 приведен пример совсем простого фильтра, выбирающего запрашиваемые клиентом по протоколу HTTP локаторы ресурсов.

Этот фильтр анализирует TCP-соединения с серверным портом 80, ищет в потоке данных цепочку символов "CBT", записывает все от места совпадения до пробела в поле tcp.bytes (предполагается, что это и будет URL), после чего отправляет поддерживающему сервису исходные и целевые IP-адреса и номера TCP-портов, а также выявленный URL.

В данном случае разыскиваемый шаблон весьма прост. Подчеркнем, что язык N позволяет сделать его сколь угодно сложным.

Программы на N, поддерживающий сервис, интерпретатор могут генерировать сигналы тревоги, для обработки которых существует специальная программа, работающая в фоновом режиме. Эта программа на основе ассоциированной информации определяет дальнейший маршрут и приоритет сигналов тревоги.

```
filter server tcp (client, port: 80, start: "GET ", stop: " ") {
     record    ip.src,    ip.dst,    tcp.sport,
     tcp.dport, tcp.bytes to urlRecorder;
}
```

Листинг 4. Фильтр на языке N, фиксирующий запрашиваемые пользователем локаторы ресурсов

NFR не является универсальной системой активного аудита, но представляет несомненный интерес, прежде всего, как хорошо сделанный строительный блок, который можно установить в управляющую среду, объединить со средствами выявления подозрительной активности на хостах и т.п. Язык N обладает достаточной мощностью и для записи сигнатур атак с учетом возможных вариаций,

2. РАЗРАБОТКА АЛГОРИТМА АКТИВНОГО АУДИТА ИНФОРМАЦИОННОЙ СИСТЕМЫ

2.1. Метод обнаружения атак, основанный на нейросетевых подходах

Традиционные методы обнаружения атак, такие, как сигнатурный метод или метод обнаружения аномалий, не позволяют достичь оптимальных характеристик обнаружения внутренних атак. Нейросетевые методы обнаружения атак в принципе позволяют достичь приемлемых характеристик, однако обладают такими недостатками, как трудность выбора параметров и структуры нейронных сетей, ресурсоемкий характер обучения нейронной сети, сложность дообучения и переобучения нейронной сети.

Поэтому возникает необходимость в выборе и применении метода, который позволил бы избежать указанных выше недостатков при допустимом уровне надежности обнаружения внутренних атак. Анализ показал, что достаточно перспективным для этих целей является построение систем активного аудита на основе технологий искусственных иммунных систем. Этот подход обладает рядом преимуществ по сравнению с другими методами, обеспечивая:

- высокую скорость работы;
- сравнительно простой алгоритм обучения;
- низкую ресурсоемкость.

Под "активным аудитом" понимается непрерывный системный процесс проверки информационных систем (ИС) на соответствие декларируемым целям политики безопасности, организации обработки данных, норм эксплуатации средств вычислительной техники, а также автоматического реагирования на выявленные отклонения. Таким образом, "система активного аудита" сочетает в себе как элементы традиционных систем аудита

(сканеров безопасности), так и элементы систем обнаружения и предотвращения вторжений.

2.2. Функциональная модель системы активного аудита

Функциональная модель IDEF0 системы активного аудита состоит из блоков "собрать информацию", "обработать информацию", "выявить нарушение политики безопасности" и "реагировать на нарушение". Данные блоки отражают различные функции системы активного аудита, включая функции сбора информации, обнаружения атак и выработки реакции на атаку. Поскольку состояние защищенности ИС зависит от совокупности происходящих в этой сети событий, ее функционирование описывается с помощью нечеткой сети Петри. Для этого определяется множество

$$S = \{S_1, S_2, S_3, S_4, S_5\} \quad (1)$$

где S_1 – состояние нормального функционирования ИС;

S_2 – состояние атаки на ИС, при котором злоумышленник воздействует на ИС с целью нарушения еè нормального функционирования;

S_3 – состояние нарушения конфиденциальности ресурсов ИС;

S_4 – состояние нарушения целостности ресурсов ИС;

S_5 – состояние нарушения доступности ресурсов ИС.

Определяется множество событий в ИС

$$K = \{K_1, ..., K_6\} \quad (2)$$

где K_1 – событие появления злоумышленника;

K_2 - множество событий, приводящих к нарушению конфиденциальности;

K_3 – множество событий, приводящих к нарушению целостности;

K_4 – множество событий, приводящих к нарушению доступности;

K_5 – множество событий срабатывания средств защиты ИС;

K_6 – множество событий восстановления ИС после атаки.

Множество событий в ИС представляет собой объединение множеств указанных выше событий в ИС, т.е.:

$$K = K_1 \cup K_2 \cup K_3 \cup K_4 \cup K_5 \cup K_6 \quad (3)$$

Нечеткая сеть Петри (НСП), описывающая поведение ИС, представляется в виде:

$$C_j = (N, f, \lambda, m_0) \quad (4)$$

где N – структура НСП, $N = (P, T, I, O)$;

$f = \{f_1, ..., f_u\}$ – вектор значений функции принадлежности нечеткого срабатывания переходов, $f_j \in [0,1],\ j = 1, ..., u$;

$\lambda = (\lambda_1, ..., \lambda_u)$ – вектор значений порогов срабатывания переходов, $j_j \in [0,1],\ j = 1, ..., u$;

m_0 - вектор начальной маркировки, $m_i^0 \in [0,1],\ i = 1, ..., n$.

Структура НСП $N = (P, T, I, O)$ при этом аналогична структуре традиционных сетей Петри и может быть представлена следующими элементами (рис. 2.1):

$P = \{p_1, ..., p_n\}$ – множество позиций НСП;

$T = \{t_1, t_2, ..., t_u\}$ – множество переходов НСП, $u \in N$;

I – входная функция переходов, $I : P \times T \to \{0,1\}$;

O – выходная функция переходов, $O : T \times P \to \{0,1\}$.

Сформулируем базу правил нечеткого логического вывода, определяющих условия срабатывания переходов НСП. Каждому предикату из составленных правил сопоставляется определенная позиция НСП. Каждой позиции $P = \{p_1, ..., p_n\}$ сопоставляются элементы множеств S и K:

$$P = \{S_1, K_1, S_2, K_2, K_3, K_4, K_5, S_3, S_4, S_5, K_6\}$$

Определяется вектор начальной маркировки:

$$m_0 = \left(m_1^0, m_2^0, m_3^0, m_4^0, m_5^0, m_6^0, m_7^0, m_8^0, m_9^0, m_{10}^0, m_{11}^0\right)$$

Здесь $m_0^i (i = 1,3,8,9,10)$ – значения функций принадлежности наличия маркеров в позициях $S_{1..5}$, т.е. значения функций принадлежности определяющих различные состояния ИС;

m_2^0 - значение функции принадлежности наличия маркера в позиции K_1, т.е. фактически вероятность появления злоумышленника в ИС;

$m_j^0 \ (j = 4,5,6)$ – значения функций принадлежности наличия маркеров в позициях $K_2, K_3 K_4$, т.е. значения функций принадлежности возникновения событий, приводящих к нарушению конфиденциальности, целостности и доступности информации в ИС;

m_7^0 – значение функции принадлежности наличия маркера в позиции K_5, т.е. фактически вероятность корректной реакции на атаку средств активного аудита;

m_{11}^0 – значение функции принадлежности наличия маркера в позиции K_6, т.е. вероятность правильной реакции средств восстановления после атаки.

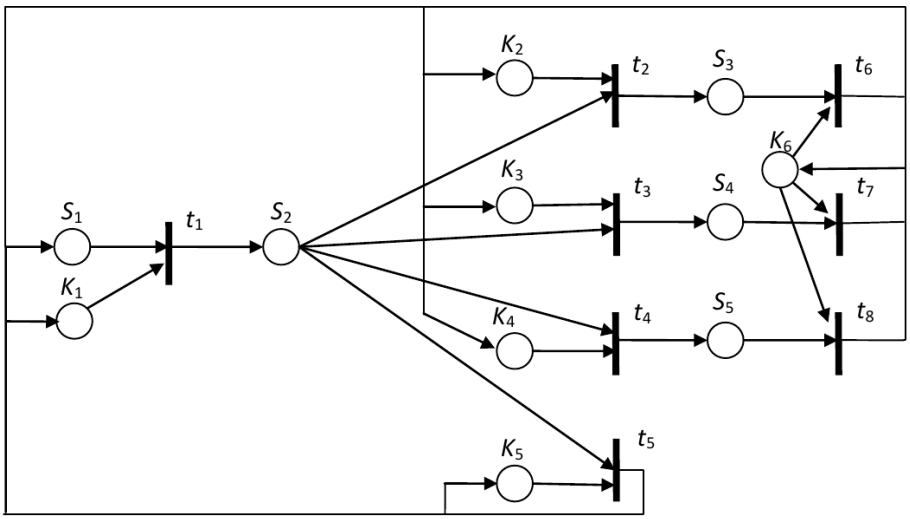


Рис. 2.1. Структура нечеткой сети Петри

Примем следующие значения функций принадлежности:

$$m_1^0 = 1,\ m_{3,8,9,10}^0 = 0,\ m_{4,5,6}^0 = 1,\ f_{1-8} = 1.$$

Динамика изменения маркировок НСП определяется следующими правилами:

1) правило определения текущей маркировки. Любое состояние НСП определяется вектором m, компоненты которого интерпретируются как значения функции принадлежности наличия одного маркера в соответствующих позициях НСП;

2) правило активности перехода. Переход $t_k \in T$ НСП является активным, если выполнено условие:

$$\frac{\min}{\left(i \in \{1,2,...,n\}\right) \wedge \left(I(p_i, t_k) > 0\right)} \frac{\{m_i\} \geq \lambda_k}{} \tag{5}$$

3) правило нечеткого срабатывания перехода. Если переход $t_k \in T$ НСП является активным, то нечеткое срабатывание приводит к новой маркировке m^v компоненты вектора которой определяются следующим образом:

$$m_i^v = 0,\ \left(\forall p_i \in P\right) \wedge \left(I(p_i, t_k) > 0\right),$$

$$m_j^v = \max\left\{m_j,\ \min\left\{m_i,\ f_k\right\}\right\},\quad \left(\forall p_i \in P\right) \wedge \left(I(p_i, t_k) > 0\right)$$

$$i \in \{1,2,...,n\} \wedge \left(I(p_i j_k) > 0\right)$$

Отмечается, что при начальной маркировке переход t_1 является активным при

$$m_2^0 \geq \lambda_1 \tag{7}$$

т.е. в случае, если вероятность появления злоумышленника будет больше порога срабатывания перехода t_1. Далее производится анализ следующих переходов в информационной системе. Если условие (7)

выполняется, тогда нечеткое срабатывание перехода t_1 приведет к новой маркировке m_1. При этом $m_1^1 = m_2^1 = 0$, поскольку позиции S_1 и K_1 являются входными для перехода. Для позиции $S_2 : m_3^1 = \max\{0, \min\{m_2^0, 1\}\}$, т.е. $m_3^1 = m_2^0 \geq \lambda_1$. Все остальные позиции остаются без изменений. Поскольку $m_{4,5,6}^1 = 1$, то переходы t_2, t_3 è t_4 будут активными при выполнении условий $m_3^1 > \lambda_2, m_3^1 > \lambda_3, m_3^1 > \lambda_4$. Переход t_5 будет активным при выполнении условия: $\min\{m_3^1, m_7^1\} > \lambda_5$ или

$$\min\{m_2^0, m_7^0\} > \lambda_5. \quad (8)$$

Анализ выражений (7) и (8) показал, что безопасная работа ИС достигается:

а) повышением значения коэффициента λ_1, что достигается корректной настройкой правил политики безопасности ИС;

б) уменьшением значения коэффициента λ_5, который представляет собой порог чувствительности системы активного аудита. Кроме того, необходимо добиваться увеличения коэффициента m_7^1.

2.3. Структура системы активного аудита

Предложена структура системы активного аудита (рис. 2.2), которая включает в себя *набор сенсоров* для анализа и обработки информации о функционировании информационной системы и действиях пользователя, *базу данных*, в которой хранится полученная информация, *блок анализа* и обработки данных для потоковой обработки поступающих данных и выработки управляющих воздействий на информационную систему, блок реагирования, воздействующий на информационную систему, консоль администратора, журнал работы системы активного аудита.

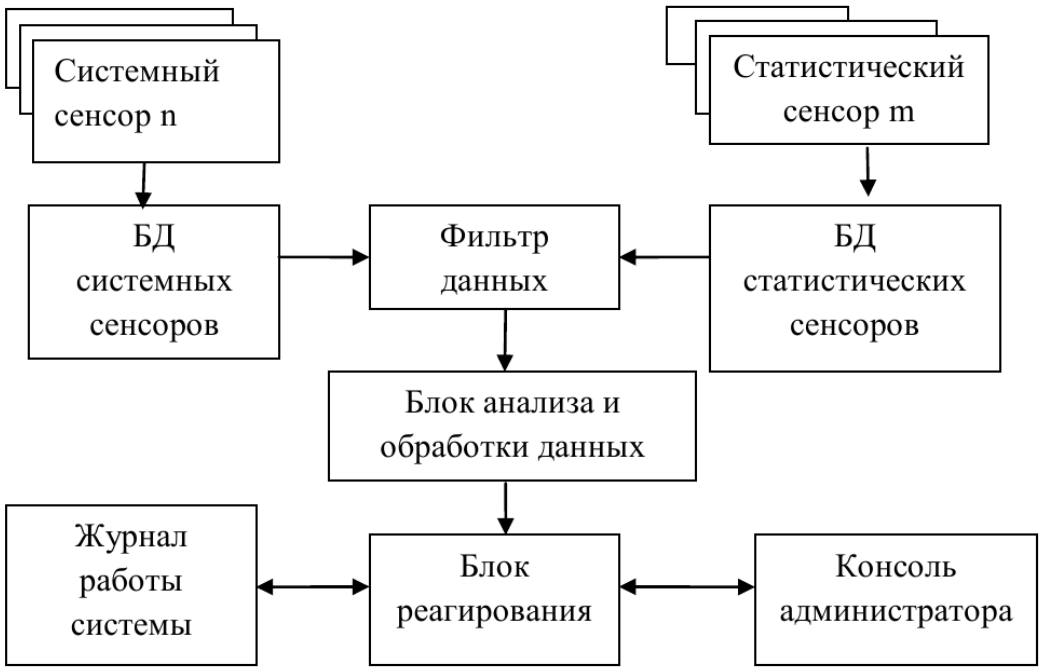


Рис. 2.2. Структура системы активного аудита

Системные сенсоры предназначены для анализа параметров системы и действий пользователя, а также выдачи предупреждений для обработки в блоке анализа и обработки данных о заранее заданных событиях, например, о попытках перебора паролей, монтирования носителей, входе/выходе пользователя из системы и т.д. Статистические сенсоры анализируют поведение каждого пользователя системы. При этом для каждого пользователя создаются отдельные профили, в которые заносятся информация о типичном поведении пользователя, собираемая в течение определенного интервала времени. Фильтр данных предназначен для удаления из очереди повторяющихся предупреждений для ускорения работы системы.

2.4. Практическая реализация прототипа системы активного аудита

Активный аудит, в зависимости от точки зрения, можно считать и весьма зрелой, и только формирующейся областью информационных технологий.

С одной стороны, исследования по выявлению подозрительной активности ведутся давно, в процессе этих исследований были получены интересные математические и программистские результаты. Исследования носят комплексный характер, они направлены на создание эффективных, гибких, расширяемых, масштабируемых систем, способных стать надежным защитным рубежом в корпоративных сетях произвольного размера. На наш взгляд, почти все необходимые концептуальные и архитектурные решения уже найдены; начинается фаза инженерной «доводки». Наиболее неисследованной областью остается обнаружение низкоскоростных, скоординированных атак из нескольких источников.

С другой стороны, коммерческие системы активного аудита появились относительно недавно и соответствующий рынок пока невелик. К сожалению, разработчики коммерческих систем предпочли «искать под фонарем», взяв на вооружение, прежде всего, звучный термин «обнаружение вторжений», но ограничившись применением самых простых методов. Часть систем является просто перелицованными сканерами безопасности, что, конечно, экономически оправдано с точки зрения производителя, но едва ли благоприятно сказывается на качестве продукта. Слишком много вариантов атак пропускается, слишком много ложных тревог генерируется, слишком много времени проходит от появления новой атаки до установки у заказчика соответствующих сигнатур.

Реальность, однако, состоит в том, что при любом взгляде на проблему выявления подозрительной активности подобные системы, несомненно, нужны. Если на самом деле обнаруживается лишь 4% атак, то это даже меньше, чем видимая часть айсберга, а ведь и сейчас статистика нарушений информационной безопасности выглядит угрожающе. Нужно находить (и наказывать) злоумышленников, нужно что-то делать с оставшимися 96% нарушений, и основная надежда связывается именно с активным аудитом (если, конечно, не считать кардинального решения в виде

революции в технологии создания больших информационно-безопасных систем).

На наш взгляд, должно пройти еще 3-5 лет, прежде чем коммерчески доступные, недорогие системы активного аудита станут реальным защитным средством, пригодным для эффективной эксплуатации массовым заказчиком, но уже сейчас их можно использовать для повышения безопасности критически важных сервисов или отдельных участков сети. Целесообразно сочетать их с более простыми средствами контроля целостности, автоматизируя реакцию на выявленные нарушения. Возможно, части организаций следует подумать о мониторинге своей информационной системы с привлечением профессионалов.

Работы в области активного аудита ведутся исключительно интенсивно. Они просто не могут не дать положительного результата. Нужно только немного подождать.

3. БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ

3.1. Анализ условий труда

3.1.1. Режим труда и отдыха

В соответствии с требованиями СНиП режим труда и отдыха организовывается в зависимости от вида и категории трудовой деятельности при работе на персональном компьютере (ПК).

Виды трудовой деятельности приведены в таблице 3.1.

Таблица 3.1 – Виды трудовой деятельности

Группа	**Вид трудовой деятельности**
А	Работа по считыванию информации с экрана с предварительным запросом
Б	Работа по вводу информации
В	Работа в режиме диалога с ПК

Большую часть рабочего времени операторы находятся в помещении операторской, но периодически операторам приходится находится в помещении автоматного зала. Для обеспечения оптимальной работоспособности и сохранения здоровья пользователей на протяжении рабочей смены устанавливаются регламентированные перерывы, продолжительность которых зависит от длительности рабочей смены, вида и категории трудовой деятельности. Перерывы входят в общее рабочее время и указаны в таблице 3.2.

Продолжительность работы с ПК без перерыва не превышает двух часов.

Рабочий день операторов составляет восемь часов. При работе с ПК в ночную смену (с 22 до 6 часов) независимо от категории и вида трудовой деятельности, продолжительность перерывов увеличивается на 60 минут.

Помещение IP-телефонии соответствует категории 1а – легкая физически, так как работа производится сидя и не требует физического напряжения, а энергозатраты организма (расход энергии при выполнении работы) составляют менее 138 ккал/ч [10].

Табл. 3.2. Категория условий труда

Категория работы с ПК	Уровень нагрузки за рабочую смену			Суммарное время регламентированных перерывов	
	Группа А, кол. знак.	Группа Б, кол. знак.	Группа В, час.	При 8-ми часовой смене	При 12-ти часовой смене
1а	до 20000	до 15000	до 2,0	30	60

Помещение автоматного зала, где располагается оборудование является помещением с повышенной опасностью, так как имеет следующие признаки:

а) температура воздуха до 30^0С;

б) влажность до 60%;

в) наличие токопроводящего пола.

3.1.2. Требования к оборудованию помещений

Так как при поступлении на аккумуляторную приходит переменный ток напряжением 380/220 В и при выпрямлении в постоянный ток напряжением 58/60 В подается на оборудование IP-телефонии, то все оборудование является электро- и пожароопасным и подлежит защитному заземлению. Соответствие устройств защитного заземления требованиям ГОСТ 12.1.030-81 “Электробезопасность. Защитное заземление, зануление” [11] устанавливается при приемо-сдаточных испытаниях после их монтажа на месте эксплуатации.

В данном случае для обеспечения электробезопасности все оборудование заземлено к выносному контурному заземлителю, расположенному по периметру здания.

В зависимости от взрывопожарной и пожарной опасности здания и помещения подразделяют на категории А, Б, В, Г, Д.

В зависимости от категории определяются соответствующие нормы по огнестойкости строительных конструкций, планировке зданий, оснащенности устройствами противопожарной защиты и другими мероприятиями.

Помещение опраторской IP-телефонии соответствует категории В (пожароопасное), так как в нем используются горючие и трудногорючие жидкости.

Учитывая высокую стоимость оборудования, а так же специфику загорания ПК в помещении установлены десять дымовых датчиков. Каждый датчик соединен с электронным блоком, который оповещает в каком помещении произошло возгорание. Согласно условиям размещения датчиков этого достаточно для данной площади помещения (один извещатель может контролировать площадь 5 $м^2$. Так же в помещении для обеспечения пожаробезопасности установлены порошковые огнетушители типа ОП-5 и ОП-10.

В зависимости от пределов огнестойкости строительных конструкций, СНиП 2.01.02-85 “Противопожарные нормы” [11], установлено восемь степеней огнестойкости зданий. Данное помещение относится к первой степени огнестойкости, так как оно находится в здании, построенном из несгораемых и трудносгораемых материалов. Минимальные пределы огнестойкости строительных конструкций первой степени приведены в таблице 3.3.

Таблица 3.3 - Минимальные пределы огнестойкости строительных конструкций

Час

Степень огнестойкости	Стены				Колонны	Лестничные пло-щадки, ступеньки и балки	Плиты, настилы и дру-гие несущие конструк-ции покрытий	Элементы покрытий	
	Несущие лест-ничных клеток	Самонесущие	Наружные несущие	Внутренние несущие				Плиты, настилы и прогоны	Балки, арки и рамы
I	2,5	1,25	0,5	0,5	2,5	1	1	0,5	0,5

3.1.3. Микроклимат помещения

Обеспечение параметров микроклимата в помещении операторов IP-телефонии. Для создания нормальных условий труда для персонала и надежности технологического процесса установлены нормы производственного микроклимата, которые приведены в таблице 3.4.

Поскольку в помещении операторской выполняется более 60%, а также исходя из категории работы, температура воздуха превышает допустимые нормы, т.е. в помещении все время находится обслуживающий персонал, который выделяет тепло.

Чтобы нормализовать микроклимат применяют системы вентиляции и кондиционирования воздуха. Но такие системы представляют дополнительную пожарную опасность для помещения, так как с одной стороны они обеспечивают подачу кислорода во все помещения, а с другой - при возникновении пожара быстро распространяют огонь и продукты горения.

Таблица 3.4 – Нормы микроклимата

Период года	Категория работ	Температура, ^{0}C				Относительная влажность			Скорость движения воздуха		
		Оптимальная	Допустимая на раб.месте		Фактическая	Оптимальная	Допустимая на рабочем месте	Фактическая	Оптимальная	Допустимая на рабочем месте	Фактическая
			Постоян-ных	Непостоян-ных							
Хо-лод-ный	1а	22-24	21-25	18-26	25-28	40-60	75 при 28^{0}C	60-65	0,1	0,1	0,1
Теп-лый	1а	23-25	22-28	28-30	28-30	40-60	55 при 28^{0}C	40-45	0,1	0,1-0,2	0,1

Оборудование IP-телефонии относится к разряду шумных. Шум согласно ГОСТ 12.1.003-83 ССБТ “Шум. Общие требования безопасности” [15] должен соответствовать требованиям, представленным в таблице 3.5.

Таблица 3.5. Допустимые уровни звукового давления

Помещение	Среднестатистические частоты активных полос, Гц								Уровни звука и эквивалентные уровни звука, дБ
	63	125	250	500	1000	2000	4000	8000	
Комната ПК	71	61	54	49	45	42	40	38	50

Действительное значение превышает допустимый уровень на 15 дБ. Для борьбы с шумом используют следующие мероприятия:

- рациональное размещение оборудования и рабочих мест;

- использование в качестве изоляции и снижения специальных крышек;
- своевременная замена изношенных деталей.

3.1.4. Естественное и искусственное освещение

Так как в помещении операторской постоянно находится обслуживающий персонал, следовательно, согласно СНиП II–4-79 “Естественное и искусственное освещение” [16] имеем естественное освещение, которое осуществляется через окна (боковое освещение).

Ввиду узких окон освещение рабочих мест операторов недостаточно и составляет – 1,7%. Нормированное значение КЕО должно составлять 2,5% [17]. Нормированное значение КЕО выбирается в зависимости от характеристики и разряда работы. Для данного объекта выполняемые работы – работы очень высокой точности. Так как освещение рабочих мест операторов от оконных проемов недостаточное, установлены светильники местного освещения для подсветки документов.

Исходя из данного анализа условий труда в помещении операторской произведем расчет параметров, не соответствующих нормированным значениям (таблица 3.6).

Табл. 3.6. – Сравнение нормированных и фактических параметров

		Нормированное значение	Фактическое значение
ОСВЕЩЕНИЕ (КЕО), %		2,5	1,7
ТЕМПЕРАТУРА, ^{0}С	Холодный период года	22-24	25-28
	Теплый период года	23-25	28-30

3.2. Организация рабочего места, оснащенного компьютером

Научно-технический прогресс внес серьезные изменения в условия производственной деятельности работников умственного труда. Их труд стал более интенсивным, напряженным, требующим значительных затрат умственной, эмоциональной и физической энергии. Это потребовало комплексного решения проблем эргономики, гигиены и организации труда, регламентации режимов труда и отдыха.

В настоящее время компьютерная техника широко применяется во всех областях деятельности человека. При работе с компьютером человек подвергается воздействию ряда опасных и вредных производственных факторов: электромагнитных полей (диапазон радиочастот: ВЧ, УВЧ и СВЧ), инфракрасного и ионизирующего излучений, шума и вибрации, статического электричества и др.

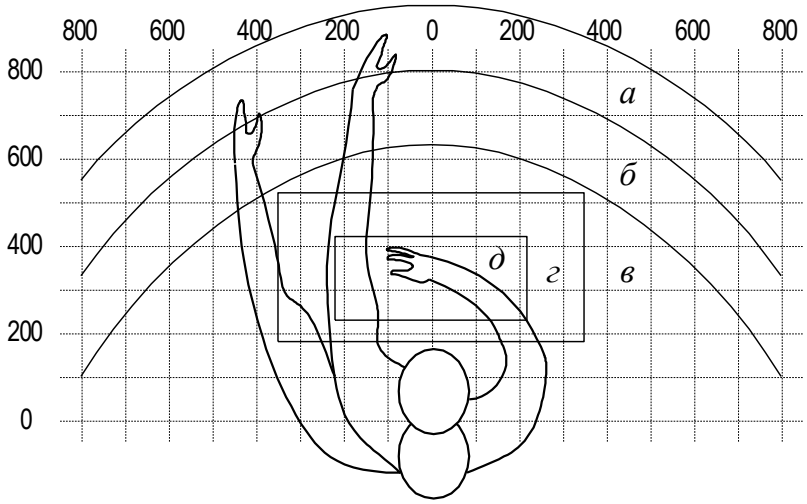
Работа с компьютером характеризуется значительным умственным напряжением и нервно-эмоциональной нагрузкой операторов, высокой напряженностью зрительной работы и достаточно большой нагрузкой на мышцы рук при работе с клавиатурой ЭВМ. Большое значение имеет рациональная конструкция и расположение элементов рабочего места, что важно для поддержания оптимальной рабочей позы человека-оператора.

В процессе работы с компьютером необходимо соблюдать правильный режим труда и отдыха. В противном случае у персонала отмечаются значительное напряжение зрительного аппарата с появлением жалоб на неудовлетворенность работой, головные боли, раздражительность, нарушение сна, усталость и болезненные ощущения в глазах, в пояснице, в области шеи и руках.

Большое значение имеет также характер работы. В частности, при организации рабочего места программиста должны быть соблюдены следующие основные условия: оптимальное размещение оборудования, входящего в состав рабочего места и достаточное рабочее пространство, позволяющее осуществлять все необходимые движения и перемещения.

Главными элементами рабочего места программиста являются стол и кресло. Основным рабочим положением является положение сидя.

Рабочая поза сидя вызывает минимальное утомление программиста. Рациональная планировка рабочего места предусматривает четкий порядок и постоянство размещения предметов, средств труда и документации. То, что требуется для выполнения работ чаще, расположено в зоне легкой досягаемости рабочего пространства (рис. 3.1.).



а - зона максимальной досягаемости;
б - зона досягаемости пальцев при вытянутой руке;
в - зона легкой досягаемости ладони;
г - оптимальное пространство для грубой ручной работы;
д - оптимальное пространство для тонкой ручной работы.

Рис. 3.1. Зоны досягаемости рук в горизонтальной плоскости

При оборудовании рабочего места (рис. 3.2.) необходимо установить монитор на специальном столике так, чтобы задняя панель была обращена к стене (так как около нее зарегистрирован максимальный уровень напряженности электрического поля), экран не должен располагаться напротив окна или других прямых источников света, дающих блики на экране.

Рис.3.2. Рекомендуемое положение во время работы за компьютером

Стол, на котором устанавливается монитор, должен быть достаточной длины, чтобы расстояние до экрана составляло 60-70 (не ближе 50) см, и в то же время можно было работать с клавиатурой в непосредственной близости от пользователя (30-40 см). Конструкция рабочей мебели (столы, кресла, стулья) должна обеспечивать возможность индивидуальной регулировки соответственно росту работающего и создавать удобную позу. Часто используемые предметы труда должны находится в оптимальной рабочей зоне, на одном расстоянии от глаз работающего. На поверхности рабочего стола необходимо разместить подставку для документов, расстояние которой от глаз должно быть аналогичным расстоянию от глаз до клавиатуры. Рабочее кресло должно иметь подлокотники. На рабочем месте необходимо предусмотреть подставку для ног.

Для того чтобы устранить блики на экране, монитор должен быть установлен перпендикулярно столу, а пользователь должен смотреть на экран несколько сверху вниз (10° от горизонтальной линии) (Рис. 4.2, 4.3). Условия освещенности в комнате играют большую роль в сохранении зрительного комфорта. С одной стороны, ничто не должно мешать восприятию информации с экрана, с другой - пользователь должен хорошо видеть клавиатуру, бумажные тексты, которыми приходится пользоваться, а

также общую обстановку и людей, с которыми приходится общаться при работе.

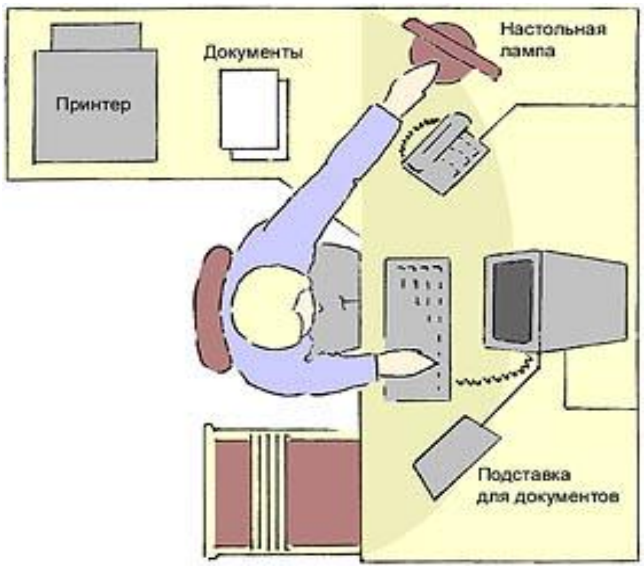
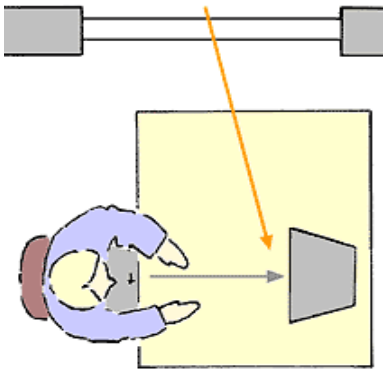
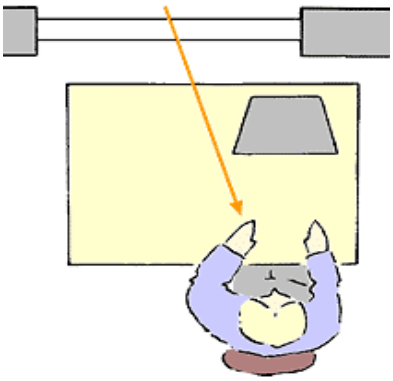


Рис.3.3. Удобное рабочее место с "Г-образным" столом

Общая освещенность в комнате не должна быть слишком большой, но и не слишком малой, она должна быть в пределах 300-500 люкс. Если помещение светлое, то окна должны иметь шторы или жалюзи. Рабочие места пользователей дисплеев желательно не располагать непосредственно у окон. Во всех случаях экран монитора следует ориентировать так, чтобы он не давал бликов, а именно - под углом к окну, близким к прямому (рис. 3.4., 3.5., 3.6.). Искусственное освещение не должно быть слишком ярким. Но помимо общих ламп, освещающих комнату, необходима местная яркая (не менее 60 Вт) лампа с хорошим плотным абажуром, освещающая только текст, с которым работает пользователь. Она должна иметь возможность ориентации в разных направлениях и быть оснащена устройством для регулирования яркости. Лампы накаливания предпочтительнее люминесцентных, т.к. последние дают пульсирующий свет, в определенных условиях усиливающий мерцание экрана дисплея.

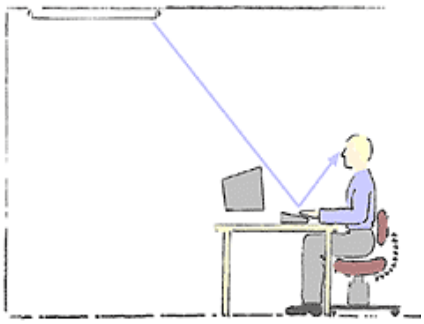


А) Линия взора параллельна окну(рекомендуется)

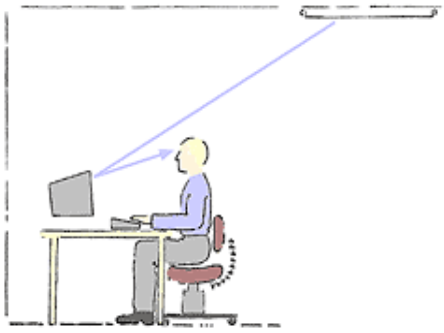


Б) Яркий свет в поле зрения(не рекомендуется)

Рис.3.4. Расположение монитора относительно окна



А) Отражение света лампы от поверхности стола и клавиатуры (не рекомендуется)



Б) Блик от лампы на экране монитора (не рекомендуется)

Рис.3.5. Расположение источника искусственного освещения относительно монитора

Рис.3.6. Правильное расположение монитора относительно стены и источника света

Перед началом работы с монитором необходимо установить с помощью рукояток наиболее комфортные контрастность и яркость на экране. Они подбираются индивидуально, так как слишком низкая контрастность и высокая яркость могут приводить к быстрому утомлению.

При подборе светового режима на рабочем месте пользователя дисплея необходимо учитывать то, что у лиц после 40 лет возникают возрастные изменения в зрительной системе (сужение зрачка, пожелтение хрусталика, снижение зрительной активности и контрастной чувствительности сетчатки). Все это требует усиления яркости экрана и дополнительной освещенности рабочего места (бумажного текста). У молодых лиц при зрительно-напряженной работе наибольшую нагрузку несет аккомодационная система глаза, которая во время работы находится в постоянном напряжении. Это может приводить к астенопическим явлениям, возникновению нарушений в аккомодационной системе глаза и, в конечном счете, к появлению и росту близорукости. Чтобы избежать этого, работа с экраном монитора должна проводиться с расстояния не менее 60-70 см, при этом напряжение аккомодации минимально.

У взрослых с близорукостью, которые постоянно носят очки, другие очки для работы с компьютером необходимы только в том случае, если в своих очках пользователь с трудом читает газетный шрифт с расстояния 60-70 см (до экрана) и 30-33 см (до печатного текста) от глаз. В случае если с одними и теми же линзами чтение с обоих расстояний невозможно, назначают бифокальные очки. [26,27].

3.3. Чрезвычайные ситуации. Защита предприятия в чрезвычайных ситуациях и ликвидация последствий Понятие о чрезвычайных ситуациях. Стадии чрезвычайных ситуаций

Известно, что любая деятельность потенциально опасна, а сами опасности носят перманентный характер (перманентный - постоянный,

непрерывно продолжающийся, от латинского permaneo - остаюсь, продолжаюсь).

Потенциальная опасность - это опасность скрытая, неопределенная во времени и пространстве. Реализуется потенциальная опасность через причины и в случае, если нежелательные последствия будут значительные, то это событие классифицируется как чрезвычайная ситуация.

Чрезвычайная ситуация (ЧС) - это обстановка на определенной территории, сложившаяся в результате аварии, опасного природного явления, катастрофы, стихийного или иного бедствия, которые могут повлечь или повлекли за собой человеческие жертвы, ущерб здоровью людей или окружающей природной среде, значительные материальные потери и нарушение условий жизнедеятельности людей.

Независимо от причин появления ЧС, в их развитии можно выделить основные пять стадий:

- *Зарождения* - возникновение условий или предпосылок для ЧС (усиление природной активности, накопление деформаций, дефектов и т.п.).
- *Инициирования* - начало ЧС. На этой стадии важен человеческий фактор, поскольку статистика свидетельствует, что до 70% техногенных аварий и катастроф происходит вследствие ошибок персонала.
- *Кульминации* - стадия высвобождения энергии или вещества. На этой стадии отмечается наибольшее негативное воздействие на человека и окружающую среду вредных и опасных факторов ЧС.
- *Затухания* - локализация ЧС и ликвидация ее прямых и косвенных последствий. Продолжительность данной стадии различна, возможны дни, месяцы, годы и десятилетия.
- *Период ликвидации* последствий.

Задачи, решаемые в ЧС. Классификация ЧС

Все ЧС можно классифицировать по трем основным принципам - масштабу распространения, темпу развития и природе происхождения.

При классификации ЧС по масштабу распространения (рис. 4.7.) следует учитывать не только размеры территории, подвергнувшейся воздействию ЧС, но и возможные ее косвенные последствия. К ним относятся тяжелые нарушения организационных, экономических, социальных и других существенных связей, действующих на значительных расстояниях. Кроме того, принимается во внимание тяжесть последствий, которая и при небольшой площади ЧС может быть огромной и трагичной.

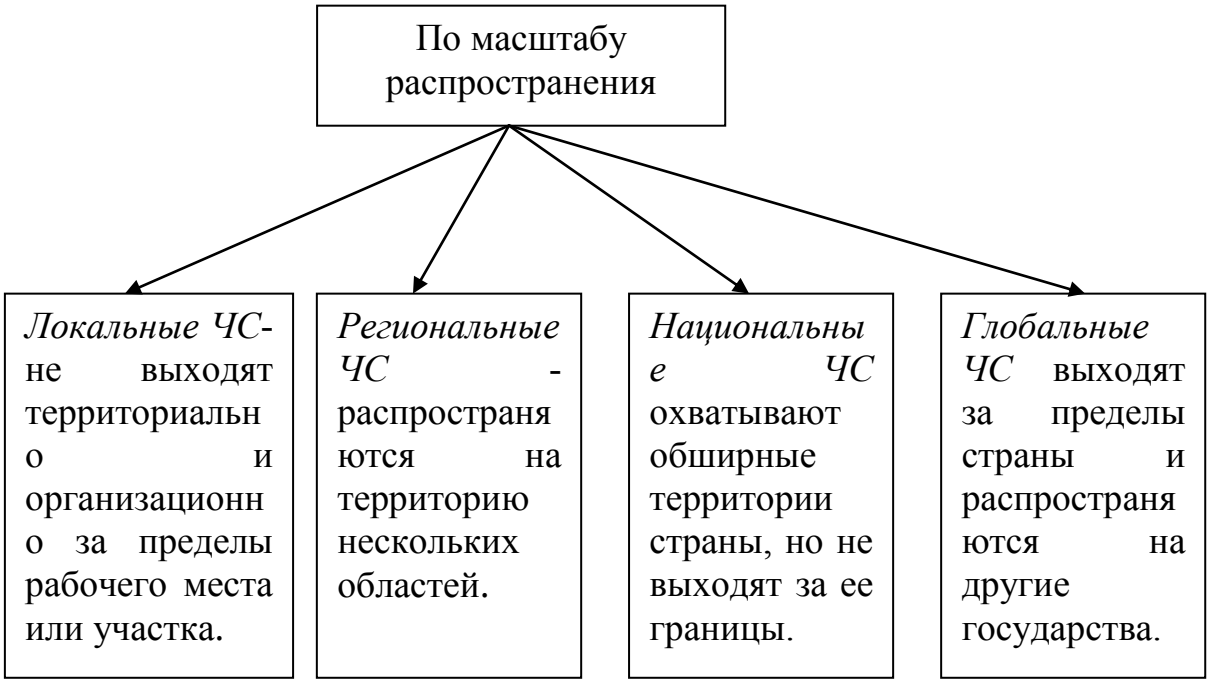


Рис.3.7. Классификация ЧС по масштабу распространения

Каждому виду ЧС свойственна своя скорость распространения опасности, являющаяся важной составляющей интенсивности протекания чрезвычайного события и характеризующая степень внезапности воздействия поражающих факторов. С этой точки зрения ЧС можно классифицировать по темпу развития (рис.3.8.).

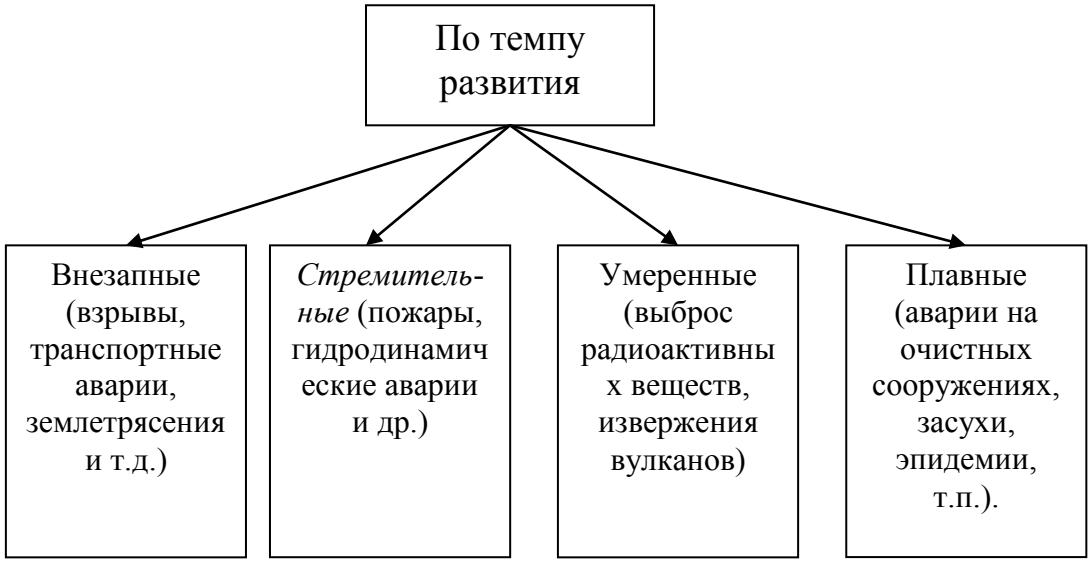


Рис.3.8. Классификация ЧС по темпу развития

Каждая ЧС имеет свои причины, в этой связи их можно классифицировать по происхождению (рис.3.9.).

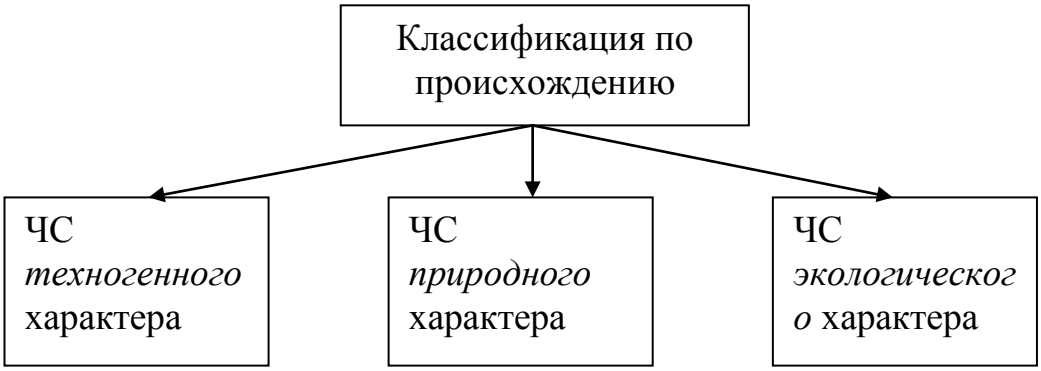


Рис.3.9. Классификация ЧС по происхождению

Заключение

1. Активный аудит можно считать только формирующейся областью информационных технологий. В процессе этих исследований были получены интересные математические и программистские результаты. Наиболее не исследованной областью остается обнаружение низкоскоростных, скоординированных атак из нескольких источников.

2. Активный аудит целесообразно сочетать с более простыми средствами контроля целостности, автоматизируя реакцию на выявленные нарушения, т.е. организации необходимо проводить мониторинг информационной системы.

3. Проведен анализ субъектов и объектов ИС на основе SADT-методологии, позволяющей представить основные процессы в ИС и ее компонентах в графическом, удобном для понимания виде. Разработана функциональная модель системы активного аудита. Функциональная модель IDEF0 системы активного аудита состоит из блоков «собрать информацию», «обработать информацию», «выявить нарушение политики безопасности» и «реагировать на нарушение».

4. Предложен алгоритм активного аудита ИС, основанные на применении технологий искусственных иммунных систем, что позволяет повысить эффективность обнаружения атак за счет отказа от использования конечного множества сигнатур известных атак и выполнить переход к использованию более общего принципа распознавания «свой - чужой».

5. Предложена структура системы активного аудита, которая включает в себя набор сенсоров для анализа и обработки информации о функционировании информационной системы и действиях пользователя, базу данных, в которой хранится полученная информация, блок анализа и обработки данных для потоковой обработки поступающих данных и выработки управляющих воздействий на информационную систему, блок

реагирования, воздействующий на информационную систему, консоль администратора, журнал работы системы активного аудита.

Список использованной литературы

1. Постановление Президента Республики Узбекистан "О мерах по дальнейшему внедрению и развитию современных информационно-коммуникационных технологий. (Собрание законодательства Республики Узбекистан, 2012 г., № 13, ст. 139).

2. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. Под ред. В.Ф. Шаньгина. - 2-е изд., перераб. и доп. - М.: Радио и связь, 2001. - 376 с.: ил.

3. Конеев И.Р., Беляев А.В. Информационная безопасность предприятия. - СПб.: БХВ-Петербург, 2003.

4. Галатенко А. Активный аудит // Jet Info. 2002, № 5.

5.. Котухов М. Нужна ли регламентация IT-аудита? // Информационная безопасность. 2004, № 4.

6. Медведовсикй И. Практические аспекты проведения аудита информационной безопасности в соответствии с лучшей западной практикой // Connect! Мир связи. 2006, № 10.

7. Вихорев С.В., Кобцев Р.Ю., Как узнать – откуда напасть или откуда исходит угроза безопасности информации // Конфидент, №2, 2001.

8. Симонов С. Анализ рисков, управление рисками // Информационный бюллетень Jet Info № 1(68). 1999. с. 1-28.

9. ISO/IEC 17799, Information technology – Code of practice for information security management, 2000

10. Экология и безопасность жизнедеятельности: Учебное пособие для студентов ВУЗов / ред. Л. А. Муравий, 2002.

11. Белов С.В. Безопасность жизнедеятельности М.: Высшая школа. 2003.

12. http://www.asoiu.narod.ru/25-1.html

13. http://www.infotex72.ru/content/zakaz/bondarev.pdf

14. http://www.osp.ru/pcworld/1997/03/157204/

15. http://mind-control.wikia.com/wiki/Быстрая_цифровая_подпись
16. http://www.aladdin.kz/476.html
17. http://www.naukaspb.ru/arhiv/v_kr_kl_sod.htm
18. http://masteroid.ru/content/view/1321/49/
19. http://masteroid.ru/content/blogsection/4/15/91/91/
20. http://books.dore.ru/bs/f11bid1736.html
21. http://lpcs.math.msu.su/ver/teaching/cryptography/2008-2009-log.html