ЧАСТЬ V

Решения и средства защиты информации

В этой части

- *Решения*
- *Средства*

Решения

26

В этой главе

- *Архитектура СЗИ*
- *Системы сетевой безопасности*
- *Комплекс обнаружения и анализа ПЭМИН*
- *Брандмауэры*

<<< Этапы	Направления >>>	010				020				030				040				050			
		Защита объектов ИС				Защита процессов и программ				Защита каналов связи				ПЭМИН				Управление системой защиты			
	Основы >>>	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства
		011	012	013	014	021	022	023	024	031	032	033	034	041	042	043	044	051	052	053	054
100	Определение информации, подлежащей защите	111	112	113	114	121	122	123	124	131	132	133	134	141	142	143	144	151	152	153	154
200	Выявление угроз и каналов утечки информации	211	212	213	214	221	222	223	224	231	232	233	234	241	242	243	244	251	252	253	254
300	Проведение оценки уязвимости и рисков	311	312	313	314	321	322	323	324	331	332	333	334	341	342	343	344	351	352	353	354
400	Определение требований к СЗИ	411	412	413	414	421	422	423	424	431	432	433	434	441	442	443	444	451	452	453	454
500	Осуществление выбора средств защиты	511	512	513	514	521	522	523	524	531	532	533	534	541	542	543	544	551	552	553	554
600	Внедрение и использование выбранных мер и средств	611	612	613	614	621	622	623	624	631	632	633	634	641	642	643	644	651	652	653	654
700	Контроль целостности и управление защитой	711	712	713	714	721	722	723	724	731	732	733	734	741	742	743	744	751	752	753	754

Архитектура системы защиты информации для АС

Рассмотрим вариант построения системы технической защиты информации, реализующей ***концепцию централизованного управления безопасностью***, для иерархической распределенной автоматизированной системы, элементами которой являются локальные вычислительные сети, реализованные на платформах Mainframe и PC в средах и с интеграцией механизмов защиты операционных систем типа OS/390, Windows NT, СУБД Oracle и DB2. Подсистема реализует автоматизированное построение моделей защищенной системы, включая модели субъектов информационной деятельности, объектов защиты и правил разграничения доступа.

Работа выполнена коллективом авторов ОАО "КП ВТИ" в составе: члена-кореспондента Академии инженерных наук Украины Будько Николая Николаевича, доктора технических наук, профессора, академика Академии инженерных наук Украины, заслуженного деятеля науки и техники Украины Матова Александра Яковлевича, кандидата физико-математических наук Дмитрука Юрия Васильевича, Короленко Михаила Петровича, члена-кореспондента Академии инженерных наук Украины, кандидата технических наук, доцента Василенко Вячеслава Сергеевича, Федченко Евгения Леонидовича, Могильного Станислава Михайловича.

Назначение ПЗИ

Для предотвращения возможности реализации угроз, в соответствии с Законами, государственными стандартами и требованиями нормативных документов в автоматизированных системах необходима разработка и использование комплексных систем технической защиты информации (ТЗИ). Требования к таким системам предусматривают централизованное управление техническими средствами на основе определенной владельцем АС политики информационной безопасности и реализующего ее конкретного плана технической защиты информации.

Определение

Совокупность организационных и инженерных мероприятий, а также программно-аппаратурных средств, которые обеспечивают защиту информации в АС, принято называть комплексной системой технической защиты информации. Именно на нее нормативными документами Системы ТЗИ возлагается задача обеспечения основных функциональных свойств защищенных АС. Она решается использованием как стандартных технических и программных средств (базового и прикладного ПО), так и специально разрабатываемых аппаратурных и программных средств ТЗИ.

Наиболее перспективными средствами защиты информации в АС являются программные средства защиты (ПСЗ). ПСЗ позволяют создать модель защищенной автоматизированной системы с построением правил разграничения доступа, централизовано управлять процессами защиты, интегрировать различные механизмы и средства защиты в единую систему, создать достаточно удобный для пользователей интерфейс администратора безопасности. Причем, с учетом сложности решения, а также необходимости комплексного использования всех автоматизированных средств ТЗИ, их эффективной управляемости, значительную часть этих средств целесообразно выделять в достаточно автономную часть комплексной системы защиты АС (специфичный функциональный компонент или подсистему). Будем называть этот компонент ***Подсистемой защиты информации*** (ПЗИ).

Подсистема защиты информации автоматизированной системы предназначена для обеспечения безопасной информационной технологии обработки, сохранения и обмена информации с ограниченным доступом, которая циркулирует в АС (обеспечения основных функциональных свойств защищенной АС, предусмотренных требованиями Нормативных документов Системы технической защиты информации, таких как конфиденциальность, целостность, доступность, наблюдаемость).

Подсистема защиты информации АС обеспечивает функциональные свойства защищенности информации АС путем реализации следующих функций:

1. Конфигурирования ПЗИ АС;
2. Администрирования объектов;
3. Администрирования ролей;
4. Ведения организационно-штатной структуры предприятия;
5. Администрирования субъектов;
6. Администрирования групп субъектов;
7. Администрирования правил разграничения доступа;
8. Регистрации событий;
9. Контроля целостности;
10. Администрирования, управления и контроля доступа к физическим ресурсам.

Реализация данных функций обеспечивается комплексным использованием (интеграции в состав ПЗИ) всех возможных средств технической защиты, включая проблемно-ориентированные средства защиты (ПОСЗ) используемых операционных систем, систем управления базами данных (СУБД), средств защиты прикладного программного обеспечения, а также механизмов защиты собственно ПЗИ.

Основной задачей ПЗИ при этом является обеспечение автоматизированного управления следующими механизмами защиты информации:

- механизмами защиты информации, встроенными в прикладное программное обеспечение АС;
- механизмами защиты информации операционных системы;
- механизмами управления доступом СУБД;
- механизмами контроля целостности информации;
- механизмами обеспечения наблюдаемости за состоянием защищённой системы;
- механизмами управления доступом к физическим ресурсам АС.

В ПЗИ АС реализованы основные технические решения концепции централизованного управления защитой автоматизированной системы, которая позволяет обеспечить определённую политику защиты информации.

Средства и механизмы обеспечения функциональных услуг безопасности

Обеспечение функциональных свойств АС, как защищённой системы, ***достигается использованием необходимой совокупности средств и механизмов защиты, которые предназначены для:***

- обеспечения конфиденциальности информационных ресурсов АС;
- обеспечения целостности информации и ресурсов АС, защита которых возложена на ПЗИ;
- обеспечения доступности информации и ресурсов АС механизмами Подсистемы защиты информации в части управления через средства ПОСЗ ограничениями на количество данных, объектов, которые выделяются отдельному пользователю или группам пользователей, и механизмами прикладного программного обеспечения;
- обеспечения наблюдаемости всех подконтрольных для ПЗИ процессов, связанных с циркулированием информации и использованием ресурсов АС.

Модель защищенной системы

Одной из основных задач системы защиты информации есть обеспечение автоматизированного формального построения правил разграничения доступа пользователей и процессов к информационным ресурсам АС на основе определенной политики безопасности. Правила разграничения доступа являются абстрактным механизмом, который выступает посредником при любом взаимодействии субъектов и субъектов — процессов с объектами автоматизированной системы и есть наиболее существенный элемент политики безопасности. Правила разграничения доступа вместе с моделью субъектов и моделью объектов составляют модель защищенной системы. Структура модели защищенной системы представленная на рисунке 26.1.

Модель защищенной системы включает:

- модель субъектов информационной деятельности;
- модель объектов защиты;
- правила разграничения доступа (ПРД).

Субъектами информационной деятельности АС являются:

- функциональное руководство АС;
- администраторы безопасности АС;
- администраторы функциональных подсистем АС;
- пользователи ресурсов АС;
- внешние системы АС;
- обслуживающий персонал АС.

Правила разграничения доступа определяются установленной собственником АС политикой безопасности и состоят в предоставлении полномочий субъектам АС на доступ к ресурсам, которые ограждаются, а также в установлении типов доступа субъектам к объектам защищенной системы. На основе такой информации внутренними алгоритмами проверки полномочий ПОСЗ реализуется санкционирование доступа субъекта к объекту. Таким образом обеспечивается доверительный и административный принципы управление доступом.

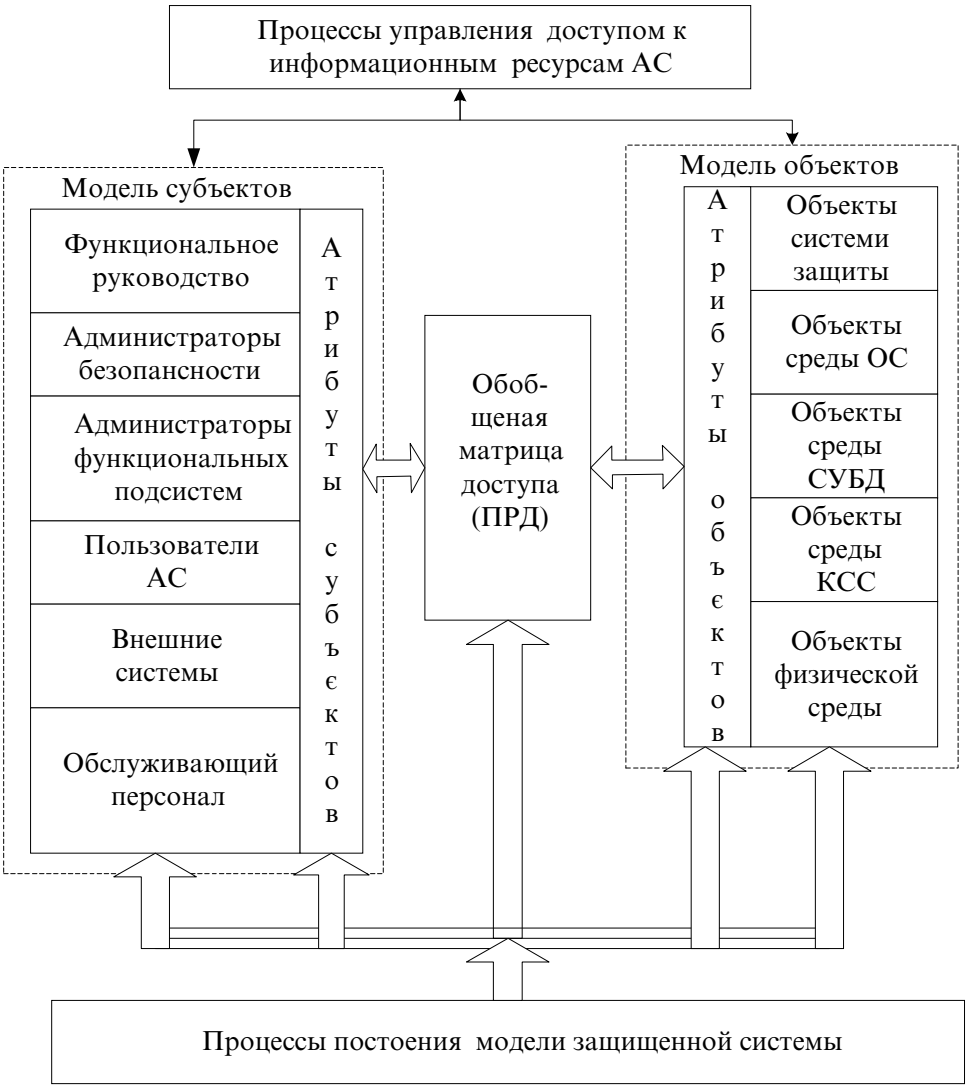
Правила разграничения доступа должны формально описывать все возможные отношения каждого субъекта из множества субъектов к каждому объекту из множества объектов и определять режим доступа субъекта к объекту.

Для формализации построения правил разграничения доступа целесообразно применять обобщенную матрицу доступа. Обобщенная матрица доступа является трехмерной матрицей. Трехмерность обобщенной матрицы доступа обусловленная наличием множества разнородных проблемно — ориентированных средств защиты, которые интегрируются в единую модель управления доступом.

Для любой ПОСЗ в обобщенной матрице доступа строится своя двумерная матрица доступа с учетом особенностей режимов доступа и типов объектов, которые защищаются механизмами защиты данного ПОСЗ. Такая матрица устанавливает также способ (тип) реагирования на попытки нарушения ПРД.

Объектами защиты ПЗИ АС являются:

1. Сведения (независимо от вида их представления), отнесенные к ИсОД или к другим видам информации,



Примечание: КСС- комуникационная сеть связи

РИСУНОК 26.1. *Структура модели защищенной системы*

которые подлежат защите (например, информация о лице в соответствии с Законом о персональных данных), обработка которых осуществляется в АС и которые могут находиться на бумажных, магнитных, оптических и других носителях.

2. Объекты среды операционных систем и СУБД(системные ресурсы любого из узлов АС и элементов коммуникационной сети связи — операционные системы OS/390 (AIX), Windows NT (Windows 2000), СУБД Oracle, DB2).

3. Объекты системы защиты (информационные ресурсы любого из узлов АС — наборы данных и файлы операционных систем OS/390 (AIX), Windows NT (Windows 2000), информационные массивы и базы данных — объекты СУБД Oracle, DB2 и резервные копии), а также прикладные ресурсы (программное обеспечение любого из узлов АС, в том числе его резервные копии).

4. Объекты среды коммуникационной сети связи (информационные данные и отдельные сообщения, которые передаются в каналах коммуникационной сети связи АС);

5. Объекты физической среды (оснащение и прочие физические ресурсы АС — серверы и прочие средства вычислительной техники, прежде всего, их терминальное оснащение, системные блоки, носители информа-

ции, коммуникационные каналы и коммуникационное оснащение, средства печати, другие устройства ввода/вывода, накопители информации, зоны безопасности — здания и помещение, где расположенные элементы АС и т.п.).

Следует предусматривать, что вместе эти объекты могут быть привлекательными для несанкционированного доступа со стороны тех или других нарушителей с использованием тех или других каналов и видов угроз ресурсам ЄДАПС.

Архитектура ПЗИ

Архитектура ПЗИ представлена на рис. 26.2. В ее состав, как элементы, входят компоненты (в свою очередь, каждый из компонентов может также состоять из элементов или компонент), каждый из которых предназначен для реализации определенного набора услуг. Совокупность таких услуг обеспечивает все основные функциональные свойства защищенных АС.

Ядро Подсистемы защиты информации — совокупность компонент, которая реализует основные принципы функционирования и управления ПЗИ, правила взаимодействия ее компонент, позволяет гибко конфигурировать состав средств обеспечения защиты в зависимости от динамично изменяющихся условий эксплуатации АС и модели угроз системе. ***В составе ядра можно выделить:***

1. Компонент ***контроля доступа к сервисам ПЗИ*** реализует функции генерации сеансовых ключей для каждого подключения к серверу ПЗИ, контроля полномочий администраторов на выполнение команд управления процессом защиты и ведения базы данных полномочий администраторов.

2. Компонент ***управления ПЗИ*** реализует функции управления и контроля за функционированием ее ядра.

3. Компонент управления конфигурацией ПЗИ реализует функцию ведения внутренней базы данных, определяющую текущую структуру активных средств защиты и ключевые параметры их взаимодействия, правил разграничения доступа к ресурсам самой Подсистемы защиты информации, настройки внутренней базой данных параметров функционирования других компонент, реализующих ПЗИ.

4. Компонент ***диагностики и тестирования*** обеспечивает контроль целостности и, при необходимости, восстановление целостности программных средств самой ПЗИ, а также локализацию ошибок при сбоях и авариях. Обеспечивает тестирование и диагностику при старте системы, при восстановлениях после сбоев и по запросу администратора безопасности.

5. Компонент ***управления транзакциями*** реализует функции поддержки транзакционной модели выполнения команд ПЗИ, т. е. команда считается выполненной успешно только в том случае, если успешно выполнены все составляющие ее операции. В случае система должна быть возвращена в исходное состояние; необходима синхронизация базы данных модели защищенной системы и реального состояния защищенной системы.

6. Компонент ***ведения базы данных ПЗИ*** реализует функции: интерпретации команд ПЗИ в команды управления данными; поддержки эффективного функционирования базы данных ПЗИ (настройка индексов, оптимизация запросов); резервирования и восстановления базы данных ПЗИ после сбоев.

7. Компонент ***расширенного аудита базы данных ПЗИ*** реализует функции: визуального построения и выполнения сложных запросов по базе данных Подсистемы защиты информации (аудит модели системы, аудит журнала событий); представления результатов запросов в любой удобной для Администратора безопасности форме с выводом результатов на дисплей или принтер в формате наиболее распространенных текстовых редакторов; анализ базы данных Подсистемы защиты информации с применением методов искусственного интеллекта с целью выявления "узких" мест в защите АС или попыток несанкционированного доступа.

8. Компонент ***обеспечения интерфейсов с внешними средствами защиты*** реализует функции: установления и поддержки связи с активными компонентами управления средствами контроля физического доступа; управления средствами контроля целостности и криптографической защиты и компонентами управления средствами защиты базового и прикладного программного обеспечения; предоставления сервисов подходящего компонента управления в зависимости от команды, полученной от компоненты построения и реализации модели защищенной системы.

Для централизованного управления защищенной системой служат компоненты, обеспечивающие деятельность администраторов ПЗИ в составе:

1. Автоматизированного рабочего места (АРМ) администратора ПЗИ, которое реализует функции предоставления графического интуитивного интерфейса администратора; выдачи визуальных или звуковых предупреждений о событиях имеющих критическое влияние на безопасность системы.

2. Компонент взаимодействия с удаленными АРМ Подсистемы защиты информации реализует функции предоставления сервисов ПЗИ для удаленного использования; защиты потока информации между компонентами ПЗИ и удаленным АРМ (в том числе и с использованием криптографических методов).

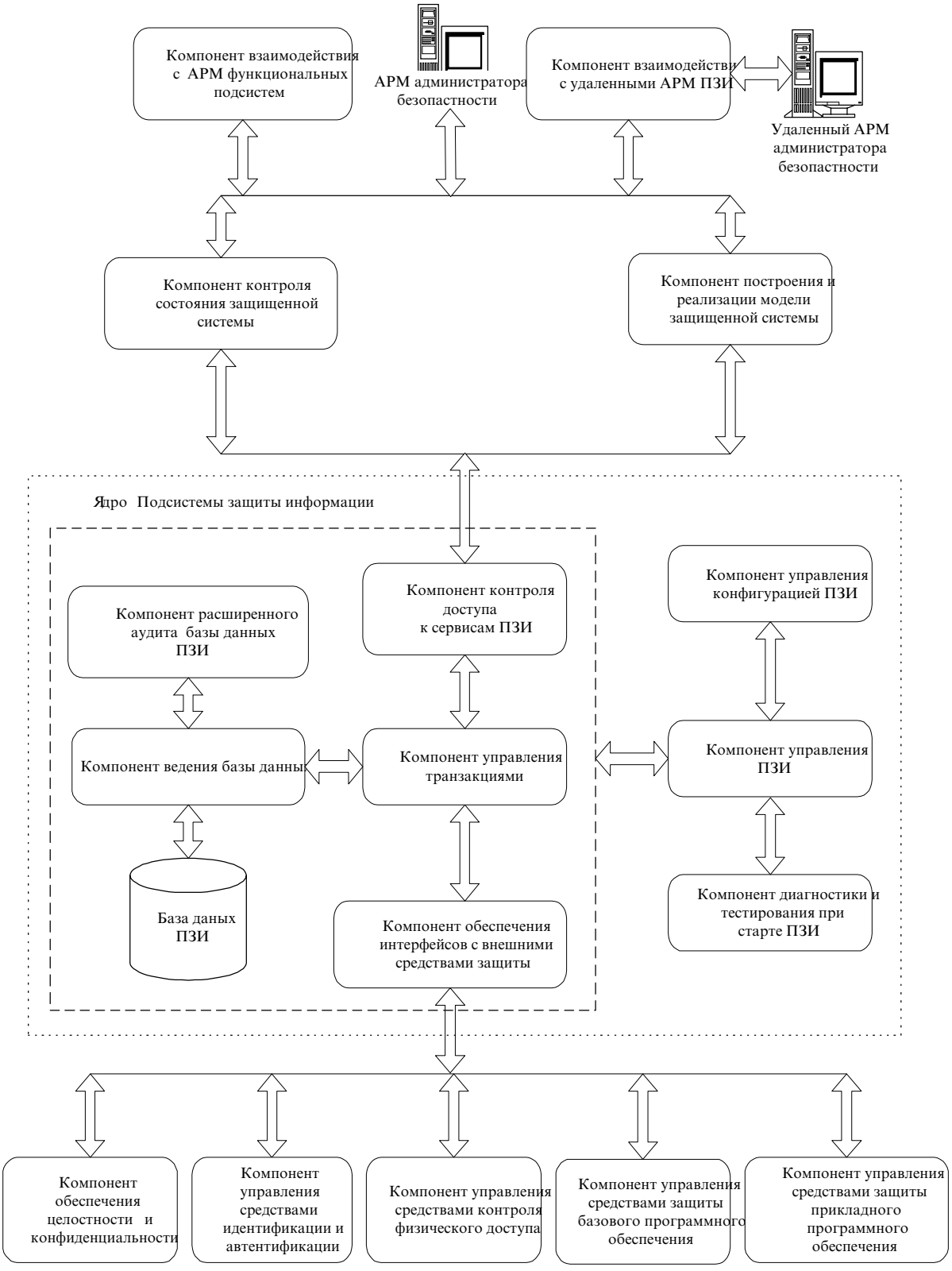


РИСУНОК 26.2. *Архитектура Подсистемы защиты информации*

3. Компонент взаимодействия с АРМ функциональных подсистем реализует функции управления потоком информации между ПЗИ информации и АРМ функциональных подсистем, а именно: АРМ администратора базы данных, АРМ администратора программно-технического комплекса (ПТК), АРМ администратора телекоммуникаций и сетей.

4. Компонент построения и реализации модели защищенной системы реализует функции: автоматизированного построения модели защищенной системы, т. е. создание структуры объектов, субъектов и правил разграничения доступа в соответствии с выбранной политикой безопасности для данной защищенной системы; ведения классификаторов типов объектов, субъектов, режимов доступа и полномочий субъектов; ведения классификаторов событий. Созданная модель может быть реализована (спроецирована) в защищенной системе вне зависимости от прикладного и базового программного обеспечения, которое используется непосредственно для реализации функций АС.

5. Компонент контроля состояния защищенной системы реализует функции: ведения журнала событий, влияющих на состояние безопасности защищенной системы; отслеживания и обработки критичных событий (передача команд на выдачу визуальных и звуковых сообщений АРМ Подсистемы защиты информации, выдача команд на блокирование компонент АС, сигнализирующих о критических событиях и т. д.); предоставление средств управления правилами отслеживания событий для отдельных компонент АС (полный контроль, контроль событий с определенной степенью критичности и т. д.).

Для реализации услуг и механизмов защиты или управления защищенной системой используются компоненты:

1. Компонент управления средствами идентификации и аутентификации реализует функции: управления сервисами идентификации и аутентификации, реализованными в ПЗИ, включая средства идентификации и аутентификации базового или прикладного программного обеспечения АС (NTLMSSP, Kerberos); предоставления сервисов идентификации и аутентификации базовому или прикладному программному обеспечению АС, в случае, если данные сервисы не реализованы или их использование нежелательно (невозможно) по каким либо причинам.

2. Компонент обеспечения целостности и конфиденциальности реализует функции: управления доступом к ресурсам АС, управления сервисами контроля и восстановления целостности, а также криптографических преобразований, реализованными, в том числе, и базовым или прикладным программным обеспечением АС; предоставления сервисов обеспечения целостности и конфиденциальности базовому или прикладному программному обеспечению АС, в случае, если данные сервисы не реализованы или их использование нежелательно (невозможно) по каким либо причинам

3. Компоненты управления средствами защиты базового программного обеспечения (при их наличии) реализуют функции: интерпретации команд Подсистемы защиты информации в команды управления средствами защиты базового программного обеспечения; прием и обработка сообщений о события от средств защиты базового программного обеспечения.

4. Компоненты управления средствами защиты прикладного программного обеспечения реализуют функции: интерпретации команд Подсистемы защиты информации в команды управления средствами защиты прикладного программного обеспечения; прием и обработку сообщений о событиях от средств защиты прикладного программного обеспечения.

5. Компонент управления средствами контроля физического доступа реализует функции: интерпретации команд Подсистемы защиты информации в команды управления средствами контроля физического доступа; прием и обработку сообщений о событиях от средств контроля физического доступа.

Предложенная архитектура может служить основой для построения типовых ПЗИ в автоматизированных системах, обеспечивая при этом возможность интеграции различных средств и механизмов защиты с целью обеспечения основных функциональных свойств защищенной системы.

Система сетевой безопасности и мониторинга "ЗАХИСНИК"

Компания "Геос-Информ"
http://www.geos-inform.com,
E-mail: info@geos-inform.com

Система сетевой безопасности и мониторинга "ЗАХИСНИК" представляет собой комплексную систему, позволяющую реализовать функции защиты данных, контроля действий пользователей и администрирования.

Система состоит из подсистем:

1. защиты данных
2. аудита действий пользователей и работы приложений
3. администрирования и настройки
4. создания и печати отчетов
5. централизованного хранения и репликации данных

Каждая подсистема представляет собой независимый модуль или группу модулей, каждый из которых можно использовать по отдельности, при этом максимальный эффект достигается только при использовании всех подсистем.

Подсистема защиты данных (ПЗ)

ПЗ реализует функции:

Санкционирование доступа

- На этапе старта рабочей станции производится запрос имени и пароля пользователя. В случае ввода корректного имени и пароля загрузка системы продолжится. Если же имя или пароль будут введены некорректно, процесс загрузки рабочей станции прекратится.
- При наличии аппаратного модуля выполненного в виде ISA платы расширения, встроенной внутрь рабочей станции, процесс аутентификации пользователя произойдет до этапа загрузки операционной системы. Более того, загрузка с любого типа носителя будет невозможной до успешной аутентификации пользователя.
- В случае использования системы без платы расширения, процесс аутентификации произойдет сразу после начала загрузки операционной системы. При этом полностью исключить возможность загрузки операционной системы с типов носителей, отличных от жесткого диска, невозможно.
- При наличии устройства считывания Smart Card, пользователь будет идентифицироваться путем предъявления личной карты.
- При использовании подключаемого к параллельному порту аппаратного ключа, его уникальный код будет использован при идентификации пользователя. Без этого ключа загрузка системы будет невозможна.
- Допустимо также санкционирование доступа по времени: для каждого дня недели Администратор может задать интервалы времени, в течение которого доступ в систему будет разрешен. Вне указанных интервалов доступ в систему будет запрещен.

Разграничение доступа

- к локальным файлам. Файлам на локальной машине присваивается набор атрибутов, определяющий режимы доступа пользователей к этим файлам.
- к сетевым ресурсам. Для каждого пользователя определяется перечень сетевых ресурсов и атрибуты доступа к ним. При этом атрибуты доступа не должны превышать полномочий доступа к ресурсам, указанных на файловом сервере. Разграничение доступа производится для любого типа сетевых ресурсов, размещенных на серверах произвольного типа.
- к принтерам. Каждому пользователю можно разграничить доступ к сетевым и локальным принтерам.
- к ресурсам Internet. Для каждого пользователя можно вести список узлов и страниц Internet, доступ к которым запрещен. При задании таких узлов можно использовать символы шаблона, например, *kiev.ua.
- к системным настройкам. Допускается запрещать пользователю изменение конфигурации операционной системы и оборудования, в частности: настроек сети, аппаратного обеспечения, рабочего стола, установленных приложений.

Контроль целостности объектов

Наряду с атрибутами доступа, с объектами связан уровень контроля целостности этих объектов:

- Контроль выключен: целостность объекта не контролируется.
- Контроль по требованию: целостность объекта контролируется только при выполнении операции контроля пользователем или Администратором.
- Контроль автоматический: целостность объекта контролируется при каждом старте системы.

Более того, допускается указание любой совокупности реакций системы безопасности при обнаружении нарушения целостности объекта:

- занесение события в журнал;
- предупреждение пользователя;
- немедленное предупреждение администратора;
- блокировка работы;

Электронный документооборот

Для реализации механизма защищенного электронного документооборота реализованы следующие возможности:

- Ведение защищенной базы данных пользователей, рабочих станций, групп пользователей и компьютеров, категорий пользователей.
- Для каждого пользователя и категории пользователей хранится пара ключей: секретный и открытый; секретный ключ защищается ключевой фразой пользователя.
- При посылке файла требуется открытые ключи пользователей получателей документа.
- Для подписи документа используется электронная цифровая подпись. Для подписи документа пользова-

тель вводит свою ключевую фразу и расшифровывает этим свой секретный ключ.

- Пользовательский интерфейс оформлен как расширение Windows Explorer, позволяющий выполнять шифрование и расшифрование файлов из контекстного меню, а проверку ЭЦП в виде дополнительного листа свойств для зашифрованных файлов.
- Проверка подписи осуществляется непосредственно из дополнительного листа свойств и при расшифровке документа.

Статическое шифрование данных

Подсистема реализует следующие функции:

- Шифрование и расшифрование файлов пользователей с помощью алгоритма ГОСТ 28147-89 имеющего ключ размером 256 бит. Одноразовый ключ алгоритма генерируется с помощью датчика псевдослучайных чисел для каждого шифруемого файла отдельно.
- Таблица замен алгоритма едина для всей организации и хранится в подсистеме централизованного хранения и репликации данных (ПЦ).
- Реализацию криптографически стойкого алгоритма разделения доступа к файлу различных пользователей с помощью алгоритма RSA.
- Для каждого пользователя системы генерируется пара ключей алгоритма RSA размером в 1024 бита, которые в дальнейшем будут называться открытым и секретным ключом пользователя.
- Открытый ключ пользователя хранится в подсистеме ПЦ.
- Секретный ключ пользователя в зависимости от конфигурации системы может храниться:
- В подсистеме централизованного хранения данных;
- В смарт карте, iButton или другом физическом идентификаторе пользователя, позволяющем хранение ключевой информации;
- Файл пользователя шифруется алгоритмом ГОСТ с помощью одноразового ключа.
- Для каждого пользователя, которому должен быть доступен файл, одноразовый ключ шифруется с помощью алгоритма RSA с помощью открытого ключа пользователя-получателя.
- Для каждой категории пользователей, которой должен быть доступен файл, одноразовый ключ шифруется супомощью алгоритма RSA с помощью открытого ключа категории.
- Для файла рассчитывается два значения хеш-функции — для открытых данных и для зашифрованных данных.

Динамическое шифрование данных

Система динамического шифрования дисков представляет собой многофункциональную комплексную систему, позволяющую реализовать все необходимые функции защиты данных. ***Система состоит из следующих подсистем:***

- Набор драйверов виртуальных дисковых контроллеров и виртуальных дисков;
- Приложение для администрирования, управления и создания шифрованных дисков.

Каждая подсистема представляет собой независимый модуль или группу модулей, каждый из которых можно использовать по отдельности, при этом максимальный эффект достигается только при использовании всех подсистем.

Система сетевой безопасности и мониторинга "Инспектор"

Компания "Геос-Информ"
http://www.geos-inform.com,
E-mail: info@geos-inform.com

Система сетевого мониторинга "ИНСПЕКТОР" представляет собой многофункциональную комплексную систему, позволяющую реализовать все необходимые функции контроля действий пользователей, администрирования, конфигурирования параметров пользователей и рабочих станций.

Место предлагаемых решений в общей структуре СЗИ показано на рис. 26.3. в виде соответствующих элементов матрицы знаний

Система состоит из следующих подсистем:

- Подсистема аудита действий пользователей и работы приложений
- Подсистема администрирования и настройки
- Подсистема создания и печати отчетов
- Подсистема централизованного хранения и репликации данных

Каждая подсистема представляет собой независимый модуль или группу модулей, каждый из которых можно использовать по отдельности, при этом максимальный эффект достигается только при использовании всех подсистем. Далее будут детально рассмотрены функциональные возможности каждой подсистемы.

Подсистема аудита действий пользователей и работы приложений (ПА) позволяет отследить:

- Работу пользователей и приложений с файлами
- Печать документов на сетевых и локальных принтерах

<<< Этапы	Направления >>>	010				020				030				040				050			
		Защита объектов ИС				Защита процессов и программ				Защита каналов связи				ПЭМИН				Управление системой защиты			
	Основы >>>	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства
		011	012	013	014	021	022	023	024	031	032	033	034	041	042	043	044	051	052	053	054
100	Определение информации, подлежащей защите	111	112	113	114	121	122	123	124	131	132	133	134	141	142	143	144	151	152	153	154
200	Выявление угроз и каналов утечки информации	211	212	213	214	221	222	223	224	231	232	233	234	241	242	243	244	251	252	253	254
300	Проведение оценки уязвимости и рисков	311	312	313	314	321	322	323	324	331	332	333	334	341	342	343	344	351	352	353	354
400	Определение требований к СЗИ	411	412	413	414	421	422	423	424	431	432	433	434	441	442	443	444	451	452	453	454
500	Осуществление выбора средств защиты	511	512	513	514	521	522	523	524	531	532	533	534	541	542	543	544	551	552	553	554
600	Внедрение и использование выбранных мер и средств	611	612	613	614	621	622	623	624	631	632	633	634	641	642	643	644	651	652	653	654
700	Контроль целостности и управление защитой	711	712	713	714	721	722	723	724	731	732	733	734	741	742	743	744	751	752	753	754

РИС. 26.3. *Место предлагаемых решений в общей структуре СЗИ*

- Запуск и завершение задач
- Вход пользователей в систему и выход из нее
- Нажатия клавиш
- Установку и удаление приложений Windows
- Доступ к сетевым ресурсам
- Доступ к локальным ресурсам из сети
- Изменение данных системного реестра Windows
- Изменение конфигурации системы

ПА работает прозрачно для пользователя, передавая данные о событиях на сервер безопасности системы. В случае если сервер недоступен, данные временно сохраняются на локальной рабочей станции. Они перенаправляются на сервер, как только он становится доступным. В системе приняты меры по предотвращению уничтожения файлов событий на локальной машине, а также против деактивации агента контроля за событиями.

Подсистема администрирования и настройки (ПН) позволяет Администратору оперативно конфигурировать систему мониторинга с одного или нескольких рабочих мест. При этом ПН построена так, что Администратор может управлять рабочими станциями, а также следить за действиями пользователей в реальном времени, не отходя от своего рабочего места. При этом все сделанные изменения вступят в силу непосредственно после подтверждения Администратора. Кроме того, Администратор имеет возможность оперативно реагировать на действия пользователей: отправлять сообщения пользователям или блокировать их работу.

Создание структуры организации

Система позволяет создать иерархическую структуру организации с неограниченным уровнем подчиненности групп и подгрупп, которая рассматривается системой как дерево объектов, в котором роль групп и подгрупп могут играть этажи, отделы, звенья, комнаты, и т. д. В каждой группе находятся рабочие станции и пользователи ей принадлежащие. Каждый пользователь может быть связан с произвольным количеством рабочих станций, на которых он имеет право работать.

Настройка параметров ПА

Для произвольной связи пользователь–рабочая станция допускается настройка параметров ПА, включающая в себя перечень контролируемых действий пользователя и рабочей станции, список шаблонов файлов и приложений, подлежащих контролю, а также список шаблонов-исключений, которые не следует учитывать при ведении журнала событий. Среди них могут быть, например, файлы операционной системы, действия которых не представляют интереса при анализе работы пользователей.

Управление активными подключениями

На своем рабочем месте Администратор может оперативно получить информацию об активных (подключенных к системе) рабочих станциях, времени их работы, а также пользователях, работающих на этих станциях. При этом Администратору предоставляются возможности активного взаимодействия с пользователями и рабочими станциями, подключенными к системе:

Блокировка работы пользователя

В случае обнаружения каких-либо некорректных или опасных действий пользователя, его работу можно немедленно заблокировать для предотвращения опасных последствий.

Отправка сообщения пользователю

Служит для немедленной отправки предупреждающих или оповещающих сообщений пользователям. Данная функция реализована независимо от служб оповещений операционных систем на рабочих станциях и серверах сети.

Исполнение команды на удаленной станции

Администратору предоставляется возможность выполнить любую команду операционной системы или запустить какое-либо приложение на удаленной рабочей станции. Это позволит выполнять некоторые действия на рабочем месте пользователя без его ведома и участия. Кроме того, существует возможность передачи управления клавиатурой и мышью Администратору.

Просмотр списка активных приложений на рабочей станции

Позволяет Администратору увидеть все запущенные процессы системы и программы, в которых работает пользователь. Это дает возможность отслеживать нежелательные приложения (игры, развлекательные программы) и оперативно их завершать.

Просмотр экрана на удаленной станции

С помощью этой возможности достаточно просто увидеть изображение экрана на рабочем месте пользователя непосредственно с рабочего места Администратора. Эта операция незаметна для пользователя, поэтому пользователь не будет стараться скрыть изображение на своем мониторе путем закрытия или минимизации задач, а также путем перезагрузки или выключения рабочей станции.

Механизм оповещения администратора. Любым более или менее критическим событиям ***можно назначать различный уровень оповещения Администратора:***

- сохранение в журнале событий;
- сохранение в журнале событий с пометкой "критическое";
- блокировка работы пользователя;
- немедленное сообщение на рабочее место Администратора (с возможностью звукового сопровождения).

Подсистема создания и печати отчетов (ПО)

Основное назначение ПО — предоставить руководителю возможность контролировать работу своих сотрудников, получать информацию о том, каким образом использовалось компьютерное время. ***Подсистема обладает следующими функциональными возможностями:***

- Просмотр журнала событий;
- Создание различных отчетов;
- Задание фильтров (критериев выбора информации из базы данных);
- Создание новых и использование ранее созданных шаблонов для отбора необходимых данных;
- Расчет статистических параметров работы пользователей, просмотр полученной информации и генерирование отчетов по статистике с возможность задания фильтров и/или использования шаблонов;
- Создание/удаление программных групп и масок файлов, использующихся при создании укрупненных отчетов о работе пользователя.

Перед просмотром журнала событий, информации по статистике работы пользователей, перед созданием отчетов необходимо задать фильтры для определения критериев выбора информации из базы данных. Если для заданных критериев в базе нет ни одной соответствующей записи, результат запроса будет пустым.

Дата и время начала интересующего периода, также как дата и время окончания периода, по умолчанию совпадают с текущей датой и текущим временем. Поэтому, если результативность выполнения запроса имеет значение, хотя бы один из этих параметров желательно установить.

Для экономии времени, при дальнейшей работе наиболее часто используемые фильтры можно сохранить в базе данных как шаблон. При этом необходимо определить имя шаблона. Когда появится необходимость применить фильтры, использовавшиеся ранее, нужно будет просто загрузить шаблон с соответствующим именем.

Сгенерировать отчет можно после просмотра журнала событий или сразу же после задания фильтров.

Программа предоставляет возможность создания следующих типов отчетов:

- Полная информация о работе пользователя: перечень рабочих станций, имена файлов и программ, с которыми работал пользователь, выполненные действия;
- Полная информация о функционировании рабочей станции: имена пользователей и их действия, имена файлов и программ, к которым обращались с рабочей станции;

- Развернутый отчет по группам файлов: перечень типов файлов, с которыми работал пользователь на различных рабочих станциях, количество файлов, используемых пользователем в численном и процентном выражении;
- Краткий отчет по группам файлов: обобщенная информация о типах файлов, с которыми работал пользователь на различных рабочих станциях, количество файлов, используемых пользователем в численном и процентном выражении;
- Сведения о выполнении пользователем инсталляции программ;
- Сведения о выполнении пользователем де инсталляции программ;
- Статистика работы пользователей: время работы пользователя в конкретном приложении, расчет показателя интенсивности работы;
- Рабочее время пользователей: время работы пользователя в течение дня, расчет показателя интенсивности работы;
- Информация о времени работы компьютеров в течение дня;

При значительном объеме базы данных расчет статистических показателей работы пользователей занимает довольно много времени. Поэтому после проведения расчетов полученная информация сохраняется в базе. Просмотр статистических данных и генерация отчетов (последние три отчета в списке — по статистике) выполняются на основании этой сохраненной информации, а повторные расчеты не производятся.

Подсистема централизованного хранения и репликации данных

Организация защищенного соединения

Перед тем как какое-либо приложение пользователя системы получит право на извлечение или помещение данных в хранилище происходит процедура идентификации и авторизации пользователя приложения.

Проверка целостности компонентов системы

Каждый исполняемый или загружаемый компонент системы проверяется на целостность при его загрузке или активизации. При обнаружении нарушения целостности генерируется соответствующее критическое событие.

Для каждого приложения организуется виртуальный канал, данные по которому передаются в зашифрованном виде, для шифрования используется алгоритм ГОСТ 28147-89. Шифрование данных происходит с помощью сеансового ключа, вырабатываемого с помощью алгоритма Диффи-Хелмана (Diffie-Helman).

Создание, удаление, модификация объектов и их атрибутов

В подсистеме существуют объекты различных типов (сведения о компьютерах, пользователях, группах и т.д.). Каждый из объектов имеет набор атрибутов. С каждым атрибутом ассоциирована маска доступа, которая определяет, какой из пользователей может читать или записывать значение атрибута. Существуют атрибуты, значение которых зашифровано. При этом расшифровка значения осуществляется на компьютере получателе, используя ключевую фразу пользователя.

Синхронизация локальных данных и данных сервера

Для обеспечения возможности работы системы при отсутствии соединения с сервером на машине пользователя ведется локальная база данных. В эту базу данных помещаются сведения о пользователях, которые имеют право работы на этом компьютере.

Синхронизация данных происходит при старте компьютера или при принудительном запросе администратора.

Для минимизации затрат на сопровождение системы предусмотрена возможность централизованного обновления и замены версий.

Автоматизированный программно-аппаратный комплекс обнаружения и анализа побочных электромагнитных излучений "Астра-В"

Фирма "БУМЕКС"
Http:\\ www.security.kiev.ua
E-mail: bumeks@webber.net.ua
(044) 241-09-80, 241-09-81

Комплекс предназначен для обнаружения радиосигналов, анализа характеристик электромагнитного поля и предназначен для проведения специальных исследований на сверхнормативные побочные электромагнитные излучения (ПЭМИ), регистрации, хранения, обработки и документирования полученных результатов. Он создан на основе современного анализатора спектра, управляемого персональной ЭВМ, с использованием специального программного обеспечения.

Комплекс "Астра-В" представляет собой гибкую (настраиваемую) систему автоматизации процесса радиоизмерений, включающих в себя необходимый

спектр функций для обнаружения и анализа побочных электромагнитных излучений.

Базовый комплект комплекса состоит из следующих компонентов:

- анализатор спектра Hewllet Packard серии 8560 с опцией управления (HP-IB-интерфейс);
- IBM-совместимая ПЭВМ с платой HP-IB;
- комплект измерительных антенн;
- пакет программного обеспечения "АСТРА".

Автоматизация достигается за счет использования прикладного программного обеспечения "АСТРА", которое обеспечивает:

- дистанционное управление настройкой анализатора спектра, получение с него данных об измерении;
- пересчет полученных результатов согласно калибровочных составляющих радиотракта;
- "соединение" данных об измерениях по поддиапазонам в единый спектр;
- отображение в удобной форме результатов измерений на дисплее ПЭВМ;
- мощный механизм масштабирования отображения результатов измерения (отображение как "части" спектра так и всего спектра);
- удобный механизм анализа составляющих спектров;
- сохранение в файл и загрузку из файла результатов измерений и анализа, а также их печать;
- необходимый спектр опций для обнаружения и анализа побочных электромагнитных излучений различных объектов.

Прикладное программное обеспечение (ППО) "АСТРА" функционирует в среде Windows 9X, NT и имеет интуитивно понятный интерфейс, характерный для "стандартных" Windows − приложений, не требующих дополнительного (в области интерфейса) обучения оператора.

В состав ППО "АСТРА" входят:

- ***"Редактор устройств"*** — утилита для визуального построения, редактирования, сохранения в файл (файл описания устройства) и построения из файла информации об устройстве, входящем в состав р/тракта.
- ***"Редактор трактов"*** — утилита для визуального построения, редактирования, сохранения в файл (файл описания тракта) и считывания из файла информации о составе тракта.
- ***"Редактор файлов управления"*** — утилита для визуального построения, редактирования, сохранения в файл (файл управления анализатором) и считывания из файла информации о правилах настроения спектроанализатора на поддиапазоны, оптимизации уровня и шага шкалы в каждом поддиапазоне.
- ***"Редактор файла сценариев"*** — утилита для визуального построения, редактирования, сохранения в файл (файл сценариев измерения) и считывания из файла информации о сценариях измерения.
- ***"Программа управления и анализа"*** (ПУ) − основной модуль ППО, осуществляющий выполнение измерения и анализ результатов.

Все программы выполнены согласно стандарта Windows и имеют основные элементы управления, характерные для Windows − приложений (главное меню, элементы управления размерами окна, стандартные поля ввода и выбора, таблицы для отображения и ввода данных и т.д.).

Гибкость применения комплекса определяется уникальной возможностью оперативного изменения условий измерений, таких как:

- калибровочные характеристики составляющих тракта;
- правила настройки анализатора спектра на поддиапазоны, оптимизация REF LVL, шага шкалы и т.д.;
- идентификаторы имен спектров и результатов измерений;
- опции измерений ПЭМИН, и др.

Вариации условий измерений задаются и редактируются утилитами из ППО. Причем параметры этих условий хранятся в файлах текстового формата, что существенно упрощает их обработку любым редактором Windows.

Указанные параметры условий измерений содержатся в следующих файлах:

- файл описания Р-тракта (антенна, усилитель, коммутатор и др.), в котором хранится информация о типе устройства (под устройством понимаем и его калибровочные характеристики;
- файл описания ФТ-тракта, который содержит список ссылок на файлы описания устройств;
- файл управления анализатором, в котором сосредоточена информация о правилах настройки спектроанализатора на поддиапазоны, оптимизации REF LVL, шага шкалы уровня полосы пропускания и т.д.;
- файл сценариев измерения, в котором хранится информация о наборе сценариев измерений.

В случае необходимости многократных измерений по одним и тем же параметрам, используется специальная утилита, которая изменяет главное меню основного модуля программы, устанавливая соответствующие значения измерений "по умолчанию".

Для удобства работы оператора в измерительном комплекс "Астра-В" применяется дружественный интерфейс. На рис 26.4 изображен внешний вид экрана ПК при вызове подпункта "Вид – Изменить – Укажи рамкой"

Достоинства комплекса

Простота

Комплекс не требует от оператора НИКАКИХ ОСОБЫХ НАВЫКОВ, кроме общих знаний операционных систем WINDOWS 9.X, NT, 2000.

Автоматизация процесса измерений полностью ОСВОБОЖДАЕТ ОПЕРАТОРА от необходимости знать назначение и правила пользования органов управления анализатором спектра.

Применяемая технология настройки интерфейса в соответствии с выбранным набором сценариев измерений в сочетании с автоматической селекцией уровней сводит задачу проведения специсследований к последовательному нажатию нескольких кнопок на панели инструментов

Надежность

В составе комплекса используется оборудование ведущих “Brand Name” производителей, таких как Intel и Hewlett Paccard отличающихся ВЫСОКОЙ НАДЕЖНОСТЬЮ, низкой требовательностью к обслуживанию и условиям эксплуатации. Программное обеспечение комплекса выполнено по модульному принципу и состоит из набора полностью функциональных 32-х разрядных приложений содержащих многоуровневую систему перехвата и обработки ошибок, протестированную на платформах WINDOWS 9.X, NT 2000 в режимах реальной многозадачности.

Точность

Комплекс позволяет строить спектральную картину в любом заданном диапазоне, ограниченном только возможностями анализатора, без потери информации о гармонических составляющих сигналов. Применяемые технологии квазиодновременного измерения, уточнения указанных уровней, статистической обработки результатов измерений, а также режим ручной верификации с использованием осциллографического режима работы анализатора спектра для наблюдения демодулированного тестового сигнала с его прослушиванием через встроенный динамик позволяет производить отбор и максимально точное измерение уровней гармонических составляющих даже в условиях сложнейшей шумовой обстановки

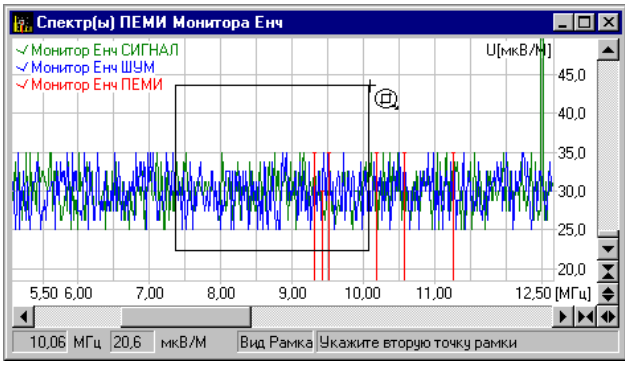


РИС. 26.4. *Вид Экрана при вызове подпункта «Вид – Изменить – Укажи рамкой».*

Безопасность структурированных кабельных систем (СКС)

ООО "Iv Кабельные системы"
E-Mail: cs@iv.com.ua
Телефон: 490-51-01
03035, Киев, Соломенская пл.2, офис 806.

Характерной чертой современных ИС является их звездообразная топология, которая обеспечивает высокую производительность сети и возможность гибкого маневра сетевыми ресурсами. Однако это обстоятельство приобретает особое значение при решении задач обеспечения информационной безопасности.

Это важно

Сосредоточение в коммуникационных центрах вычислительной сети сетеобразующих ресурсов (активного и пассивного сетевого оборудование) приводит к тому, что сетевая среда – основа децентрализованной обработки данных – становится более уязвимой к разрушающим воздействиям случайного или умышленного характера. Кроме того, в коммуникационных центрах выполняется вся работа по реализации схемы физических соединений, в них пересекаются все информационные потоки и именно там максимальна вероятность реализации угроз безопасности информации.

Таким образом, выполнение в рамках функционирования безопасной информационной технологии канонических требований конфиденциальности, целостности и доступности информации невозможно без реализации соответствующих мероприятий на самом нижнем уровне иерархии технических средств — на уровне физической среды передачи данных, которые де-факто образуют фундамент безопасности автоматизированной системы обработки информации в целом. При этом важнейшей задачей, решаемой средствами

обеспечения информационной безопасности должно быть принятие эффективных мер по защите не только отдельных информационных носителей или отдельных вычислительных средств, а всей сетевой среды, скелет которой образует структурированная кабельная система.

Основными видами угроз, которым подвергается СКС являются:

- несанкционированный доступ к ее компонентам;
- физическое разрушение ее компонентов;
- утечка циркулирующей информации по техническим каналам.

Для эффективного противостояния перечисленным видам угроз физический уровень информационной сети должен создаваться с учетом ряда принципов, гарантирующих работоспособность и прогнозируемость состояния схемы физических соединений как в штатных, так и в аварийных режимах. Этими ***основополагающими принципами являются:***

- управление доступом;
- управление реконфигурацией;
- избыточность;
- наблюдаемость;
- гарантированное восстановление;
- блокирование утечки информации по техническим каналам.

Управление доступом к коммутационным ресурсам СКС предполагает наличие процедуры предоставления персоналу права доступа к местам расположения коммутационного оборудования с документальной фиксацией каждого такого факта.

Управление реконфигурацией СКС предполагает наличие процедуры внесения изменений в схему физических соединений, включающей: разработку технологического задания на внесение изменений; выдачу предписания на выполнение изменений; уполномоченное выполнение изменений; контроль правильности внесенных изменений; актуализацию базы данных, хранящей схему физических соединений.

Избыточность предполагает дублирование всех основных компонентов СКС для повышения ее живучести и обеспечения возможности оперативного перехода на резервный компонент в критической ситуации, при этом резервирование должно трактоваться в расширенном смысле, а именно:

- резервирование соединения (например, установка трех-четырех и более однородных соединений);
- резервирование физической среды соединения (например, дублирование оптического соединения радиоканалом, соединения на витой паре — коаксиальным и т.п.);
- резервирование маршрута соединения (например, проход альтернативных кабельных трасс по разным стенам зданий, в разных шахтах и т.п.);
- резервирование центра соединения (например, организация дублирующего коммутационного центра в другом конце здания).

Наблюдаемость физических соединений СКС предполагает установление постоянного контроля за состоянием коммутационного оборудования и его ближайшего окружения с фиксацией и протоколированием всех фактов доступа к коммутационным ресурсам и внесения изменений в карту физических соединений.

Гарантированное восстановление схемы физических соединений СКС предполагает наличие комплекса организационно-технических мероприятий, обеспечивающих восстановление разрушенной схемы физических соединений СКС за нормированное время.

Проблема обслуживания и управления ресурсами СКС при определенном ее размере трансформируется в отдельную задачу, которую нельзя эффективно решать без использования автоматизированных средств. На порядок сложнее становится решение этой проблемы при необходимости обеспечить мониторинг за состоянием соединений в СКС и минимизировать время перехода на новую конфигурацию при выполнении плана аварийно-восстановительных работ в случае реализации угроз информации.

Блокирование утечки информации по техническим каналам предполагает в процессе создания ИС принятия мер, снижающих как вероятность образования технических каналов утечки информации, так и вероятность ее снятия. При этом выделяются два направления действий:

- разработка архитектурных решений по расположению компонентов СКС с учетом взаимного влияния на них цепей вспомогательных технических средств и систем для конкретной создаваемой информационной технологии, состава ее активного сетевого оборудования, режимов его работы, структуры и интенсивности потоков циркулирующей в сети конфиденциальной информации, совмещения во времени моментов обработки информации разных категорий конфиденциальности и др.;
- внедрение организационных мер и поддерживающих их технических средств по регламентации работы пользователей и технического персонала ИС с компонентами СКС.

Средства управления СКС

Особое место в ряду организационно-технических мероприятий повышения безопасности СКС занимают

автоматизированные средства управления физическими соединениями. Эти средства замыкают ***цепь технических мероприятий по обеспечению безопасности СКС на всех технологических этапах цикла обслуживания кабельной системы, включающих:***

- разработку схемы физических соединений, которая реализуется в коммутационных центрах СКС под конкретные нужды информационной технологии;
- выполнение монтажных работ по физической реализации спроектированной схемы соединений СКС или восстановление разрушенной схемы соединений;
- документирование актуального состояния всех соединений в коммутационных центрах СКС;
- мониторинг в реальном времени состояния схемы физических соединений СКС и обнаружение несанкционированного ее изменения;
- мониторинг в реальном времени за состоянием окружающей среды, в которой размещено сетевое оборудование и немедленная сигнализация при приближении величин ее параметров к критическим значениям, выход за которые может привести к отказу активного оборудования или к нарушению условий безопасной обработки в ИС конфиденциальной информации.

Сегодня на рынке оборудования СКС представлены следующие ***системы автоматизированного управления физическими соединениями СКС:***

- PatchView (производства компании RiT Technologies, Израиль);
- LANSense (производства компаний CableSoft и ITT Cannon, Великобритания);
- iPatch (производства компании Avaya, США).

Кроме того, заявления о подготовке к выпуску систем аналогичного назначения заявили компании BICC Brand Rex (Великобритания) и Panduit (США).

Использование автоматизированных средств управления СКС многократно сокращает затраты времени обслуживающего персонала на выполнение рутинной работы поиска и идентификации соединений, их верификации и документирования. Кроме того, процедуры изменения схемы физических соединений СКС выполняются быстро и безошибочно под дистанционным управлением и контролем со стороны административного персонала.

В состав программных и технических средств систем автоматизированного управления физическими соединениями входят:

- программное обеспечение рабочего места администратора сети;
- активные устройства, дистанционно управляемые по сети с рабочего места администратора — сканеры, которые хранят информацию о конфигурации физических соединений, выполненных на подключенных к сканеру коммутационных панелях;
- интеллектуальные коммутационные панели, взаимодействующие непосредственно со сканерами в процессе выполнения операций обслуживания и мониторинга физических соединений.

Программные средства рабочего места сетевого администратора упомянутых автоматизированных систем отличаются интуитивно понятным графическим интерфейсом и развитыми возможностями по созданию виртуальной модели физической архитектуры сети, ведению статистики по изменению состояния сетевых соединений, формированию отчетов и т.д.

Пример

Например, система PatchView предоставляет администратору графические средства для визуализации сетевой архитектуры на иерархических уровнях:

- комплекс задний, содержащих коммутационные центры;
- коммутационный центр, содержащих монтажные шкафы;
- монтажный шкаф, содержащий коммутационные панели и активное оборудование;
- коммутационная панель, представляющая активные и пассивные порты;
- информационный порт с формуляром, содержащем характеристики подключенного к нему терминального окончания или порта активного сетевого оборудования.

Следует особо отметить то, что использование автоматизированных средств делает процедуры управления физическими соединениями СКС быстрыми, точными и человеко-независимыми. Все варианты конфигурации физических соединений в штатных и критических режимах работы ИС готовятся заранее и хранятся в архиве. В случае реализации угроз безопасности информационной системы требуемая по плану аварийных и восстановительных работ конфигурация СКС реализуется точно и за минимальное время с использованием извлеченной из архива информации. Кроме того перечисленные системы непрерывно и постоянно производят мониторинг корректности всех физических соединений, что дает дополнительную гарантию надежности и целостности сетевой инфраструктуры.

Компания "Iv Кабельные Системы" является системным партнером восьми производителей оборудования

СКС, в том числе пяти выше упомянутых компаний, которые предлагают средства автоматизированного управления соединениями СКС, а кроме того — компаний Alcatel (Франция), Molex (США) и Reichle & De-Massary (Швейцария).

Symantec Enterprise Security

Стратегия Symantec в области защиты информации получила название Symantec Enterprise Security. Новая концепция защиты корпоративной информации позволит заказчикам построить систему информационной защиты на основе многоплатформенных решений Symantec в области защиты при работе с Internet, средств управления и администрирования и технической поддержки мирового класса. Symantec Enterprise Security также включает ***Информационную иммунную систему (Digital Immune System)***, технологию автоматического обнаружения и уничтожения вирусов и других опасных для информационной среды объектов.

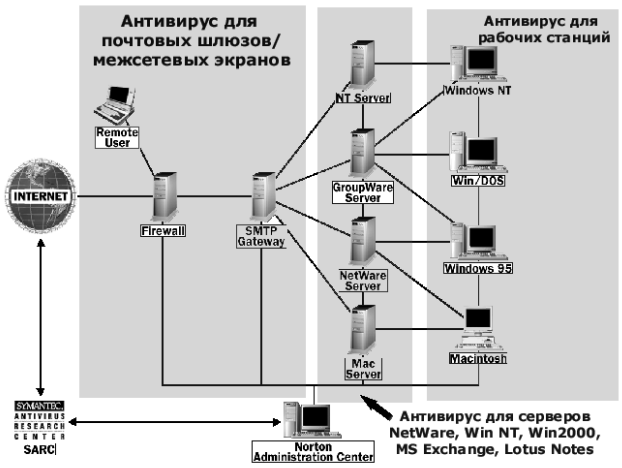
Многоуровневые и многоплатформенные продукты для обеспечения безопасности предприятий

Symantec Enterprise Security включает продукты трех основных категорий: препятствие проникновению, антивирусная защита и фильтрация содержимого Internet и электронной почты.

- Продукты Symantec для ***предотвращения проникновений*** позволяют оценивать возможность проникновения в корпоративную сеть, создавать карту сети, а также быстро и эффективно обеспечивать ее защиту на уровне рабочих станций и межсетевых экранов.
- ***Антивирусная защита*** Symantec, в основе которой лежит технология Norton AntiVirus, обеспечивает автоматическое обнаружение, анализ и уничтожение вирусов, вредоносных кодов ActiveX, Java-апплетов и других опасных объектов.
- Продукты Symantec для ***фильтрации содержимого*** включают инструменты для сканирования и фильтрации электронной почты и содержимого Internet. Эти решения позволяют компаниям защищать коммерческую и частную информацию, контролировать использование Internet, снижать риск потери информации и повышать производительность труда служащих.

Использование комплекса этих решений делает возможным определение, контроль и укрепление политики безопасности для эффективной защиты коммерческой информации предприятий.

Продукты Symantec Enterprise Security в настоящее время поддерживают платформы Windows NT, Solaris



и Windows 2000, обеспечивая эффективную защиту информации на всех возможных уровнях. Выступая в качестве единого поставщика решений, Symantec обеспечивает полную интегрированность решений, что позволяет достичь максимальной производительности систем и снизить затраты на их поддержку.

Решения в области управления и администрирования

Symantec System Center представляет собой центральную управляющую консоль, позволяющую устанавливать и администрировать антивирусные продукты Symantec Enterprise Security в масштабе всего предприятия. Symantec System Center позволяет осуществлять удаленные операции, управление по запросу, укрепление политики безопасности и создание журнала событий. Кроме того, с помощью продуктов Symantec Ghost и pcAnywhere системные администраторы смогут осуществлять удаленное управление и поддержку пользователей.

Антивирусные технологии и Информационная иммунная система Symantec (Digital Immune System)

Стало ясно, что недостаточно предотвращать заражение на одном отдельно взятом компьютере — необходимо иметь стратегию защиты всей сети. Появившаяся стратегия получила название трехуровневой.

Очевидно, что необходимо защищать точку входа в сеть из Internet, поскольку именно оттуда попадает большая часть (около 70 процентов) вирусов. Это уровень почтовых шлюзов и межсетевых экранов. Кроме того, необходимо защищать файл-сервера и сервера групповой работы, поскольку именно на них содержится наиболее ценная информация.

Безусловно, антивирус не является заменой резервному копированию, так как есть возможность оказаться в ситуации, когда резервные копии заражены, а вирус активируется спустя полгода после заражения.

Имеет смысл также защищать рабочие станции, поскольку это второй по частоте источник попадания вирусов. Даже если рабочие станции не содержат важной информации, защита снизит время аварийного восстановления.

Подобно человеческой иммунной системе, Информационная иммунная система (Digital Immune System) позволяет компьютерной сети мгновенно обнаруживать потенциально опасные участки или ненормальные условия и предпринимать необходимые меры по защите. Информационная иммунная система автоматически выявляет опасность и обеспечивает защиту для рабочей станции или всей корпоративной сети. Использование Информационной иммунной системы и сложной инфраструктуры, состоящей из аппаратных средств и архитектуры, позволит корпорациям реализовать все возможности информационных технологий.

Консалтинговые услуги Symantec

Консалтинговые услуги Symantec в области безопасности (Symantec Security Consulting Services) оказываются заказчикам с целью предложить оптимальные для них решения. Консультанты Symantec специализируются на вопросах информационной безопасности и имеют в своем распоряжении всю инфраструктуру технической поддержки Symantec. Symantec Security Consulting Services помогают организациям минимизировать нерациональное использование ИТ, обучить персонал и снизить общую стоимость владения информационными ресурсами (TCO).

Кроме того, сеть независимых поставщиков решений Symantec специалистов по безопасности обеспечивают заказчиков технической поддержкой и базой практических знаний. Партнеры Symantec в области безопасности оказывают поддержку от проверки защищенности корпоративных сетей до глобального анализа уязвимости и рисков, оценки потенциального коммерческого ущерба, разработки и внедрения плана мер по защите и дальнейшего мониторинга защищенности.

NetSonar

Компания Cisco Systems

NetSonar предназначен для сетевых администраторов и администраторов безопасности. Данный продукт представляет собой сетевой сканер, позволяющий получить полную картину структуры сети и сетевого оборудования, а также протестировать сеть предприятия на наличие уязвимых мест в системе защиты.

NetSonar анализирует все составляющие сети (активное оборудование, операционные среды, сетевые сервисы) на предмет наличия потенциальных угроз безопасности.

Основные возможности NetSonar:

- Сбор информации о сетевых устройствах.
- Анализ безопасности системы.
- Эффективное управление рисками.
- Сбор данных по результатам тестирования и генерации отчетов.
- Проверка корректности политики безопасности при инсталляции систем защиты.

Сбор информации о сетевых устройствах

NetSonar позволяет определить и протестировать защищенность следующих сетевых устройств:

- Сетевые рабочие станции на базе ОС UNIX
- Сетевые рабочие станции на базе Windows NT
- Web — серверы
- Mail — серверы
- FTP серверы
- Межсетевые экраны
- Маршрутизаторы
- Коммутаторы

По каждому устройству предоставляется полная информация: используемые компоненты, операционная система, версия ОС и т.д.

Анализ безопасности системы

Программа NetSonar производит полный анализ безопасности рабочих станций, прикладных серверов (WWW, Ftp, Mail), устройств управления доступом (серверы доступа, межсетевые экраны), а также активного сетевого оборудования (маршрутизаторы, коммутаторы). Используются как пассивные, так и активные методы тестирования.

По каждой обнаруженной угрозе безопасности формируется подробное описание, рекомендации по устранению, ссылки на другие источники.

Возможности по анализу данных и генерации отчетов

Программа NetSonar представляет широкие возможности по анализу данных включающих описание угрозы, степень риска и способы ликвидации.

При генерации отчетов используется большое число различных форматов представления данных. Возможно представление полученных данных в виде различных схем и графиков.

Дополнительные возможности

- Запуск как в интерактивном, так и в автоматическом режиме работы (по расписанию, определяемому пользователем).
- Формирование собственных правил (пользовательских сценариев) сканирования.
- Постоянно обновляемая база данных уязвимостей, доступная для загрузки в динамическом режиме.

Cisco PIX Firewall

Компания Cisco Systems

Межсетевой экран PIX компании Cisco Systems относится к классу пакетных фильтров, использующих технологию контроля состояния (stateful inspection). Он позволяет контролировать доступ как из Интернет во внутреннюю сеть, так и наоборот.

Для настройки PIX можно использовать графическую оболочку, что облегчает и упрощает этот процесс. В отличие от обычных пакетных фильтров, PIX позволяет осуществлять аутентификацию пользователей. Для аутентификации используются протоколы TACACS+ и RADIUS, которые позволяют использовать для аутентификации как обычные UNIX пароли, так и систему одноразовых паролей S/Key.

PIX позволяет поддерживать до 16 000 одновременных TCP/IP соединений и обеспечивать пропускную способность до 90 Мбит/с. PIX построен на базе сетевой операционной системы CISCO IOS, что обеспечивает полную совместимость по протоколам и средствам мониторинга и управления с оборудованием CISCO, масштабируемость сетей, построенных на базе CISCO, привычный для администраторов CISCO маршрутизаторов интерфейс.

Основные свойства

- Защита на основе технологии контроля состояния защита сетевых соединений, позволяет ограничить неавторизованных пользователей от доступа к сетевым ресурсам.
- Технология перехвата соединений на прикладном уровне позволяет обеспечить аутентификацию пользователей с использованием стандартных протоколов TACACS+ и RADIUS
- Поддерживает более 16,000 одновременных соединений
- Удобный и простой менеджер межсетевых экранов обеспечивает легкое администрирование нескольких межсетевых экранов PIX
- Поддержка третьего сетевого интерфейса для поддержки открытых для пользователей Интернет сервисов типа WWW, электронной почты и др.
- Поддержка протокола Point-to-Point Tunneling Protocol (PPTP) компании Микрософт для реализации виртуальных корпоративных сетей (VPN)
- Поддержка протокола Oracle SQL*Net для защиты приложений клиент/сервер
- Командный интерфейс, присущий CISCO IOS системе
- Высокая надежность благодаря возможности дублирования и горячего резерва
- Трансляция сетевых адресов (NAT) согласно RFC 1631
- Трансляция портов (PAT) позволяет расширить пул адресов компании — через один IP адрес можно отображать 64000 адресов (16,384 одновременно)
- Псевдонимы сетевых адресов позволяют отобразить перекрывающиеся IP адреса в одно адресное пространство
- Для зарегистрированных IP адресов можно отменить режим трансляции адресов, что позволяет пользователям использовать их настоящие адреса
- Прозрачная поддержка всех распространенных TCP/IP сервисов — WWW, FTP, Telnet и т.д.
- Поддержка мультимедийных типов данных с использованием трансляции адресов и без нее, включая Progressive Networks' RealAudio, Xing Technologies' Streamworks, White Pines' CuSeeMe, Vocal Tec's Internet Phone, VDOnet's VDOLive, Microsoft's NetShow, VXtreme's Web Theater 2
- Поддержка приложений для работы с видеоконференциями, совместимыми с H.323 спецификацией, включая Internet Video Phone (Intel) и NetMeeting (Микрософт)
- Возможнсоть фильтрации потенциально опасных Java апплетов
- Защищенная система реального времени
- Поддержка нескольких уровней входа в систему
- Поддержка прерываний (trap) SNMP протокола

- Сбор аудита через syslog утилиту
- Поддержка Management Information Base (MIB) для syslog
- Аудит использования URL и обменов по FTP протоколу
- Поддержка удаленного вызова процедур (RPC)
- Программа контроля почтового траффика позволяет отказаться от размещения внешнего почтового сервера в демилитаризованной зоне (DMZ)
- Защита от SYN атак защищает хост от атак типа "отказ в обслуживании"
- Трансляция NetBIOS протокола обеспечивает поддержку взаимодействия клиентов и серверов Microsoft Networking через PIX
- Две аппаратные платформы (PIX и PIX10000) позволяют обеспечить производительность от 45 Мбит/с до более чем 90 Мбит/с

Основные преимущества

Строгая защита

В основе работы PIX лежит алгоритм адаптивной защиты (ASA), который обеспечивает защиту соединений с контролем состояния. ASA отслеживает адреса источника и назначения, порядковые номера TCP соединений, номера портов и дополнительные TCP флаги для каждого пакета. Эта информация заносится в таблицу и все входящие и выходящие пакеты сравниваются со значениями в таблице. Это дает возможность прозрачной работы с Интернет внутренним пользователям и в то же время защищает внутреннюю сеть от несанкционированного доступа. Кроме того, в PIX используется встроенная система реального времени, которая по уровню защиты превосходит стандартные открытые системы вроде UNIX.

Аппаратная расширяемость

Строгая защита, обеспечиваемая операционной системой реального времени, дополняется возможностью расширения аппаратных возможностей. В первую очередь это возможность встраивания третьего сетевого интерфейса. Это позволяет разместить за ним доступные извне WWW сервера, почту, сервера доменных имен. Другим применением третьего интерфейса может быть размещение за ним серверов, которые фильтруют содержимое пакетов. Размещения этих приложений, тербующих значительных вычислительных ресурсов, на отдельной платформе, обеспечивает как высокий уровень защиты, так и высокую производительность.

Производительность системы аутентификации

Межсетевые экраны PIX обеспечивают производительность намного выше, чем конкурирующие продукты. Высокая скорость обеспечивается за счет сквозных (cut-through) proxy. В отличие от обычных proxy серверов, которые анализируют каждый пакет на уровне приложений согласно семиуровневой модели OSI (что отнимает много времени и ресурсов процессора), PIX запрашивает у сервера TACACS+ или RADIUS информацию для аутентификации. Когда пользователь ввел свое имя и PIX проверил права доступа, образуется прямое соединение между сторонами и контролируется только состояние сессии. Таким образом, производительность PIX благодаря сквозным proxy много выше, чем у обычных proxy-серверов.

Еще одним фактором, который тормозит работу обычных proxy-серверов является то, что для каждой TCP сессии последний должен запустить отдельный процесс. Если работают 300 пользователей, должно быть запущено 300 процессов, а эта процедура занимает значительные ресурсы процессора. PIX может поддерживать более 16000 сессий одновременно. При полной загрузке PIX модели 10000 поддерживает пропускную способность 90 Мбит/с (два T3 канала)

Низкая удельная стоимость

Удельная стоимость PIX оказывается гораздо ниже, чем для большинства систем защиты.

Во-первых, PIX благодаря наличию менеджера межсетевого экрана прост в установке и конфигурации, при этом сеть необходимо отключать только на непродолжительное время. Кроме того, PIX разрешает прозрачный доступ для мультимедийных приложений, что позволяет избежать модификации параметров рабочих станций — довольно неприятной процедуры.

Во-вторых, расширенные возможности по сбору статистики помогают понять и контролировать использование ресурсов. При помощи менеджера межсетевого экрана легко генерировать отчеты с описанием даты и времени соединения, полного времени соединения, статистики по пользователям (байты и пакеты), порты и другую важную информацию. Эти отчеты можно использовать в системе учета для различных подразделений.

В-третьих, сопровождение PIX достаточно дешево. Поскольку системы с proxy-серверами в основном базируются на UNIX платформах, компании должны содержать высокооплачиваемых специалистов. Кроме того, поскольку большинство предупреждений CERT (Computer Emergency Response Team) имеют отношение к UNIX системам, компании должны затрачивать

усилия для изучения этих предупреждений и инсталляции патчей. PIX базируется на небольшой, защищенной системе реального времени, не требующей серьезных ресурсов для сопровождения. Поскольку все программное обеспечение PIX загружается из FLASH памяти, не требуется жестких дисков, что обеспечивает более высокий срок службы и период времени между ошибками.

В-четвертых, межсетевые экраны PIX обеспечивают высокий уровень масштабируемости, поддерживая от 64 (минимум) до более чем 16000 одновременных соединений. Это позволяет защищать инвестиции пользователей, поскольку при росте компании можно заменить версию на более высокую.

В-пятых, наличие сквозных proxy позволяет снизить затраты, время и деньги за счет использования базы данных сервера доступа компании, использующего TACACS+ или RADIUS

IntranetWare

Компания Novell

Система IntranetWare предназначена для компаний, которые собираются использовать Internet и интрасети для распространения информации и обеспечения доступа к ней. IntranetWare включает в себя NetWare 4.11, Novell Web Server, Netscape Navigator, NetWare MultiProtocol Router (MPR) и IPX/IP Gateway. MPR и шлюз IPX/IP обеспечивают две линии защиты от несанкционированного доступа к внутренней сети из Internet или из корпоративной интрасети.

NetWare MPR — маршрутизатор с фильтрацией пакетов — обеспечивает первую линию обороны для сети на базе IntranetWare. Используя загружаемый модуль FILTCFG.NLM (утилиту, работающую на сервере MPR), можно сконфигурировать маршрутизатор таким образом, чтобы он фильтровал входящие и исходящие пакеты в соответствии с IP-адресами и номерами портов отправителя и получателя. NetWare MPR может также фильтровать пакеты, генерируемые FTP, HTTP и Telnet.

Шлюз IPX/IP — естественный брандмауэр который обеспечивающий вторую линию защиты для сетей IntranetWare. Основное назначение этого шлюза заключается в том, чтобы дать возможность IPX-клиентам использовать сервисы Internet и интрасети, не устанавливая на их компьютерах стек протоколов TCP/IP. Вместо этого файл WINSOCK.DLL на клиентской машине "вкладывает" пакеты TCP в пакеты IPX (а не IP). Перед передачей пакетов на внешний хост шлюз IPX/IP удаляет из них IPX-заголовки и заменяет их IP-заголовками. "С точки зрения" внешнего хоста, все пакеты, передаваемые из данной сети, имеют единый IP-адрес шлюза, благодаря чему осуществляется эффективная защита от внешнего хоста сети IntranetWare.

Файл WINSOCK.DLL делает работу шлюза IPX/IP "прозрачной" для пользователей. При работе с браузером Netscape Navigator пользователю достаточно ввести имя хоста, например www.novell.com. Все действия по преобразованию имени в реальный IP-адрес выполняются шлюзом IPX/IP и DNS, после чего шлюз устанавливает от имени пользователя соединение с внешним хостом и в процессе обмена информацией заменяет IPX-заголовки на IP и наоборот.

Шлюз IPX/IP также имеет встроенный механизм контроля доступа. Сетевой администратор может ограничивать исходящие пакеты в соответствии с IP-адресами хостов или номерами портов определенных сервисов Internet.

Нападения на сети IPX бывают только в теории. Шлюзы IPX/IP (такие как IPX/IP Gateway компании Novell, IntranetWare Connect компании Quarterdeck и NOV*IX for Internet компании FTP Software) являются естественными брандмауэрами. Они всегда действуют от имени авторизованного клиента, запрашивая службы в IP-сетях, и таким образом, защищают его от нападений из внешней сети.

IntranetWare Border Services

Компания Novell

IntranetWare Border Services, обеспечивает кэш-посредников (proxy cache), службы виртуальной частной сети (Virtual Private Network — VPN) и службы безопасности. Кэш-посредники хранят часто запрашиваемые HTML-страницы в локальном кэше, обеспечивая значительно более быструю доставку информации, чем в тех случаях, когда не используется кэширование. Службы VPN позволяют создать канал контролируемой шифрованной связи с Internet, гарантируя конфиденциальность пакетов, передаваемых по этому каналу. Таким образом, компании получают возможность создавать защищенные частные сети, соединенные через Internet.

В VPN используется специальный метод шифрования, основанный на 40-битной реализации криптографического алгоритма RC2. Этот алгоритм обеспечивает приемлемую производительность работы на WAN-каналах и может выполняться в симметричных мультипроцессорных системах, что позволяет повысить скорость шифрования данных. Службы безопасности включают в себя фильтрацию пакетов, шлюз сеансового уровня, программу-посредника HTTP прикладного уровня и используют технологии трансляции адресов.

Используя IntranetWare Border Service, можно фильтровать и регистрировать следующую информацию, содержащуюся в пакетах:

- IP-адрес хоста-отправителя или получателя (для ограничения доступа к определенным хостам Internet и доступа с них во внутреннюю сеть компании);
- IPX-адрес отправителя или получателя (для ограничения доступа к определенным серверам и клиентам сети);
- номер IP-порта (для ограничения доступа к отдельным сервисам Internet, например FTP или HTTP);
- информацию протокола IPX (для ограничения к отдельным видам запросов к базовому протоколу NetWare — NetWare Core Protocol, NCP).

Шлюз сеансового уровня поддерживает IPX- и IP-клиентов, использующих соответствующие стеки протоколов. Вначале шлюз устанавливает контрольное соединение с клиентом, который пытается инициировать сеанс связи с удаленным хостом. Затем он запрашивает информацию в сетевом каталоге (NDS — Novell Directory Services), чтобы определить, имеет ли данный пользователь соответствующие полномочия.

Если пользователь оказывается авторизованным, шлюз устанавливает соединение с хостом, а затем копирует и перенаправляет поступающие пакеты. Поскольку шлюз использует информацию, хранящуюся в базе данных NDS, администратор может использовать NDS для ограничения прав доступа пользователей к Internet точно так же, как это делается для локальной сети. С помощью утилиты NetWare Administrator, можно задать права доступа конкретного пользователя или группы пользователей к отдельным сервисам Internet (например, FTP, HTTP или Telnet), хостам или доменам..

Посредник HTTP

Посредник HTTP является шлюзом прикладного уровня, который фильтрует HTTP-пакеты. Как и шлюз сеансового уровня, перед установлением соединения с удаленным хостом посредник HTTP использует информацию в NDS, чтобы проверить полномочия пользователя на запрашиваемый сеанс связи. После установления соединения посредник HTTP копирует, перенаправляет и фильтрует поступающие пакеты. При этом он заменяет адреса отправителей в исходящих пакетах своим собственным IP-адресом, "маскируя" адреса клиентов и серверов, отправивших эти пакеты.

Трансляция адресов

IntranetWare Border Services также обеспечивает трансляцию сетевых адресов для таких систем, как Macintosh и UNIX, которые не могут использовать стеки протоколов, необходимые для работы шлюзов сеансового и прикладного уровней. Кроме того, обеспечивается трансляция адресов как для IPX-, так и для IP-пакетов. Трансляция адресов IPX позволяет преобразовать все IPX-адреса отправителей в единый сетевой адрес IPX, что дает возможность использовать дублирующиеся адреса IPX-клиентов, относящиеся к разным виртуальным сетям.

Трансляция IP-адресов может быть как динамической, так и статической. При динамической трансляции все исходные IP-адреса преобразуются в единый IP-адрес, эффективно "маскируя" реальные IP-адреса клиентов и серверов внутренней сети, осуществляющих доступ к Internet (без использования шлюза сеансового уровня и посредника HTTP). При статической трансляции отдельные адреса преобразуются фиксированные IP-адреса, что позволяет обеспечить доступ из Internet к ресурсам интрасети, например, к Web — или FTP-серверам.

Брандмауэр ON Guard

Компания ON Technologies

Брандмауэр экспертного уровня — ON Guard компании ON Technology разработан специально для защиты сетей NetWare 3.11, 3.12 и 4.x. Он работает на стандартных ПК с процессором Intel 486 и выше. Поскольку ON Guard может фильтровать как IP-, так и IPX-пакеты, его можно использовать и для защиты сети NetWare от IP-трафика, поступающего из Internet или интрасети, а также для защиты отдельных серверов NetWare от внутреннего "неавторизованного" IPX-трафика. Одной из сильных сторон продукта ON Guard является использование 32-битной операционной системы Secure32OS, специально разработанной компанией ON Technology для этого брандмауэра. Данная ОС является значительно более защищенной, чем универсальные ОС, такие как UNIX и Windows NT.

ON Guard, как и другие брандмауэры прикладного и экспертного уровней, обеспечивает хорошую защиту внутренней сети от хакерских нападений типа spoofing, беспорядочного сканирования IP-адресов и блокировки служб (denial-of-service). Нападения последнего типа заключаются в переполнении сервера запросами злоумышленника, что делает его недоступным для других пользователей.

"ШИП"

Пензенский научно-исследовательский экспериментальный институт

ШИП представляет собой программно-аппаратный комплекс, с помощью которого можно шифровать все IP-пакеты, передаваемые между сегментами или отдельными компьютерами корпоративной сети в со-

ответствии со спецификацией IPSec. Система поставляется в виде компьютера с программным обеспечением, построенным на базе специализированной операционной системы. Оно позволяет шифровать потоки информации с максимальной скоростью до 15 Мбит/с, которой, как правило, достаточно для передачи информации между сегментами корпоративной сети. Кроме собственно ШИПов в системе должен быть как минимум один Центр управления ключевой системой (ЦУКС), который занимается распределением сеансовых ключей между различными ШИПами.

Пандора

В комплект МЭ "Пандора" входят следующие сервисные агенты (proxy): Telnet, rlogin (эмуляторы терминалов); FTP (передача данных); SMTP, POP3 (электронная почта); HTTP (WWW); Gopher, Whois (системы поиска); X11 (оконная система X Windows); LP (сетевая печать); Rsh (удаленное исполнение программ); Finger (информационный сервис); NNTP (телеконференции); RealAudio (передача звука по сети). Кроме того, в "Пандору" включены сервер общего назначения для TCP/IP, который контролирует передачу через МЭ TCP-пакетов. С помощью этого сервера можно расширить возможности системы, подключив любую программу, использующую TCP/IP в качестве транспортного протокола.

"Пандора" имеет ряд отличительных особенностей:

- использование пакета не требует изменения или замены клиентских программ;
- "прозрачный режим" сервисных агентов позволяет легко подключаться внутренним клиентам к внешним серверам;
- система контроля целостности дает возможность избежать изменения конфигурации брандмауэра, а запись всей важной информации в системный журнал позволяет выслеживать попытки нападения на сеть.

Система работает в любых TCP/IP-сетях, и может быть установлена на границе между корпоративной и открытой сетями или между двумя подсетями одного предприятия.

GIF

Компания Trusted Information Systems

Состав поддерживаемых посредников зависит от операционной системы. GIF работает под управлением UNIX (BSD — или BSD/OS — Solaris, и HP-UX) и NT. Посредник SQLNet для Oracle поддерживается в Solaris и HP-UX. В 1997 году TIS представила для Gauntlet графический пользовательский интерфейс на базе Java, намного упрощающий администрирование для менее опытных пользователей.

GIF имеет две его отличительные особенности:

- обрабатывая почту, он использует механизм посреднических услуг с промежуточным хранением, благодаря чему пользователи получают большую гибкость в обработке почты без ослабления модели защиты,
- функции системного администрирования, например проверка целостности и резервирование, встроены в продукт и легко вызываются.

CyberCop Server

Компания Network Associates

Система выполняется как на Windows NT 4.0, так и на Solaris. Данный продукт дополняет брандмауэр в деле защиты серверных ресурсов и обнаружения таких атак, как незаконная регистрация и несанкционированное изменение узла Web. Он автоматически регистрирует информацию об атаке и отправляет предупреждение системному администратору, а также прерывания SNMP на центральную станцию управления.

Kane Security Monitor

Компания Security Dynamics

Этот продукт позволяет защитить серверы Windows NT от таких нежелательных действий пользователя, как неудачные попытки регистрации и доступ к файлам, злоупотребление идентификаторами администратора и получение чрезмерных привилегий. Продукт состоит из трех частей: Console выполняется на клиентской машине администратора, Auditor Service — на сетевом сервере, а Agents устанавливаются с Console на машинах под NT, за которыми они должны следить.

Secured

Компания Memco Software

Семейство продуктов Secured для обнаружения атак на хосты от Memco Software оптимизировано для конкретных типов приложений на базе серверов. Эта группа продуктов состоит из Secured for Web, Secured for E-mail и Secured for Firewalls. Все продукты выполняются на HP-UX от Hewlett-Packard и Solaris. Продукт для Web поддерживает Web-серверы Netscape Communications и Apache и предотвращает крах серверов или изменение страниц Web в результате несанкционированных действий пользователей. Secured for

E-mail защищает серверы Sendmail посредством предотвращения случайных остановок. И, наконец, Secured for Firewalls защищает Firewall-1 компании Check Point Software от несанкционированного доступа.

Продукты Secured используют технологию защиты от переполнения буферов (Stack Overflow Protection, STOP) — любимого способа взлома серверов хакерами. Memco продвигает свою линию продуктов скорее как средство предупреждения атак, чем сообщения об атаках.

NetRanger

Компания Cisco Systems

Продукт для обнаружения атак на сеть, NetRanger появился в результате приобретения компании Wheel Group.

NetRanger состоит из двух компонентов: Sensor и Director.

Sensor может работать практически в любой сети TCP/IP и следить за трафиком в сегментах локальной сети, соединениях Internet и сетевой части пулов модемов, связывающих компанию с внешними партнерами. Этот компонент анализирует заголовки и содержимое всех пакетов, а также взаимосвязь пакетов с другими в потоке данных. Сенсоры могут быть настроены для той области, мониторинг за которой они призваны осуществлять.

Например, если какой-то пользователь часто подает по своей природе безвредные запросы ping, то Sensor может быть сконфигурирован на игнорирование таких сигналов с конкретного сетевого адреса. При обнаружении возможного вторжения Sensor посылает предупреждение на консоль Director, другой компонент NetRanger.

Director осуществляет надзор за несколькими сенсорами и подает предупреждения на пейджер, электронную почту и даже в приложения справочной службы. Кроме того, он помогает администратору определить, где именно произошла атака и насколько она серьезна. Информационная база данных содержит рекомендации о контрмерах и другие сведения об атаках.

RealSecure 3.0

Компания Internet Security Systems

Одна из наиболее известных компаний-разработчиков систем обнаружения атак, предлагает один из первых гибридов RealSecure 3.0. ***Он позволяет обнаружить аномалии как на уровне сети, так и на уровне операционной системы*** и немедленно отреагировать на атаку.

RealSecure состоит из двух основных компонентов: RealSecure Detectors и RealSecure Manager. Детекторы располагаются в стратегических местах предприятия и осуществляют мониторинг сетевого трафика в реальном времени; кроме того, они следят за журнальными и системными файлами ОС. Менеджер позволяет конфигурировать и управлять детекторами из нескольких точек, включая HP OpenView и собственную консоль управления ISS.

Internet Scanner

Компания Internet Security Systems

Многие из компаний-разработчиков систем обнаружения атак предлагают и продукты другого типа, где реализован несколько иной подход к мониторингу подозрительной сетевой активности. Обычно называемые инструментарием для оценки рисков, или сканерами, эти продукты в действительности служат для нахождения потенциально уязвимых мест в сетевой среде. Большинство таких продуктов имеет огромные базы данных по известным атакам, которые они и пытаются провести против сети для выяснения степени надежности ее защиты.

Установив программное обеспечение сканеров, администратор может указать подлежащие проверке IP-адреса, после чего сканер проверит операционные системы, маршрутизаторы, серверы и любые другие сетевые устройства, имеющие IP-адрес. Сканеры способны выявить самые разные бреши в защите, в том числе незащищенные паролем области, неправильно сконфигурированное программное обеспечение, переполнение буферов сервера и другие свидетельства потенциальных проблем. Кроме того, сканеры имеют развитые средства составления отчетов. Среди их ключевых возможностей — распределение потенциальных рисков по приоритетам, предложение исправлений и предоставление информации о контрмерах.

Internet Scanner осуществляет автоматическое сканирование сети и поиск дыр в защите с помощью базы данных об известных атаках. Он способен оценить слабость всей защиты компании, включая маршрутизаторы, брандмауэры, серверы Web и приложения.

Продукт позволяет выявить "потайные ходы", такие, как программа Back Orifice, получившие много внимания в последнее время, и удалить их прежде, чем злоумышленник сумеет ими воспользоваться. ISS гордится постоянным обновлением своего продукта,

благодаря чему он предоставляет самую последнюю информацию об уязвимых местах защиты.

Компания Check Point Software Technologies

Компания является одним из лидеров в области разработки программного обеспечения для защиты корпоративных сетей. Основная сфера деятельности компании — разработка продуктов для защиты интрасетей и обеспечения безопасного доступа в Internet.

Брандмауэры экспертного уровня являются очень популярным решением для защиты узлов Internet и интрасетей, поскольку они "прозрачны" для пользователей, работают на самом высоком уровне модели OSI и не требуют внесения изменений в клиентское ПО и установления отдельных посредников для каждой защищаемой брандмауэром службы. ***Один из самых популярных коммерческих брандмауэров FireWall-1 компании Check Point Software Techno-logies является именно брандмауэром экспертного уровня.***

FireWall-1 — брандмауэр, объединяющий в себе все средства, необходимые для защиты решений Internet/intranet, удаленного доступа и контроля за ним, аутентификации внешних пользователей, шифрования данных и преобразования сетевых адресов.

SecuRemote — модуль для Windows 95, который может быть использован мобильными и удаленным пользователями для надежной связи с центральным офисом через Internet. С помощью этого модуля можно строить виртуальные корпоративные сети и подключать к ним домашние или портативные компьютеры.

FireWall First — облегченный вариант FireWall-1, которым можно управлять через Web. Продукт предназначен для организаций, которые не могут себе позволить держать достаточно большой штат специалистов по безопасности.

Компания Raptor Systems

Raptor Systems разработала семейство брандмауэров Eagle, которое позволяет выделить в корпоративной сети пять областей с различной степенью защиты (Internet, интрасеть, мобильные пользователи, пользователи, работающие в филиалах компании, собственно корпоративная сеть предприятия) и управлять их взаимодействием с помощью брандмауэров. Такой комплексный подход обеспечивает более надежную защиту, чем обычные средства защиты от внешних нападений.

Eagle использует посредников для различных сервисов. Кроме того, Eagle не имеет функций администрирования системы, однако предусматривает функцию проверки файловой системы на предмет несанкционированного изменения старых (осуществляемого не через графический интерфейс) и появления новых файлов. По существу эта функция позволяет проверять целостность системы. Этот посредник весьма схож с GIF, однако он выполняется на Solaris и NT, причем NT является основной платформой. Операционная система укрепляется в процессе установки Eagle.

Eagle Enterprise и EagleNT — брандмауэры, предназначенные для защиты корпоративной сети от нападений из Internet, которые работают на прикладном уровне и сочетают в себе надежный контроль за действиями пользователей с возможностями управления в реальном времени и выявления подозрительных действий.

EagleLAN/EagleDesk — модули, работающие совместно с Eagle и предназначенные для защиты конфиденциальной информации в пределах корпоративной интрасети.

EagleMobile — модуль, который дает возможность пользователям персональных компьютеров подключаться к виртуальной корпоративной сети из Internet через шифрованный канал. Он использует те же методы шифрования, что и другие продукты семейства Eagle.

EagleRemote — модуль, предназначенный для управления системой защиты в филиалах и создания защищенных каналов обмена сообщениями с ними, независимо от способа их подключения к Internet.

EagleNetwatch — средство контроля состояния сети, которое позволяет объединять в одну систему четыре указанных выше продукта в любой комбинации и управлять получившейся сетью. Продукт упрощает работу со всем защитным комплексом, построенным на базе Eagle, и обеспечивает удобное управление им.

Компания Milkyway Network

Компания занимается разработкой, продажей и поддержкой программных продуктов, обеспечивающих ***защиту компьютерных сетей и каналов связи с Internet.*** Milkyway обеспечивает своим клиентам техническую поддержку и своевременную поставку новых версий продуктов.

Black Hole — шлюз прикладного уровня, располагающийся между защищаемой сетью и Internet. Он функционирует в качестве брандмауэра, обеспечивающего защиту от несанкционированного доступа к важной корпоративной информации.

Red Shift — средство, которое помогает системным администраторам выявлять и предупреждать нападение на самой ранней стадии.

Charon — модуль, позволяющий создавать шифрованный канал, через который к корпоративной сети могут подключаться удаленные или мобильные пользователи.

Secure Computing

Основная сфера деятельности компании Secure Computing — ***предоставление услуг по защите компьютерных сетей различного масштаба*** и разработка новых технологий безопасности. Компания собирается использовать свои технологии в такой бурно развивающейся области компьютерного бизнеса, как торговля через Internet.

Sidewinder использует посредников и укрепляет операционную систему в процессе установки. Однако она идет на шаг дальше: операционная система (модифицированная BSD/OS 2.1) задействует Domain Type Enforcement (DTE). Это позволяет разбить операционную систему на области (домены) для каждого интерфейса, а связь между областями осуществлять с помощью посредников.

Теоретически эта идея выглядит неуязвимой с точки зрения защиты. Однако хорошо написанный посредник не должен иметь брешей, поэтому пользователю никогда не следует обращаться к домену операционной системы за услугой. Обработка электронной почты осуществляется в соответствии с защитой на базе DTE. Пользовательский интерфейс вполне понятен, но он не столь интуитивен, как у GIF или Eagle.

Некоторые производители обеспечивают дополнительную защиту с помощью операционной системы. Secure Computing. При всей привлекательности этой функции пользователям следует тем не менее относиться к этой технологии с осторожностью, поскольку посредников никогда не стоит применять для обеспечения доступа к операционной системе. Некоторые даже предпочитают, чтобы брандмауэр разрывал все соединения и блокировал доступ в случае компрометации сервиса.

Sidewinder Security Server — высоконадежный брандмауэр, с помощью которого можно создать так называемый "периметр" безопасности. Sidewinder позволяет шифровать данные, надежно идентифицировать пользователей и выполнять фильтрацию пакетов TCP/IP.

BorderWare Firewall Server — продукт, одновременно выполняющий функции брандмауэра и шлюза к Internet. Его отличительными чертами являются управление через Web, поддержка виртуальных частных сетей, усиленная система аутентификации, легкие настройка и установка.

SafeWord — средство аутентификации пользователей. Продукт поддерживает большинство наиболее распространенных способов аутентификации, что позволяет клиентам использовать старые устройства аутентификации.

LOCKout FORTEZZA — более мощное средство аутентификации пользователей, построенное по алгоритму "запрос-ответ" и использующее стандарты шифрования DES и FORTEZZA.

Secure Network Server (SNS) — серверы, которые позволяют передавать по электронной почте важные сведения, гарантируя их секретность.

SmartFilter — средство контроля и фильтрации информации, поступающей из Internet, которое позволяет организациям контролировать доступ к ответственным Web-серверам

Комплекс средств защиты информации от несанкционированного доступа "Гриф"

ООО "Институт компьютерных технологий"
(044) 241-70-05
http://www.ict.com.ua

Комплекс "Гриф" предназначен для создания автоматизированных рабочих мест с защитой от угроз для информации, содержащей сведения, которые составляют государственную тайну, на базе автономных ПК с операционной системой Windows 95/98.

Совокупность реализованных в комплексе "Гриф" функций и механизмов защиты информации определяется функциональным профилем КА-2, КО-0, ЦА-1, ДВ-1, НР-3, НИ-3, НК-1, НО-2, НЦ-1, НТ-2, с уровнем доверия ГЗ (согласно НД ТЗИ 2.5-004-99).

Комплекс "Гриф" обеспечивает уровень защищенности информации достаточный для обработки информации, составляющей государственную тайну. Экспертное заключение зарегистрировано в ДСТСЗИ СБ Украины 18.07.2001 г. за № 10 и действительно до 18.07.2004 г.

Internet Scanner SAFEsuite

Поскольку именно сетевые сервисы во многих случаях служили объектом атак на распределенные информационные системы, возникла задача автоматизированной проверки сетевых систем на уязвимость со стороны известных атак.

Пакет программ Internet Scanner SAFEsuite предназначен для проведения комплексной оценки эффективности политики безопасности на уровне сетевых сервисов. Он предоставляет возможности для иденти-

фикации и коррекции более 140 известных слабых мест и постоянного наблюдения за состоянием безопасности для широкого диапазона сетевых устройств — от web-узлов и межсетевых экранов и до серверов и рабочих станций UNIX, Windows 95, Windows NT и всех других устройств работающих с TCP/IP.

Автоматизированное и конфигурируемое сканирование:

- автоматическая идентификация и создания отчетов по слабым местам
- плановые периодические сканирования или сканирования после определенных событий
- конфигурация сканирования по адресам IP, типам слабых мест, рискам и другим устанавливаемым пользователями критериям
- автоматическая коррекция ключевых слабых мест
- надежность и повторяемость.

Обеспечение безопасности:

- возможность управления рисками
- инвентаризация всех сетевых устройств и идентификация существующих базовых слабых мест
- распределение приоритетов по степеням риска (высокий, средний, низкий)
- анализ и сравнение базовых отчетов для использования в будущих оценках
- создание цепи обратной связи при реализации политики безопасности

Простота пользования:

- графические интерфейсы пользователя Windows NT и Motif UNIX
- создание отчетов HTML с упорядочением по типам слабых мест, классам рисков, именам host и адресам IP
- двухмерная сетевая карта, облегчающая поиск слабых мест
- централизация процедур сканирования, управления и мониторинга

Состоит из трех программ: Web Security Scanner, Firewall Scanner, Intranet Scanner.

Web Secure Scanner

Предназначен для поиска слабых мест безопасности на web-серверах. Обеспечивает аудит ОС, под управлением которой работает web-сервер, программ-приложений, установленных на web-сервере, и CSI scripts в web-приложениях. Проводит тестирование конфигурации web-сервера, оценивает уровень безопасности основной файловой системы и просматривает CSI scripts на наличие слабых мест. По итогам тестирования создается отчет с описанием обнаруженных слабых мест и с рекомендациями по корректирующим действиям.

Firewall Scanner

Обеспечивает поиск слабых мест в межсетевых экранах, прежде всего в их конфигурации, и предоставляет рекомендации по их коррекции. Проводит тестирование реакции межсетевых экранов на различные типы попыток нарушения безопасности. Выполняет сканирование сервисов — идентификацию всех сетевых сервисов, доступ к которым осуществляется через межсетевой экран. Firewall Scanner рекомендуется сделать частью установки межсетевого экрана и составной частью программы обеспечения безопасности.

Intranet Scanner

Предназначен для автоматического обнаружения потенциальных слабых мест внутри сетей с использованием различных тестов для проверки реакции на несанкционированные проникновения. Обеспечивает проверку различных сетевых устройств, включая UNIX hosts, системы, работающие под Microsoft NT/Windows 95, маршрутизаторы, web-серверы и X-терминалы.

RealSecure

Компания Internet Security Systems

Инструментальное средство ***RealSecure предназначено для административного управления большими объемами сетевой информации***. Продукт может быть использован как для простой регистрации происходящих событий, например, атак хакеров, так и для организации комплекса активных защитных мер, дополняющего функции межсетевого экрана. ***Отличительная особенность RealSecure*** состоит в том, что он создан специально для работы в сетях крупных организаций и способен одновременно отслеживать множество нарушающих безопасность событий непрерывно 24 часа в сутки и 7 дней в неделю.

RealSecure состоит из двух программных средств: ***механизма фильтрации***, осуществляющего наблюдение и активное управление сетевыми событиями, и ***графического пользовательского интерфейса***, при помощи которого пользователь получает информацию о текущих событиях, может управлять ими в реальном масштабе времени, а также устанавливать и изменять рабочую конфигурацию пакета. Это позволяет проводить фильтрацию событий с автоматическим выполнением по отношению к ним ряда действий (регистрация, отображение на дисплее, уничтожение или отсутствие дей-

ствий), характер которых определяется по устанавливаемым пользователем характерным признакам события. В пакете имеется программа записи и последующего воспроизведения информации о текущих событиях как в реальном, так и в ускоренном, и замедленном режимах просмотра, что полезно для последующего анализа происшедших событиях.

Пакет может работать под ОС SunOS, Solaris и Linux; не требует чрезмерных системных ресурсов. Для наиболее эффективной работы и максимальной реализации заложенных в него возможностей рекомендуется использовать пакет программ RealSecure на отдельном компьютере с хорошим графическим дисплеем, специально выделенном для целей административного сетевого управления.

AutoSecure

Platinum Technology (Окбрук, шт. Иллинойс)

Программное обеспечение AutoSecure (первоначально известное под именем SeOS компании Memco Software) ***представляет собой набор средств защиты вычислительных систем с серверами*** под ОС Unix, HP-UX, AIX и SunOS/Solaris и клиентскими станциями с интерфейсом Motif.

В состав программы входят три независимых модуля:

- ***AutoSecure Access Control*** — контролирует доступ пользователей к защищаемым программам и файлам, а в случае попыток несанкционированного доступа извещает о них администратора системы;
- ***AutoSecure Security Administrator*** — служит для ведения списков пользователей, групп пользователей, защищаемых ресурсов, настройки прав доступа пользователей к ресурсам;
- ***AutoSecure Single Sign On*** — открывает пользователям доступ к данным, хранящимся на мэйнфреймах. В этом случае администратор и пользователи получают такой же уровень безопасности и комфортности, как и на больших машинах, где используются системы RACF корпорации IBM или ACF2 от Computer Associates.

Ниже приведены основные особенности продукта фирмы Platinum:

- защита корпоративных данных от несанкционированного доступа за счет идентификации пользователей и проверки их полномочий;
- предотвращение случаев нарушения системы защиты и уведомление системного администратора при обнаружении попыток "взлома" и подозрительного поведения пользователей (вроде попыток подбора пароля, запуска приложений из закрытых каталогов и пр.);
- фиксация пользовательской активности в системных журналах;
- возможность администрирования системы защиты с локальных или удаленных компьютеров;
- масштабируемость системы в зависимости от размера компьютерной сети;
- минимизация сетевого трафика без снижения общей производительности за счет обработки авторизованного запроса на том компьютере, откуда он поступил;
- возможность адаптации к промышленным стандартам за счет поддержки технологии защиты, принятой в распределенной вычислительной среде DCE;
- возможность ограничения прав суперпользователя (пользователь Unix с максимальными правами доступа).

DBA-Xpert for Oracle

Compuware (Фармингтон-Хиллс, шт. Миннесота)

Средство централизованного администрирования и обеспечения защиты информации в распределенных системах.

Продукт поддерживает работу с произвольным числом баз данных. Имеются средства анализа и навигации для БД Oracle.

Состоит из трех компонентов:

Secure-Xpert (централизованное управление системой безопасности для распределенных данных), ***Change-Xpert*** (функции синхронизации) и ***Reorg-Xpert*** (операции по загрузке/выгрузке данных).

Guardian DataLynx

(Сан-Диего, шт. Калифорния)

Guardian за короткий срок стал стандартом де-факто для ***систем учета и контроля доступа в среде Unix.*** Программа поддерживает около 20 версий этой ОС и имеет общий для всех платформ графический интерфейс Motif. С помощью ПО Guardian администратор системы может назначить временные рамки, в пределах которых пользователи могут регистрироваться в системе. Как только время работы истекает, Guardian вынуждает пользователя закончить работу.

Большое внимание система уделяет дисциплине ведения паролей. Так, программа регулярно напоминает пользователям о необходимости смены паролей, заставляет всех или некоторых пользователей изменять пароли при очередной регистрации, ведет учет ранее

вводимых паролей, автоматически генерирует миллионы паролей с форматным контролем (FIPS-181). Когда пользователь превышает число допустимых попыток ввода паролей, Guardian блокирует его вход в систему. Предусмотрено постоянное ведение журналов, в которых фиксируется история работы пользователей.

Программа функционирует на компьютерах HP, IBM и Sun Microsystems.

OmniGuard

Axent Technologies (подразделение компании Raxco, Роквилл, шт. Мериленд)

Комплект продуктов, предназначен для решения проблем безопасности в системах клиент/сервер. Пакет состоит из шести компонентов, позволяющих администрировать базы данных в распределенных сетях масштаба предприятия.

Функции продукта охватывают все аспекты проблемы безопасности в архитектурах клиент/сервер, включая управление защитой данных, идентификацию и администрирование пользователей, мониторинг трафика, контроль за вторжением в систему извне, обеспечение безопасного обмена сообщениями и файлами.

OmniGuard реализован в архитектуре клиент/сервер, поддерживает несколько платформ и конструктивно состоит из трех частей: презентационной части, управляющего сервера и интеллектуального агента. По желанию интерфейс пользователя может быть настроен под X/Motif или Windows. Управляющий сервер работает на платформах NetWare, OpenVMS и различных вариантах Unix.

RACF

На протяжении всего срока существования больших машин корпорация IBM уделяла огромное внимание защите информации в своих системах, и ее основным продуктом в этой области стала система Resource Access Control Facility (RACF), которая шлифовалась в течение 25 лет. ***Указанное ПО предназначено для обслуживания семейства компьютеров IBM, работающих под управлением ОС MVS.***

Приведем некоторые функции этого продукта:

- ***Идентификация, аутентификация и авторизация пользователей***. Каждому пользователю компьютерной системы присваиваются уникальный идентификатор (ID) и пароль, по которым RACF определяет, входит ли данный пользователь в список пользователей системы и может ли он работать в ней. При этом администратор системы может управлять уровнями и средствами доступа к объектам, которые включают в себя команды, наборы данных, дисковые устройства, терминалы, накопители на магнитных лентах, т. е. "авторизировать" пользователей. В процессе работы пользователя специальные программы — менеджеры ресурсов — фиксируют все обращения пользователей к информационным ресурсам;
- ***Групповые пароли***. Часто группа пользователей, например из одного подразделения, постоянно работает с общими данными. В этом случае можно не назначать индивидуальные идентификаторы и пароли каждому пользователю группы, а "выписать" групповой пропуск (Passticket);
- ***Администрирование***. Администратор системы может контролировать и анализировать работу RACF как из центрального пункта, так и с любого терминала. Предусмотрены два режима: командный (на языке TSO) и интерактивный (посредством утилиты ISPF). Одна команда оператора может автоматически направляться всем базам данных. Например, выполнение команды Update для таблиц распределенных БД может быть синхронизировано;
- ***Аудит***. RACF поддерживает гибкие и мощные средства ведения журналов, позволяющие впоследствии легко аудировать работу пользователей в системе (длительность работы, доступ к информационным ресурсам и т. д.). Системные журналы можно просматривать динамически (утилита SMF), выгружать в виде файлов или распечатывать с помощью специального генератора отчетов;
- ***Синхронизация паролей.*** С помощью RACF пользователи могут синхронно менять свои пароли, например, на различных серверах баз данных. Кроме того, можно синхронизировать смену паролей нескольких пользователей на одной и той же системе.

Secure Network Services

Oracle (Редвуд-Шорс, шт. Калифорния)

Набор сервисных средств, предназначенный для работы с продуктом SQL*Net корпорации Oracle и поддерживающий стандарт шифрования информации R4 компании RSA Data Security. В зависимости от типа аппаратной платформы (DEC, Hewlett-Packard, Silicon Graphics и др.)

SQL Secure 31

BrainTree Technology (Норвелл, шт. Массачусетс)

Приложение класса клиент/сервер ***для администрирования средств защиты информации в базах данных Oracle.*** Программа фиксирует попытки внедрения в систему извне, синхронизирует пароли пользовате-

лей в нескольких БД, позволяет гибко настроить процесс внутреннего аудита, регламентирует доступ пользователей к таблицам базы данных на уровне строк.

Благодаря компоненту Password Manager пользователь может работать с несколькими базами данных на разных аппаратных платформах, используя единый пароль. Кроме того, возможна настройка механизма управления паролями пользователей в соответствии с принятыми в конкретной организации стандартами: предусмотрено задание минимальной длины пароля и срока его действия, допустимого числа попыток подбора пароля при регистрации в базе данных.

Администратор может запрограммировать ряд действий, выполняемых в случае обнаружения в системе несанкционированного пользователя или попыток ее "взлома", к которым относятся запрет дальнейшей работы с БД и активизация аварийной процедуры.

Программный модуль Audit Manager предназначен для просмотра аудиторских журналов. При этом возможно наложение фильтра просмотра и определение порядка сортировки записей в журналах. Дополнительно можно описать критические события и действия, которые должны выполняться в случае их возникновения.

Lucent

Компания Lucent представляет:

Мультисервисный маршрутизатор доступа Access Point 300 (ISDN, 2xT1/E1, MSSI) с производительностью IP-форвардинга 50 Мбит/с и поддержкой 500 туннелей IPSec.

Устройства доступа для удаленных пользователей и малых/домашних офисов:

- SuperPipe 170 (ADSL, 150 туннелей IPSec)
- SuperPipe 175 (голосовой шлюз H.323 v.2, ADSL, T1, E1, V.35/X.21, 4 порта).

Межсетевые экраны:

- VPN Firewall Brick 20 для малых/домашних офисов (3 порта 10/100 Ethernet, производительность 2 Мбит/с с шифрованием 3-DES, до 50 туннелей ВЧС IPSec).
- VPN Firewall Brick 1000 для крупных центров данных, поддерживает до 4 портов gigabit Ethernet и 9 портов 10/100 fast Ethernet.

На рынке брандмауэров Lucent представляет:

Lucent Managed Firewall — динамический контекстный фильтр пакетов в программно-аппаратном исполнении. Аппаратным компонентом является Lucent Managed Firewall Brick, устройство в черном корпусе на базе процессора Pentium II.

Brick выполняет программное обеспечение брандмауэра на базе защищенной операционной системы Inferno от Bell Labs.

Brick оснащен четырьмя портами Ethernet на 10/100 Мбит/с и может устанавливаться в сети между любыми устройствами Ethernet, такими, как маршрутизаторы, коммутаторы, концентраторы и серверы.

Интерфейсы Ethernet на Brick не имеют IP-адресов, вследствие чего устройство оказывается невидимым для всех остальных сетевых устройств, за исключением второго компонента продукта — управляющего сервера.

Security Management Server выполняется на Windows NT или Sun Solaris и предназначен для управления Brick и выполнения функций администрирования политики защиты и протоколирования/аудита. В состав комплекса входят: межсетевой экран Lucent VPN Firewall Brick, клиент Lucent IPSec, сервер управления безопасностью Lucent Security Management Server, а также мультисервисные маршрутизаторы доступа Access PointT, Pipeline и SuperPipe.

Для обеспечения стыковки всех продуктов имеются встроенные прикладные программные интерфейсы API.

Компьютер в защищенном исполнении

Компания "Укрспецсистема"
Украина, Киев, 03037, ул.Кривоноса 2а
Тел.: +380 (44) 495-1032

Работа средств вычислительной техники сопровождается электромагнитными излучениями и наводками на соединительные проводные линии, которая может быть восстановлена на довольно отдаленном расстоянии, не обязательно находиться около цели, это можно сделать из офиса или транспортного средства, как показывают исследования с расстояния до одного километра. Причем для этого не требуется каких-либо сверх сложных систем наблюдения, слежения и перехвата информации, может быть использован обыкновенный телевизионный приемник со специальной аппаратурой. Подобные устройства были изобретены достаточно давно – более 2 десятилетий назад

Подход к защите закрытой информации до недавнего времени был таков – создавались специальные комнаты, где находились ЭВМ, обивались (экранировались) сплавом, создавались генераторы шумов; для защиты от наводок по цепям питания и кабелям применяются специальные фильтры. Использовать данный подход могли позволить себе только крупные государственные учреждения.

В настоящее время этот подход не является единственным. Во-первых, очевидны минусы – очень большие материальные затраты на оборудование специаль-

ного помещения, неудобство нахождения в подобном помещении и т.д., во-вторых, создан обыкновенный защищенный компьютер, который является несомненно более дешевым и эффективным способом защиты информации от утечки по каналу побочных электромагнитных наводок.

Предлагается следующее решение по защите ПК от утечки информации за счет ПЭМИН.

Назначение:

- Работа с документами, содержащими закрытую информацию, в том числе государственную тайну с грифом "С", "СС", "ОВ"
- Работа в автоматизированных комплексах ближней радиоразведки и мониторинга

Закрываются каналы утечки информации:

- За счет побочных электромагнитных излучений
- По первичной сети электропитания
- За счет вторичного излучения при электромагнитном навязывании
- Через наводки на кабели питания, связи, сигнализации и пр.
- Через технические средства, внедренные в составные части компьютера ("радиозакладки")

Преимущества защищенных компьютеров:

- Большие технические запасы по уровню побочного электромагнитного излучения обеспечивают стабильность качества защиты на протяжении всего срока эксплуатации
- Модернизация или ремонт компьютеров не влияет на качество его защиты
- Современный дизайн
- Произвольная комплектация по выбору заказчика

Технология защиты включает в себя:

- Полную радиогерметизацию системного блока и максимально возможную – монитора, в том числе установку дополнительных экранов и защитных стекол
- Установку фильтра по цепям электропитания и всем сигнальным кабелям
- Многократное экранирование экрана
- Применение элементов и материалов, поглощающих электромагнитное излучение

Комплект поставки защищенных компьютеров по I и II категории:

- Защищенный системный блок со следующей стандартной комплектацией: Pentium III-600, 20 GB HDD, 128 MB, CD- 48.
- Защищенный монитор 17’
- Мышь
- Защищенный принтер HP 1100
- Сетевой фильтр

Компания "Укрспецсистема" оказывает полный комплекс услуг, связанный с установкой и сопровождением защищенного спецоборудования:

- проверка коммуникаций
- проверка наличия, назначения и расположения технических средств, находящихся на объекте;
- проверка способа электропитания защищенного оборудования;
- составление Акта категорирования;
- составление Расчета контролируемой зоны;
- составление и утверждение Акта обследования объекта;
- проведение инструментального исследования защищенного оборудования с предоставлением Протокола испытаний

Прибор для защиты телефонных линий "Скеля-1"

Фирма "БУМЕКС"
(044) 241-09-80, 241-09-81
E-mail: bumeks@webber.net.ua
Http:\\ www.security.kiev.ua

Прибор "Скеля-1" предназначен для защиты оконечного абонента устройства от несанкционированного снятия информации. Прибор "Скеля-1" гальванически развязан от телефонной линии и не потребляет от линии АТС электрический ток. На передней панели прибора "Скеля-1" расположена световая индикация с надписями: “Живлення”, “Чекання”, ”Підключення”, “Обрив”, “Стороннє”.

Прибор "Скеля-1" обеспечивает:

- полную гальваническую развязку оконечного абонента устройства от телефонной линии в режиме ожидания (телефонная трубка на устройстве положена);
- световую индикацию и срабатывание реле при подключении к контролируемой линии АТС любого устройства, сопротивление которого не превышает50 Ком;
- световую индикацию и срабатывание реле при подключении к контролируемой линии АТС любого устройства, емкость которого составляет не менее 0,1Мг;
- световую индикацию и срабатывание реле при появлении в линии постороннего напряжения переменной величины, напряжением не менее 0,1В;

• световую индикацию и срабатывание реле при обрыве телефонной линии (одного или двух проводов сразу).

После подключения линии АТС прибор переключается в режим “Чекання” (трубка должна быть положена и сигналы вызова АТС должны отсутствовать). В этом режиме должны светиться светодиоды с надписями “Живлення” и “Чекання”. При необходимости нужно отрегулировать чувствительность прибора потенциометром. Регулировки необходимо произвести таким образом, чтобы потенциометр находился в среднем положении при максимальной чувствительности в левом положении (возможно свечение светодиода “Стороннє”) и минимальной чувствительности в правом положении (возможно свечение светодиода “Обрив”).

Индикация работы прибора происходит согласно таблицы 26.1. В состоянии ожидания горят светодиоды “Живлення” и “Чекання”, при этом светодиоды “Підключення”, “Обрив”, “Стороннє” должны находиться в погашенном состоянии.

В режиме вызова (вызов со стороны АТС или поднята трубка) загорается светодиод “Підключення”, “Стороннє”, а светодиод “Чекання” гаснет.

При переходе из режима вызова в режим ожидания светодиоды “Підключення” и “Стороннє” гаснут в течении ни более 10 сек, а светодиод “Чекання” загорается в течении ни более 10 сек.

При обрыве телефонной линии на время ни менее 2 сек загорается светодиод “Обрив”.

При подключении в линию АТС прибора RJ50КОм или Ci0,1, а также появление постороннего напряжения не менее 0,1В~ загорается светодиод “Стороннє”.

В режиме “Чекання” абонентское устройство отключено от линии АТС, а в режиме “Підключення” (снятая трубка или вызов со стороны АТС) оконечное абонентское устройство подключается к линии АТС при помощи контактов реле.

В режиме “Обрив” кроме индикации срабатывает реле, с контактов которого, при необходимости, можно снять тревожное сообщение.

В режиме “Стороннє” кроме индикации срабатывает реле, с контактов которого при необходимости можно снять тревожное сообщение.

В режиме “Підключення” (трубка снята) при обрыве телефонной линии, индикация обрыва линии и срабатывание реле не происходит.

Для обнаружения обрыва линии АТС необходимо перейти в режим “Чекання” трубка положена.

Фирма Informaiton & Communication Protection (ICP) Ltd.

Фирма ICP является системным интегратором в области защиты информации в компьютерных сетях. Предлагаются комплексные решения на основе объединения в единую, взаимосвязанную систему программно-аппаратных средств защиты информации.

Сотрудники ICP прошли обучение у специалистов фирм — признанных мировых лидеров в области защиты информации CYLINK (США), Algoritmic Reseach (Израиль), Internet Security Systems (США), WatchGuard Technologies Inc. (США), Check Point (США), Websense Inc. (США), что подтверждено соответствующими сертификатами.

Фирма ICP предлагает эффективные программно-аппаратные средства защиты информации.

Таблица 26.1. Состояния индикации

	Линия АТС отключена, трубка положена	*Линия АТС подключена, трубка положена*	*Поступают сигналы вызова АТС, трубка положена*	*Линия АТС подключена, трубка снята*	*Постороннее подключение R ≤ 50КОм; C ≥ 0,14; V~≥ 0,1В, трубка положена*	*Примечания*
Живлення	+	+	+	+	+	
Чекання	+	+	-	-	+	
Підключення	-	-	+	+	-	
Обрив	+	-	-	-	-	
Стороннє	-	-	+	+	+	

Примечание.

"+" светодиод светится, "-" светодиод погашен.

СИСТЕМА АНАЛИЗА ЗАЩИЩЕННОСТИ Internet Scanner

Анализ защищенности сетевых сервисов и протоколов на базе TCP/IP. Анализ защищенности серверов, рабочих станций, маршрутизаторов, Web — серверов, межсетевых экранов и т.п.

- более 900 проверок;
- задание степени глубины сканирования;
- параллельное сканирование до 128 узлов сети;
- запуск по расписанию;
- работа из командной строки;
- различные уровни детализации отчетов;
- создание собственных проверок;
- защита компонентов и собранных данных.

СИСТЕМА АНАЛИЗА ЗАЩИЩЕННОСТИ System Scanner

Анализ конфигурации и настроек операционных систем хостов, таких как: Solaris, SunOS, HP-UX, Linux, Windows.

- более 600 проверок;
- проверки конфигурации операционной системы;
- централизованное управление;
- запуск по расписанию;
- работа из командной строки;
- различные уровни детализации отчетов;
- создание собственных проверок;
- защита компонентов и собранных данных.

СИСТЕМА АНАЛИЗА ЗАЩИЩЕННОСТИ Database Scanner

Анализ настроек и конфигурации баз данных (MS SQL Server, Oracle, Sybase), в т.ч. подсистем аутентификации, контроля целостности, аудита и т.д.

- более 400 проверок;
- прямой доступ к функциям СУБД;
- обнаружение нарушений политики безопасности;
- анализ настроек СУБД.

СИСТЕМА ОБНАРУЖЕНИЯ АТАК RealSecure

Обнаружение атак в реальном режиме времени на уровне сети и уровне операционной системы. Реагирование на атаки в реальном режиме времени. Поддержка протокола NetBIOS и стека протокола TCP/IP (IP, TCP, UDP, ICMP и других на их основе)

- более 900 контролируемых событий;
- задание шаблонов для контроля трафика;
- централизованное управление;
- различные варианты реагирования на атаки;
- распределенная архитектура.

СИСТЕМА ПОДДЕРЖКИ ПРИНЯТИЙ РЕШЕНИЙ SAFEsuite Decisions

Мощный программный продукт для поддержки принятия решения по безопасности корпоративной сети. Осуществляет сбор, обработку и анализ данных от всех средств защиты:

Internet Scanner

System Scanner

Database Scanner

RealSecure

FireWall

Система контроля и управления доступом пользователей корпоративных сетей к ресурсам Internet Websense Enterprise

Обеспечивает увеличение производительности труда служащих, разгрузку сетевого трафика и позволяет экономить Ваши деньги.

- удобство и простота инсталляции;
- гибкая система настроек (блокирование, слежение, в том числе по заданному расписанию и пользователям);
- удобный графический интерфейс;
- блокирование более 2 200 000 Web сайтов, зарегистрированных в Master Database;
- возможность самостоятельного пополнения Master Database;
- возможность ежедневного автоматического обновления Master Database;
- категорирование блокируемых Web сайтов на 64 категории;
- большое количество поддерживаемых платформ;
- гибкая система генерации отчетов;
- Web — based администрирование;
- сертификат ICSA (International Computer Security Association).

Межсетевой экран Firewall-1, програмный пакет FloodGate-1 для управления трафиком, система Meta-IP управления IP-пространством

Обеспечивает полное масштабируемое решение для реализации корпоративной безопасности, управления трафиком и IP-адресами в корпоративных интрасетях и Интернет.

СЕМЕЙСТВО МЕЖСЕТЕВЫХ ЭКРАНОВ КОМПАНИИ WatchGuard: Firebox 4500, Firebox 2500, Firebox 1000, Firebox 700, Firebox SOHO и Firebox Telecommuter

Обеспечивает надежную защиту как для штаб-квартиры корпорации, средних и небольших ее филиалов, так и для малых офисов и мобильных пользователей. Центр управления **WatchGuard Control Center** проводит мониторинг всех сетевых соединений, пользователей, сервисов и используемой полосы пропускания, а также документирование событий с возможностью последующего их анализа.

Програмный продукт PrivateWire для защиты коммуникаций между организациями и удаленными пользователями

Уникальная комбинация стойкого шифрования, двусторонней аутентификации, управления доступом, обеспечения целостности данных и передовой firewall-защиты дает возможность организациям прозрачно устанавливать защищенные коммуникации с удаленными пользователями и филиалами через любые TCP/IP-сети, в том числе и через Internet.

Акционерное общество "Институт информационных технологий"

Акционерное общество "Институт информационных технологий" (АО ИИТ) является одним из ведущих предприятий на территории Украины по производству высококачественных систем и средств криптографической защиты информации.

Приоритетная сфера деятельности АО ИИТ – научные исследования в области защиты информации; разработка систем защиты информации для локальных вычислительных сетей, корпоративных информационных систем; создание проектов и инсталляция крупных вычислительных сетей, основанных на передовых достижениях в сетевых технологиях.

Получена ***лицензия*** на проведение предпринимательской деятельности, связанной с разработкой, изготовлением, ввозом, вывозом, реализацией и использованием средств криптографической защиты информации, а также предоставлением услуг по криптографической защите информации. В рамках АО ИИТ создана и получила аккредитацию ***лаборатория по сертификации средств криптографической защиты информации.***

СЗИ в системе "Клиент-Банк"

АО ИИТ разработана СЗИ в системе "Клиент-Банк". В этой системе защиты реализован комплекс программно-технических и организационных решений, направленных на предотвращение возможных атак потенциальных нарушителей.

Система обеспечивает:

- ***подлинность и целостность информации и сообщений***, циркулирующих в системе “Клиент-Банк”, при наличии случайных искажений и целенаправленных изменений, на основе применения стандартных процедур цифровой подписи ГОСТ 34.310-95;
- ***конфиденциальность информации и сообщений*** на основе применения стандартных алгоритма симметричного шифрования ГОСТ 28147-89 для шифрования основного объема информации и направленного шифрования служебной части Диффи-Хэллмана или RSA-алгоритму;
- ***надежную идентификацию*** объектов и субъектов системы “Клиент-Банк”, защиту от НСД со стороны как санкционированных, так и несанкционированных пользователей а также защиту от несанкционированного распространения;
- ***арбитраж и юридическую ответственность пользователей*** системы за сформированные, переданные и принятые сообщения и защиты их от обмана на основе цифровой подписи информации, симметричного шифрования основного объема информации, включая цифровую подпись, а также направленного шифрования служебной части;
- ***управление ключевыми структурами*** на всех этапах жизненного цикла системы, включая плановую и аварийную смену ключей, с генерацией конфиденциальных ключей по принципу “сам себе” и передачей открытых ключей по каналам связи.

В состав системы защиты информации входят:

1. Центр генерации, сертификации и управления ключевыми структурами
2. Генератор ключей клиента
3. Рабочие станции банка и клиента, которые обеспечивают прямое и обратное криптографические преобразования передаваемых и принимаемых сообщений

Многоуровневая система защиты информации (МСЗИ) для решения задач защиты в компьютерных системах

Сотрудниками АО ИИТ разработана многоуровневая система защиты информации (МСЗИ) для решения задач защиты в компьютерных системах. МСЗИ предназначена для непрерывной и комплексной защиты информации на прикладном и (или) сетевом уровнях.

Система защиты информации на прикладном уровне обеспечивает:

- ***подлинность и целостность*** информации и сообщений, циркулирующих в системе, при наличии случайных искажений и целенаправленных изменений, на основе применения стандартных процедур цифровой подписи ГОСТ 34.310-95 или DSS с использованием модульного возведения в степень и эллиптических кривых;
- ***конфиденциальность*** информации и сообщений на основе применения стандартных алгоритмов симметричного шифрования ГОСТ 28147-89 (AES) для шифрования основного объема информации и направленного шифрования служебной части по алгоритму Диффи-Хэллмана или RSA;
- ***надежную идентификацию*** объектов и субъектов системы, а также защиты от НСД со стороны как санкционированных, так и несанкционированных пользователей;
- ***юридическую ответственность*** пользователей системы за сформированные, переданные и принятые сообщения и защиты их от обмана на основе цифровой подписи информации, симметричного шифрования основного объема информации, включая цифровую подпись, а также направленного шифрования служебной части;
- ***возможность арбитража*** за счет использования личных ключей и ключей арбитра при криптографических преобразованиях;
- ***управление ключевыми структурами*** на всех этапах жизненного цикла системы, включая плановую и аварийную смену ключей, сертификацию ключей, с генерацией конфиденциальных ключей по принципу “сам себе” и передачей открытых ключей по каналам связи.

Система защиты на сетевом уровне обеспечивает:

- высокоскоростное шифрование и цифровую подпись;
- шифрование пакетов на сеансовых ключах;
- реализацию функции причастности;
- прозрачность системы защиты информации;
- контроль доступа.

МСЗИ может быть реализована как программно, так и программно-аппаратно с использованием устройств "Гряда-1", "Гряда-1М", "Гряда-11" и "Града-31", выполняющих функции криптографических преобразований, генерации и хранения ключей в защищенном виде.

Специалисты АО ИИТ

Горбенко Иван Дмитриевич. Д.т.н., профессор, главный конструктор АО ИИТ. Заведующий кафедрой “Безопасности информационных технологий” Харьковского национального университета радиоэлектроники.

Качко Елена Григорьевна к.т.н., доцент, ведущий специалист.

Потий Александр Владимирович – к.т.н. ведущий специалист.