Осуществление выбора средств защиты

В этой главе

- *Модель ИС как объекта защиты*
- *Услуги и механизмы обеспечения безопасности сетей на основе модели ВОС*
- *Базовые сервисы для обеспечения безопасности компьютерных систем*
- *Механизмы обеспечения безопасности*
- *Использование услуг безопасности*
- *Обзор средств защиты информации в ИС*
- *Средства защиты от НСД*
- *Анализаторы протоколов*
- *Инструментальные средства тестирования системы защиты*
- *Межсетевыеэкраны*

<<< 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

Многообразие способов построения ИС, неопределенность стандартов и законодательной базы в области информационной безопасности, а также широкий выбор методов и средств защиты информации порождают обилие вариантов создания СЗИ.

Рынок средств защиты информации столь разнообразен по стоимости, назначению и качеству продуктов, что выбор наиболее оптимальных из них для конкретного объекта представляется непростой задачей. На чем остановить выбор способов и средств защиты ? Какие из принятых решений окажутся правильными?

В такой ситуации администраторы сталкиваются с проблемой выбора на основе учета принципов деятельности организации значимости целей и наличия ресурсов. Эти решения предусматривают способы защиты технических и информационных ресурсов, а также поведение служащих в тех или иных ситуациях.

Исходя из экономической целесообразности в выборе защитных мер, ***расходы на средства защиты не должны превышать предполагаемый ущерб от нарушения информационной безопасности.***

Кроме того, в центре внимания при выборе средства защиты должна быть простота использования и прозрачность. Необходимо критически оценивать заверения поставщиков в том, что предлагаемый ими продукт эффективен и прост в применении.

Следует помнить, что отобранные средства должны ***обеспечить защиту по следующим НАПРАВЛЕНИЯМ:***

- 010 Защита объектов информационных систем;
- 020 Защита процессов, процедур и программ обработки информации;
- 030 Защита каналов связи;
- 040 Подавление побочных электромагнитных излучений;
- 050 Управление системой защиты.

Состав назначение и способы применения выбранных средств защиты должны найти свое отражение в ОСНОВАХ, к которым относятся:

- 001 Законодательная, нормативно-правовая и научная база;
- 002 Структура и задачи органов (подразделений), обеспечивающих безопасность ИТ;
- 003 Организационно-технические и режимные меры и методы (политика информационной безопасности).

Модель ИС как объекта защиты (500)

Для понимания того, какие средства, механизмы и функции защиты необходимы для конкретной ИС, предлагается рассмотреть уровневую модель взаимодействия вычислительных систем и процессов.

Базовая модель взаимодействия открытых систем (BOC) содержит семь уровней:

- Физический (Physical Layer) — битовые протоколы передачи информации.
- Канальный, или уровень данных (Data Link Layer) — формирование пакетов и фреймов данных, управление доступом к среде.
- Сетевой (Network Layer) — маршрутизация и управление потоками данных.
- Транспортный (TransportLayer) — обеспечение взаимодействия удаленных процессов.
- Сеансовый (Session Layer) — поддержка диалога между удаленными процессами.
- Уровень Представления данных (Presentation Layer) — преобразование форматов данных.
- Прикладной (Application Layer) — прикладные задачи, пользовательское управление данными.

Уровневая модель OSI...

1 Физический уровень (540)

Обеспечивает интерфейс между компьютером (или станцией), участвующим во взаимодействии, и средой передачи (дискретных) сигналов. Управляет потоком данных. Определяются электрические, механические, функциональные и процедурные параметры для физической связи в системах. Для этого уровня определяются различные типы физических интерфейсов (коммуникационные — V.24 CCITT, RS-232, X.21, ISDN; локальных сетей — Ethernet/IEEE802.3, IEEE802.5, FDDI) для различных типов физических сред (коаксиальный кабель, витая пара, оптоволокно, радиоканал).

2 Канальный уровень (уровень данных) (530)

Формирует из данных, передаваемых физическим уровнем, так называемые пакеты — "кадры" или последовательности кадров. Осуществляется управление доступом к передающей среде, используемой несколькими компьютерами, синхронизация, обнаружение и исправление ошибок.

На уровне данных выделяются два подуровня: подуровень управления доступом к среде (УДС, MAC — Media Access Control), и подуровень управления логическим звеном (УЛЗ, LLC — Logical Link Control).

Особенностью УЛЗ является определение протоколов передачи данных на этом уровне с установлением и без установления связи. Одним из известных стандартов этого уровня является стандарт ISO — высокоуровневый протокол управления каналом HDLC (High Level Data Link Control).

3 Сетевой уровень (520)

Устанавливает связь в вычислительной сети между двумя абонентами. Соединение происходит благодаря функции маршрутизации, которая требует наличия сетевого адреса. Кроме того, этот уровень должен обеспечивать обработку ошибок, мультиплексирование и управление потоками данных. Наиболее известен стандарт X.25 для сетей общего пользования с коммутацией пакетов. Для локальных вычислительных сетей (ЛВС) на Сетевом уровне определяются межсетевые протоколы, как правило, различные для различных сетевых ОС.

4 Транспортный уровень (530)

Обеспечивает надежную передачу данных между двумя взаимодействующими пользовательскими процессами, а также — сквозное управление движением пакетов между этими процессами. Транспортный уровень поддерживает сегментацию и последующую сборку длинных сообщений и имеет специальные средства нумерации пакетов, упорядочения и удаления. Транспортный уровень может обеспечивать передачу данных с установлением и без установления связи.

5 Сеансовый уровень (530)

Координирует прием, передачу и установление одного сеанса связи. Обеспечивает необходимый контроль рабочих параметров, управление потоками данных промежуточных накопителей, диалоговый контроль, гарантирующий передачу данных. Кроме этого он может иметь функции:

- управление паролями
- подсчет платы за пользование ресурсами
- управление диалогом с пользователем
- синхронизация и отмена сеанса в случае сбоя при передаче данных вследствие ошибок в нижестоящих уровнях.

6 Уровень представления данных (520)

Предназначен для интерпретации данных и подготовки их для пользовательского прикладного уровня. На данном уровне анализируется представление символов, формат страниц и графическое кодирование вместе с различными правилами шифрования, происходит преобразование из кадра в экранный формат.

7 Прикладной уровень (520)

Определен в наименьшей степени, поскольку реализует все функции, которые не могут быть приписаны нижним уровням. К таким функциям относятся обслуживание сети, управление заданиями и протоколы обмена данными определенного типа. Данный уровень обеспечивает поддержку прикладных процессов конечного пользователя и эмуляцию терминалов.

Архитектурные вопросы построения безопасных компьютерных сетей (520)

Эти вопросы должны включать концепцию, терминологию по архитектурной безопасности сетей и руководство по разработке уровневых и межуровневых протоколов и услуг (или сервисов).

Архитектурным вопросам построения открытых компьютерных сетей на основе модели ВОС посвящен стандарт ISO 7498-2. В его состав включены:

- обзор вопросов безопасности,
- определение услуг и механизмов обеспечения безопасности,
- анализ существующих опасностей (угроз) нарушения работы компьютерных сетей,
- методическая информация о том, какой следует использовать механизм обеспечения безопасности для реализации конкретных услуг безопасности,
- рекомендации о том, какие услуги безопасности могут быть реализованы конкретными протоколами на каждом из семи уровней модели ВОС.

Услуги и механизмы обеспечения безопасности сетей на основе модели ВОС (550)

Архитектурная концепция безопасности ISO включает пять основных компонентов:

- определение услуг безопасности,
- определение механизмов безопасности,
- уровневая модель построения услуг безопасности,
- соотнесение услуг безопасности к уровневой модели,
- соотнесение механизмов безопасности к услугам.

Услуги безопасности представляют собой абстрактные понятия, которые могут быть использованы для характеристики требований безопасности. Услуги отличаются от механизмов безопасности, которые являются конкретными мерами для реализации этих услуг. Важнейшим архитектурным элементом стандарта явля-

ется определение, какие услуги безопасности должны обеспечиваться на каждом уровне эталонной модели.

Основой для такого определения являются следующие ***принципы построения уровневой модели безопасности:***

- Число альтернативных способов обеспечения безопасности должно быть минимизировано. Стандарт не устанавливает строгие рекомендации следовать этому принципу — она направлена на минимизацию стоимости разработки как собственно безопасных услуг и протоколов, так и приложений на их основе.
- Услуги безопасности могут появляться на многих уровнях модели безопасности. Этот принцип противоположен первому и в реальной системе должен достигаться обоснованный баланс или компромисс.
- Функции безопасности не должны дублировать коммуникационные функции, а использовать последние по возможности без нарушения безопасности системы.
- Рекомендуется не нарушать независимость уровней. Такая проблема проявляется в маршрутизаторах и мостах, которые могут анализировать информацию о протоколах более высокого уровня для лучшего контроля трафика и доступа. Эти функции могут быть нарушены при использовании криптографии или изменении протоколов высшего уровня.
- Количество неконтролируемых (доверительных, trusted) функций должно быть минимизировано. Следовательно, необходимо выделять компоненты, собственно определяющие безопасность системы.
- Если какой-либо защитный механизм одного уровня базируется на использовании услуг более низкого уровня, то не должно существовать никаких промежуточных уровней, запрещающих или не гарантирующих такую связь.
- Безопасные услуги, реализуемые на каждом уровне, должны быть определены таким образом, чтобы допускать модульное дополнение к базовым коммуникационным услугам. Этот принцип ориентирован на очень практичный подход, т.к. не все реализации уровневых протоколов и сервисов требуют и/или предлагают все безопасные услуги.

Базовые сервисы для обеспечения безопасности компьютерных систем (550)

Определены пять базовых услуг для обеспечения безопасности компьютерных систем и сетей:

1. Конфиденциальность (Confidentiality),
2. Аутентификация (Authentication),

3. Целостность (Integrity),
4. Контроль доступа (Access Control),
5. Причастность ("неотпирательство", Nonrepudiation).

Для всех этих услуг определены также варианты, как например, для коммуникаций с установлением соединения и без такового, или обеспечения безопасности на уровнях пакетов или отдельных полей. Этот набор услуг не является единственно возможным, однако он общепринят.

Конфиденциальность (553)

Конфиденциальность определена как "свойство, которое гарантирует, что информация не может быть доступна или раскрыта для неавторизованных (неуполномоченных) личностей, объектов или процессов".

Для этой услуги определяется четыре версии:

- системы с установлением связи;
- системы без установления связи;
- защита отдельных информационных полей;
- защита от контроля трафика.

Первые две версии относятся к соответствующим протоколам с установлением или без установления связи. ***Третья*** версия конфиденциальных услуг, предназначенных для защиты отдельных информационных полей, используется для обоих типов сетей (с установлением связи и без) и требует, чтобы только отдельные поля в пакетах были защищены. ***Защита от контроля трафика*** должна предотвращать возможность анализа и контроля трафика. Это достигается путем кодирова-

ния информации об источнике-назначении, количестве передаваемых данных и частоты передачи.

Аутентификация (553)

Рассматриваются два типа услуг аутентификации:

- достоверность происхождения (источника) данных
- достоверность объекта коммуникации (peer-entity).

Достоверность источника данных предполагает подтверждение того, что источник полученных данных именно тот, который указан или объявлен. Эта услуга существенна для коммуникации без установления связи, при которой каждый пакет является независимым от других, и единственное, что может быть гарантировано с точки зрения аутентификации, — это то, что источник пакета именно тот, который указан в заголовке пакета.

В системах с установлением связи, ***аутентификация объекта коммуникаций*** является необходимой функцией, определенной как подтверждение того, что объект коммуникации при соединении именно тот, который объявлен. Эта форма аутентификации подразумевает установление своевременности или фактора времени включением идентификации объекта коммуникации для конкретного случая соединения, которые недостижимы при помощи простой проверки происхождения данных.

Обе формы аутентификации определены для Сетевого, Транспортного и Прикладного уровней, на которых реализуются протоколы с установлением и без установления связи.

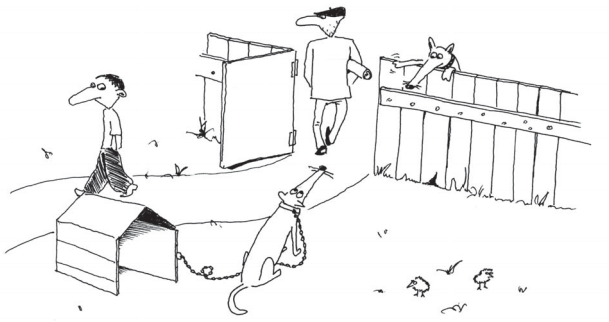
Целостность (553)

Целостность имеет две базовые реализации:

- для сетей с установлением связи
- без установления связи, каждая из которых может применяться для избранных групп информационных полей.

Услуги защиты целостности в сетях с установлением связи могут дополнительно включать функции восстановления данных в случае, когда нарушена их целостность. Таким образом, обеспечение целостности данных в сетях с установлением связи предполагает обнаружение любой модификации, включения, удаления, или повторной передачи данных в последовательности (пакетов). Эта услуга используется на уровнях Сетевом, Транспортном и Прикладном, при этом средства восстановления данных возможны только на двух верхних уровнях.

Целостность в сетях без установления связи ориентирована на определение модификаций каждого пакета, без анализа большего объема информации, например сеанса или цикла передачи. Таким образом, эта услуга не предотвращает умышленное удаление, включение или повторную передачу пакетов и является естественным дополнением аутентификации источника данных. Эта услуга также доступна на уровнях Сетевом, Транспортном и Прикладном.



Контроль доступа...

Контроль доступа (553)

Контроль доступа определен как предотвращение неавторизованного использования ресурсов, включая предотвращение использования ресурсов недопустимым способом. Т.е. данная услуга не только обеспечивает доступ лишь авторизованных пользователей (и процессов), но и гарантирует только указанные права доступа для авторизованных пользователей. Таким образом эта услуга предотвращает неавторизованный доступ как внутренних, так и внешних пользователей.

Контроль доступа часто смешивают с аутентификацией и конфиденциальностью, но в действительности эта услуга предоставляет более широкие возможности. Услуга контроля доступа используется для установления политики контроля/ограничения доступа.

Политика контроля доступа (или авторизации) устанавливается в двух измерениях:

- критерии для принятия решения о доступе,
- средства, при помощи которых регулируется контроль.

Два типа политики доступа в зависимости от используемых критериев принятия решения могут быть основаны на идентичности явлений и объектов (identity-based) или на правилах (последовательности) доступа:

- определяемые пользователем
- определяемые администратором.

Большинство операционных систем реализуют первый вариант, но второй — часто реализуется в сетях общего пользования, например X.25, UUCP и др.

Услугу контроля доступа можно использовать на уровнях Сетевом, Транспортном и Прикладном.

Причастность (553)

Причастность определяется, как предотвращение возможности отказа одним из реальных участников коммуникаций от факта его полного или частичного участия в передаче данных.

Определены две формы причастности:

- причастность к посылке сообщения,
- подтверждение (доказательство) получения сообщения.

Первая форма данной услуги предоставляет получателю доказательства, что сообщение было послано источником и его целостность не нарушена, на случай отказа отправителя от этого факта.

Вторая форма причастности предоставляет источнику доказательства того, что данные были получены получателем, в случае попыток последнего отказаться от этого факта.

Обе формы являются более мощными по сравнению с аутентификацией происхождения данных. Отличием является то, что получатель или отправитель данных может доказать третьей стороне факт посылки (получения) данных и невмешательства посторонних.

Доступность (553)

Доступность может быть определена как дополнительная услуга обеспечения защищенности сетей. Доступность, как одна из услуг обеспечения безопасности, может быть предметом атаки с целью сделать ресурсы или сервисы компьютерной системы недоступными (или сделать их качество неудовлетворительным) для пользователя.

Доступность может быть характеристикой качества данного ресурса либо услуги или, частично, определяться услугой контроля доступа. Однако характер атак с целью ограничения доступа пользователя и средства борьбы с ними не относятся к собственно услугам и ресурсам или не обеспечиваются услугами контроля доступа. Поэтому целесообразно выделение услуги обеспечения доступности, который должен реализовываться специальными механизмами на Сетевом или Прикладном уровне.

Механизмы обеспечения безопасности (554)

Данные механизмы предназначены для обеспечения услуг безопасности, как видно из заголовка. Далее дано краткое описание механизмов безопасности.

Шифрование (554)

Шифрование (Encipherment, в отличие от Encryption) предполагает использование криптографии для преобразование данных, чтобы сделать их нечитаемыми или неосмысленными. Шифрование (кодирование) обычно применяется совместно с комплиментарной функцией — дешифрованием (декодированием). Используется шифрование с симметричными (закрытыми) ключами (secret key) или несимметричными (открытыми) ключами (public key).

Шифрование обычно используется для обеспечения конфиденциальности, но может также поддерживать другие услуги безопасности. Такая возможность существует потому, что любое изменение закодированного текста (шифрограммы) приводит к непредсказуемым изменениям исходного текста. При использовании шифрования можно также реализовать механизмы обеспечения целостности и аутентификации для того же или более высоких уровней. Задача генерации, хранения и распространения криптографических ключей является отдельной задачей управления безопасностью систем.

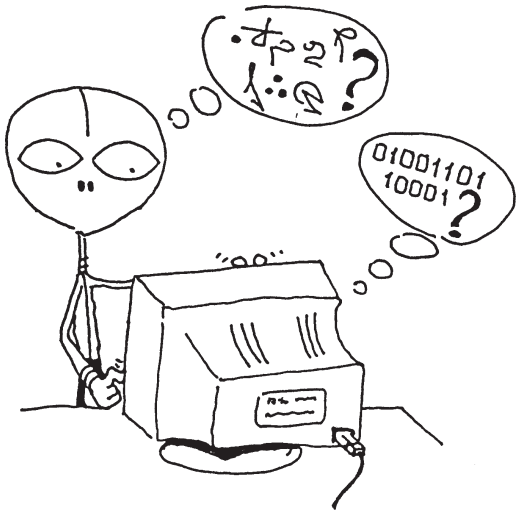
Заполнение трафика (534)

Применяется для обеспечения конфиденциальности трафика (потока) информации для уровней выше Физического (в частности, на Сетевом и Прикладном). Заполнение трафика может включать генерацию случайного трафика, заполнение дополнительными данными информативных пакетов, передачу пакетов через промежуточные станции или в ложном направлении. Оба типа пакетов, как информативный, так и случайный, могут дополняться до постоянной или случайной длины.

Управление маршрутизацией (534)

Применяется для обеспечения конфиденциальности на Сетевом и Прикладном уровнях с целью предотвращения контроля пути следования данных от Отправителя (источника) до Получателя (приемника). Выбор пути может осуществляться конечной системой (source routing — маршрутизация, определяемая источником) или выполняться промежеточной системой, основываясь на использовании меток безопасности, вводимых в пакет конечной системой. Этот механизм требует специальной надежности (доверительности) промежуточных систем и может иметь существенные вариации при использовании различных промежуточных систем. Его также можно использовать для обеспечения целостности с функциями восстановления для выбора альтернативных путей в случаях возникновения атак, приводящих к прерыванию коммуникаций.

Цифровая подпись (534)



Цифровая подпись...

Это достаточно распространенный механизм обеспечения безопасности. Обычно использует открытые ключи, генерируется отправителем данных и проверяется получателем. Несимметричная криптография может использоваться для шифрования контрольной суммы подписываемого сообщения при помощи закрытой части ключа посылателя и в последующем дешифроваться получателем при помощи открытой части ключа отправителя.

Использование открытых ключей для цифровой подписи служит для подтверждения происхождения сообщения, но не контролирует получателя сообщения. Этот механизм используется для обеспечения услуг аутентификации и целостности, для которых субъект верификации подписанных данных заранее неизвестен. При определенном выборе контролируемого параметра цифровая подпись также может применяться для обеспечения услуги причастности.

Механизмы обеспечения контроля доступа (553)

Данные механизмы используются для обеспечения услуг контроля доступа. Большинство этих механизмов пришло из практики безопасности компьютерных систем и часто относятся к вопросам обеспечения политики контроля доступа. Например, для поддержки политики доступа на основе идентификации объекта доступа используется специальная база данных, которая определяет права доступа к ресурсам для отдельных объектов доступа. Другим вариантом данного механизма может быть использование специального маркера "полномочий" для определения текущих прав доступа к имеющимся ресурсам.

Многие механизмы контроля доступа используют механизмы аутентификации для идентификации объекта доступа, или используют "метки безопасности" в случае применения политики доступа на основе правил. Политика доступа на основе правил может использовать также другие данные — время и дату, последовательность (путь) доступа и др.

Механизмы обеспечения целостности данных (553)

Целостность отдельного пакета может быть обеспечена добавлением к нему контрольной величины, которая является функцией содержащихся в пакете данных. Контрольная величина может вычисляться с использованием шифрования или без него. Если контрольная величина вычисляется на уровне, где применяется шифрование, или выше, механизмы этого типа могут быть также использованы как для подтверждения целостности данных в системах без установления связи, так и для аутентификации источника данных. Обычно для этих целей используются симметричные ключи (известные только для посылателя и получателя информации). Применение несимметричных ключей требует большего времени расчетов и поэтому считается неэффективным.

Для обеспечения целостности последовательности пакетов в протоколах с установлением связи одновременно с контрольными величинами отдельных пакетов используются обычные средства протоколов с установлением связи — нумерация пакетов, повторная передача, удаление пакетов, а также дополнительные средства — временные или синхронизирующие метки, обычно используемые для таких применений, как цифровые видео- или аудио приложения.

Механизмы аутентификации (553)

Как было сказано выше, аутентификация источника (происхождения) данных часто обеспечивается использованием механизма целостности совместно с шифрованием. Для широковещательных применений такие же функции может обеспечить цифровая подпись. Логическая аутентификация пользователя компьютерной системы выполняется на основе пароля.

Аутентификация объекта коммуникации обычно выполняется посредством двойного или тройного подтверждения связи ("рукопожатия"), аналогичного механизмам синхронизации нумерации последовательности пакетов в протоколах с установлением связи.

Односторонний (однократный) обмен обеспечивает только однократную аутентификацию и не может гарантировать своевременность обмена.

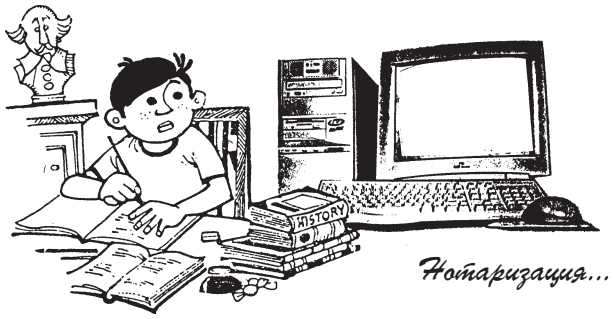
Двусторонний (двухкратный) обмен обеспечивает взаимную аутентификацию источника и приемника, но

не обеспечивает своевременность обмена без специальных средств синхронизации.

Троекратный обмен позволяет достичь полной взаимной аутентификации систем без дополнительной синхронизации. В этом случае также аутентификация использует специальные механизмы управления криптографическими ключами.

Вариант одно-, двух- или трехстороннего обмена для аутентификации источника и приемника реализован в стандарте распределенной службы директорий X.500 (в частности, X.509). При одно- и двукратном обмене аутентифицированными сообщениями используются временные метки, но для распределенных приложений синхронизация системных времен является проблемой.

Нотаризация (заверение) (553)



Механизмы нотаризации (заверения) используют третью сторону, пользующуюся доверием двух общающихся субъектов, для обеспечения подтверждения характеристик передаваемых данных. Наиболее часто механизм нотаризации применяется для обеспечения услуги причастности. Нотаризация может применяться, в частности, совместно с цифровой подписью на основе открытого ключа для подтверждения причастности отправителя данных. Использование нотаризации позволяет включить параметр времени для обеспечения достоверности механизма.

Нотаризация может также применяться для обеспечения надежной временной метки, обеспечиваемой "временным нотариусом". Такая метка может содержать цифровую подпись "нотариуса", идентификатор (кодированный) сообщения, имя отправителя и получателя, а также зарегистрированные время и дату получения сообщения. При этом "нотариус" не имеет доступа к сообщению, соблюдая его конфиденциальность.

Доверительная функциональность (523)

Содержит множество рекомендаций и способов, которые должны быть реализованы для обеспечения гарантии (уверенности) правильной работы других механизмов безопасности.

Для обеспечения надежной (доверительной) работы программного обеспечения, реализующего механизмы безопасности, необходимо соблюдать строгие спецификации и специальную технологию разработки, использование безопасных каналов распространения и многое другое.

Аппаратные средства должна разрабатываться и проверяться на основе единой методики. На этом уровне также обеспечиваются все необходимые требования и рекомендация к электромагнитным излучениям и возможностям физического вмешательства.

Метки безопасности (553)

Явно или косвенно могут быть ассоциированы с отдельными пакетами или последовательностями. Метки безопасности обычно используются для реализации политики доступа на основе правил, а также могут использоваться для управления маршрутизацией в сервисах обеспечения конфиденциальности. Возможно также применения меток для контроля целостности. Если метки безопасности применяются явно, то пакеты с такими метками должны быть защищены от нарушения целостности.

Контроль безопасности (553)

Содержит множество механизмов: обнаружение попыток нарушения безопасности, анализ случаев успешного вмешательства, возникших потерь и др. Но при этом необходимо решение вопросов, какую информацию в системе следует накапливать и как ее затем анализировать. Проблемой при этом является определение того минимума информации, который бы позволил выявить (не пропустить) возможные события по вмешательству в работу компьютерной системы.

Использование услуг безопасности

Физический уровень (554)

Услуги безопасности, предлагаемые на Физическом уровне, обычно обеспечивают защиту каналов "точка-точка", например, между двумя конечными системами или между конечной и промежуточной системами. Действие этой услуги заканчивается в точке окончания канала перед устройством приема или коммутации пакетов.

Однако средства и устройства, обеспечивающие безопасность на этом уровне, обычно привязаны к конкретной технологии передачи сигналов и интегрированы с физическим интерфейсом, что приводит к необходимости использовать идентичные устройства на обоих концах физического и/или виртуального соединения.

Применение средств защиты Физического уровня ограничивается услугами Конфиденциальности для коммуникаций с установлением связи и для защиты от контроля трафика. Другим ограничением использования средств защиты на Физическом уровне является сложность управления ими.

Уровень данных (канальный) (534)

Услуги безопасности уровня Данных реализуются для соединений "точка- точка" аналогично Физического уровня. Действие этой услуги заканчивается в точке приема (конечная система) или коммутации пакетов (включая транслирующие и инкапсулирующие мосты) в пределах использования единого интерфейса управления доступом к среде.

Преимуществом применения услуг безопасности на этом уровне является их независимость от протоколов более высокого уровня. Однако здесь также существует сильная зависимость практической реализации услуги от используемой технологии Физического уровня.

Сетевой уровень (524)

Безопасность на Сетевом уровне обеспечивается между конечными системами, независимо от промежуточных межсетевых коммутаторов и мостов уровня Данных. Если услуги безопасности основываются полностью на протоколах Сетевого уровня, это обеспечивает безопасность коммуникаций между конечными системами вдоль разнородных сетей, формирующих Интерсеть (Internet).

Рекомендуется применение нескольких услуг безопасности на Сетевом уровне:

Конфиденциальность (для систем с установлением и без установления связи, для защиты от контроля трафика),

Контроль доступа,

Целостность в системах с установлением связи,

Аутентификации источника данных и объекта коммуникации.

Услуги безопасности должны быть совместимы с соответствующими коммуникационными услугами на каждом уровне и, по возможности, их использовать, что часто приводит к зависимости реализуемых услуг безопасности от протоколов сетевого уровня или делает невозможным их применение.

Такая ситуация, в частности, наблюдается в сетях X.25, которые имеют собственный протокол нумерации последовательностей с установлением связи, но не имеют средств обеспечения целостности отдельных пакетов, что делает невозможным применение стандартных услуг безопасности. В этом случае возможно применение соответствующих услуг на более высоких уровнях, но приводит к зависимости услуг безопасности от соответствующей технологии Сетевого уровня.

Независимая реализация услуг безопасности на Сетевом уровне позволяет применять эти услуги только в отношении таких объектов, как сети, что является достаточно грубым подходом.

Включение услуг безопасности Сетевого уровня в состав функций конечной системы, как правило, требует модификации ядра операционной системы, так как большинство сетевых операционных систем включают функции сетевого уровня в ядро в целях достижения большей производительности и безопасности системы. Отсюда следует, что включение услуг безопасности Сетевого уровня является задачей поставщиков программных и аппаратных средств конечных и промежуточных систем.

Транспортный уровень (534)

На этом уровне стандарт определяет набор услуг безопасности, очень близкий по составу с Сетевым уровнем:

1. Конфиденциальность (для систем с установлением и без установления связи),
2. Контроль доступа,
3. Целостность в системах с установлением связи и без,
4. Аутентификации источника данных и объекта коммуникации.

Отличием является то, что услуги безопасности Транспортного уровня обеспечиваются только в конечных системах, в отличие от возможности реализации услуг на базе Сетевого уровня в промежуточных системах.

Услуги безопасности Транспортного уровня с установлением связи, в общем случае, обеспечивают более высокую защищенность коммуникаций по сравнению с реализацией таких же услуг на более высоких уровнях с использованием протоколов и услуг более низкого уровня. Но при правильном использовании коммуникационных возможностей Транспортного уровня такие отличия могут быть несущественными.

Как и для Сетевого уровня, многие механизмы безопасности Транспортного уровня интегрированы в состав сетевых операционных систем и определяется их разработчиками.

Транспортный уровень с установлением связи...

Сеансовый уровень и уровень Представления данных (530)

Не рекомендуется применение услуг безопасности на Сеансовом уровне и уровне Представления данных. Это вызвано тем, что эти уровни не имеют хорошо определенных коммуникационных услуг и функций.

Кажущаяся уместность применения многих услуг на основе шифрования на уровне Представления данных нецелесообразна потому, что функции этого уровня обычно интегрированы в состав Прикладного уровня.

Прикладной уровень (530)

Разрешается применение всех услуг безопасности на Прикладном уровне, а применение услуги Причастности рекомендуется только на этом уровне. Однако использование услуг безопасности только на Прикладном уровне не позволяет полностью защитить системы коммуникаций от всех возможных атак, поэтому рекомендуется обеспечивать поддержку конкретных услуг также на более низких уровнях совместно с Прикладным.

Очевидно, что приложения типа обмена сообщениями или службы директорий могут быть реализованы только на Прикладном уровне. ***В частности, обмен сообщениями требует использования услуг безопасности на этом уровне по следующими причинам***:

- Некоторые услуги обеспечения защиты сообщений разработаны только для Прикладного уровня, как например, контроль Причастности.
- Сообщения могут быть адресованы нескольким адресатам и анализ адресов выполняется только на уровне сообщения.
- Услуги безопасности более низких уровней обеспечиваются в реальном времени при обработке потоков данных "точка-точка", в то время как обработка сообщений на уровне "отправитель- получатель" требует полной функциональности сервисов X.400.
- Полная защищенность услуг директорий, согласно X.500, также не может быть обеспечена только использованием услуг более низких уровней. Например, принятие решения о доступе пользователя к серверу директорий или дальнейшая передача запроса должна выполняться только самим сервером.
- Наиболее привлекательной чертой применения услуг безопасности на Прикладном уровне является их независимость от операционной системы и возможность реализовать эти услуги в составе приложений, но при этом используемые механизмы становятся специфическими для конкретного приложения.

Обзор средств защиты информации в ИС (500)

В настоящее время поставщики предлагают широкий спектр программно-аппаратных средств защиты от несанкционированного доступа к ресурсам информационных систем, функционирующих в рамках как отдельных рабочих станций, так и локальных или глобальных сетей. ***Поэтому очень важно понимание заказчиком:***

- своих потребностей по защите,
- финансовых возможностей,
- проблем организации работ по исследованию имеющихся технологий обработки конфиденциальной информации;
- вопросов организации внедрения систем безопасности.

Рассмотрим некоторые группы средств защиты информации.

Средства защиты от НСД (514)

Средства этого направления широко представлены на рынке. В основном они представляют собой программно-аппаратные комплексы с применением личного идентификатора (электронный идентификатор семейства Touch Memory, микропроцессорная карта и т.д.).

Продукты этого класса позволяют разграничивать доступ к информационным ресурсам вычислительной техники, вести аудит сеансов работы, администрировать используемые программные средства. Кроме этого, некоторые из них имеют встроенные антивирусные функции и средства криптографической защиты информации.

При сетевом использовании защищаемых рабочих мест имеется возможность удаленного администрирования каждого из них и получение полной статистики по попыткам доступа к компьютеру и сеансам работы.

Анализаторы протоколов (524)

В процессе управления и решения задач безопасности сетей часто возникает вопрос о сборе информации, декодировании и статистическом анализе информации

с помощью сетевых протоколов разных уровней. Некоторые системы мониторинга (например, DSS фирмы NETWORK GENERAL) содержат в себе такие средства.

Интересно

В случае администрирования небольших корпоративных систем, когда создание мощной системы мониторинга на базе концепции DSS является неприемлемым по экономическим соображениям, потребности администратора безопасности вполне могут удовлетворить портативные анализаторы серии Expert Sniffer Analyzer (ESA), известные также и под названием Turbo Sniffer Analyzer.

Выпускаемые версии продуктов обеспечивают полный анализ, интерпретацию протоколов, а также мониторинг подключенного к анализатору сегмента сети. При этом поддерживаются все те же сетевые топологии, что и для систем DSS. Как правило, ESA используется для периодической проверки некритичных сегментов сети.

Наиболее компактной версией анализатора является Notebook Sniffer Analyzer (NSA), реализованный на базе портативного компьютера Notebook.

Обеспечение безопасности распределенных информационных систем, разработанных в рамках идеологии "клиент-сервер", ставит перед администратором безопасности задачу анализа пакетов не только на уровнях модели OSI ISO, но и на уровне специфики пакетов "клиент-сервер".

Следует отметить, что программным анализаторам протоколов ЛВС, при всем удобстве работы с ними, свойствен существенный недостаток, связанный с необходимостью использования выделенной рабочей станции для выполнения задач по анализу сетевого трафика.

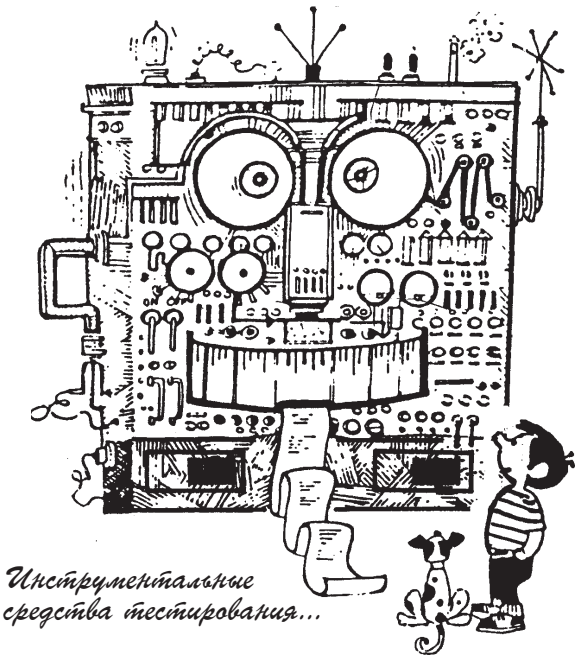
Практика показывает, что корпоративная сеть представляет собой живой организм, и трудно заранее определить тот участок сети, который нуждается в повышенном уровне контроля. Необходимость установки стационарных анализаторов в конкретных точках корпоративной сети определяется в соответствии с принятой политикой безопасности.

Следует учитывать, что эксплуатация стационарного анализатора трафика представляет собой достаточно сложный процесс, требующий участия в нем квалифицированных специалистов.

Инструментальные средства тестирования системы защиты (554)

Систему защиты корпоративной сети целесообразно считать достаточно надежной только при условии постоянного тестирования.

В идеале администратор безопасности должен собирать информацию о возможных атаках, систематизировать ее и периодически осуществлять проверки системы защиты путем моделирования возможных атак.



Инструментальные средства тестирования...

Очевидно, что выполнение этой задачи в полном объеме требует привлечения огромных материальных средств. Но можно обойтись значительно меньшими затратами, если прибегнуть к услугам специальных фирм по производству устройств проверки надежности систем защиты. К таким фирмам относится, например, компания INTERNET SECURITY SYSTEM, обладающая правами на программу INTERNET SCANNER, а также программу SATAN (Security Administrator Tool for Analyzing Networks).

В настоящее время наиболее развитым продуктом тестирования уровня защиты корпоративных сетей является система Internet Scanner SAFEsuite, разработанная фирмой ISS. Этот продукт предоставляет администратору безопасности возможность всесторонней проверки уровня реализации политики безопасности.

Межсетевые экраны (554)

Межсетевые экраны (FireWall-система или Брандмауэр) — это программные продукты, используемые для защиты от несанкционированных действий со стороны внешней сети и для разделения сегментов корпоративной сети.

Работа МЭ в качестве средства защиты осуществляется на трех уровнях:

- фильтрация пакетов,

- шлюзование уровня приложения,
- шлюзование низкого уровня.

В случае применения ***механизмов фильтрации*** пакетов пользователю предоставляется возможность использовать уже имеющиеся и создавать нестандартные фильтры.

Шлюзование уровня приложения позволяет следить за сеансом работы программы и вести его аудит. Эта возможность широко используется для наложения ограничений на трафик на конкретное приложение. Это средство защиты очень удобно благодаря простоте процесса администрирования.

Шлюзование низкого уровня позволяет защищать сетевые ресурсы, связанные с внешним TCP/IP портом.

Это средство контролирует допустимость связи по протоколам TCP/IP и UDP, не идентифицируя конкретное приложение.

Вся информация о сеансах работы протоколируется. Журнал содержит данные о предоставляемых INTERNET-услугах, временных метках событий, источниках пакетов, объемах передачи и приема, продолжительности подключения.

Приобретение брандмауэра (520)

После разработки политики, все еще остаются вопросы в отношении приобретения брандмауэра. Большинство из них аналогичны проблемам при приобретении других программ, поэтому необходимо формулирование требований, их анализ и составление спецификации. Ниже описаны некоторые дополнительные вопросы, включая простейшие критерии выбора брандмауэра, и стоит ли его покупать или лучше сделать самому.

Какими возможностями должен обладать брандмауэр? (523)

Как только принято решение использовать технологию брандмауэра для реализации политики безопасности организации, следующим шагом должно быть приобретение брандмауэра, который обеспечивает требуемый уровень защиты при приемлемой цене. Тем не менее, какие возможности должен иметь брандмауэр, чтобы обеспечивать эффективную защиту? На этот вопрос нельзя дать общего ответа, но можно рекомендовать брандмауэр. ***Брандмауэр должен:***

- иметь средства для реализации политики "все, что не разрешено — запрещено", даже если эта политика не используется в организации;
- иметь возможности полной реализации вашей политики, а не частичной;
- быть гибким, его средства должны иметь возможность адаптации для работы с новыми сервисами и учета изменений в вашей политике безопасности;
- содержать средства усиленной аутентификации или возможности установить их;
- реализовать технологии фильтрации для разрешения или блокирования сервисов на отдельных внутренних системах;
- должен иметь возможности централизованного доступа к SMTP для уменьшения числа прямых соединений по SMTP между внутренними и удаленными системами, что поможет реализовать центральный почтовый сервер сети;
- разрешать публичный доступ к сети таким образом, чтобы информационные серверы могли быть защищены брандмауэром, но отделены от систем, к которым не требуется публичный доступ;
- иметь возможности централизации и фильтрации доступа через коммутируемые каналы;
- содержать механизмы протоколирования трафика и подозрительных действий, а также механизмы уменьшения объема этих журналов для облегчения чтения и проведения анализа;
- быть разработан таким образом, чтобы можно было проверить корректность его работы; он должен иметь простую структуру, чтобы можно было понять логику его работы и сопровождать его.
- оперативно обновляться при обнаружении новых ошибок.

Конечно, существует еще много проблем и требований к брандмауэрам, но большинство из них слишком специфичны. Серьезный подход к формулированию требований или оценке риска позволит выявить самые важные проблемы и требования, но не следует забывать, что Internet — это постоянно растущая сеть. Обнаруживаются новые уязвимые места, появляются новые сервисы и улучшение старых сервисов, которые могут создать проблемы при работе брандмауэра. Поэтому всегда следует помнить о необходимости гибкости для учета изменений в требованиях.

Покупать или самому создавать брандмауэр (520)

Ряд организаций имеет возможности для самостоятельного создания брандмауэра, т.е. для объединения имеющихся программных компонентов и оборудования или написания программ с нуля. В то же время некоторые производители предлагают немало средств в области брандмауэров. Эти средства могут быть ограниченными, предоставлять только необходимое программное и аппаратное обеспечение или помощь в разработке по-

литики безопасности, оценке риска, проверке защищенности сети и обучении сотрудников.

Независимо от того, создаете ли вы брандмауэр самостоятельно или покупаете, не забывайте, что сначала нужно разработать политику и набор связанных с ней требований к брандмауэру, а уже затем начинать работу над ним. В случае трудностей при разработке политики целесообразно связаться с производителем, который может помочь в этом процессе. Если же в организации имеется свой опыт создания брандмауэров, то лучше и дешевле использовать его. ***Одним из преимуществ самостоятельного создания брандмауэра является то, что свои сотрудники знают специфику организации*** и то, как будет использоваться брандмауэр. Если брандмауэр приобретается, то такого опыта может и не быть.

Вместе с тем брандмауэр может оказаться слишком дорогим в смысле времени, необходимого для его создания и документирования, а также времени, требуемого для сопровождения брандмауэра и внесения в него изменений при возникновении такой необходимости. Затраты такого рода иногда не учитываются; организации допускают ошибку, учитывая только стоимость оборудования. При полном экономическом расчете затрат, связанных с созданием брандмауэра, может оказаться, что выгоднее купить его.

При принятии решения организацией о том, покупать или создавать брандмауэр с учетом имеющихся ресурсов, могут помочь ответы на следующие вопросы:

- Как будет тестироваться брандмауэр; кто будет проверять, что он работает так, как это ожидается.
- Кто будет сопровождать его (делать архивные копии, восстанавливать его после сбоев).
- Кто будет устанавливать обновления брандмауэра — новые прокси-серверы, исправление ошибок и другие расширения.
- Могут ли быть оперативно внесены исправления, связанные с безопасностью, и решены собственно проблемы с безопасностью.
- Кто будет обучать пользователей и обеспечивать техническую поддержку для них.

Многие производители предлагают сопровождение брандмауэра, а также помощь в его установке, поэтому организация должна учесть это при анализе вопроса, имеет ли она достаточные внутренние ресурсы для этого.

Резюме

Многообразие способов построения ИС, неопределенность стандартов и законодательной базы в области информационной безопасности, а также широкий выбор методов и средств защиты информации порождают обилие вариантов решений вопросов создания СЗИ.

Рынок средств защиты информации столь широк по стоимости, назначению и качеству продуктов, что выбор наиболее оптимальных из них для конкретного объекта представляется весьма непростой задачей. Как разобраться среди широкого выбора способов и средств защиты ? Какие из принятых вариантов решений окажутся правильными?

При принятии решений администраторы сталкиваются с проблемой совершения выбора на основе учета принципов деятельности организации, соотношения важности целей, и наличия ресурсов. Эти решения включают определение того, как будут защищаться технические и информационные ресурсы, а также как должны вести себя служащие в тех или иных ситуациях.

Стандарт ISO 7498-2 определяет пять базовых услуг для обеспечения безопасности компьютерных систем и сетей:

1. Конфиденциальность (Confidentiality),
2. Аутентификация (Authentication),
3. Целостность (Integrity),
4. Контроль доступа (Access Control),
5. Причастность («неотпирательство», Nonrepudiation).

Для всех этих услуг определены также варианты, как например, для коммуникаций с установлением соединения и без установления соединения, или обеспечения безопасности на уровнях коммуникации, пакетов или отдельных полей. Этот набор услуг не является единственно возможным, однако он является общепринятым.

В настоящее время поставщики предлагают широкий спектр программно-аппаратных средств защиты от несанкционированного доступа к ресурсам автоматизированных систем, функционирующих в рамках как отдельных рабочих станций, так и локальных или глобальных сетей. Поэтому очень важно понимание заказчиком:

- своих потребностей по защите,
- финансовых возможностей,

- проблем организации работ по исследованию имеющихся технологий обработки конфиденциальной информации;
- вопросов организации внедрения систем безопасности.

Систему защиты корпоративной сети разумно считать достаточно надежной только при условии проведения постоянного тестирования.

В идеале администратор безопасности должен собирать информацию о возможных атаках, систематизировать ее и периодически осуществлять проверки системы защиты путем моделирования возможных атак.

Очевидно, что выполнение этой задачи в полном объеме требует привлечения огромных материальных средств. Но можно обойтись значительно меньшими затратами, если прибегнуть к услугам фирм, специализирующихся на производстве устройств проверки надежности систем защиты. К таким фирмам относится, например, компания INTERNET SECURITY SYSTEM, обладающая правами на программу INTERNET SCANNER, а также программу SATAN (Security Administrator Tool for Analyzing Networks).