МЕЖДУНАРОДНЫЙ СТАНДАРТ

ISO/IEC 18043

Первое издание
2006-06-15

Информационные технологии. Методы защиты. Выбор, применение и операции систем обнаружения вторжения

Information technology — Security techniques — Selection, deployment and operations of intrusion detection systems

Ответственность за подготовку русской версии несёт GOST R (Российская Федерация) в соответствии со статьёй 18.1 Устава ISO

Ссылочный номер
ISO/IEC 18043:2006(R)

Отказ от ответственности при работе в PDF

Настоящий файл PDF может содержать интегрированные шрифты. В соответствии с условиями лицензирования, принятыми фирмой Adobe, этот файл можно распечатать или смотреть на экране, но его нельзя изменить, пока не будет получена лицензия на интегрированные шрифты и они не будут установлены на компьютере, на котором ведется редактирование. В случае загрузки настоящего файла заинтересованные стороны принимают на себя ответственность за соблюдение лицензионных условий фирмы Adobe. Центральный секретариат ISO не несет никакой ответственности в этом отношении.

Adobe - торговый знак фирмы Adobe Systems Incorporated.

Подробности, относящиеся к программным продуктам, использованные для создания настоящего файла PDF, можно найти в рубрике General Info файла; параметры создания PDF были оптимизированы для печати. Были приняты во внимание все меры предосторожности с тем, чтобы обеспечить пригодность настоящего файла для использования комитетами-членами ISO. В редких случаях возникновения проблемы, связанной со сказанным выше, просьба проинформировать Центральный секретариат по адресу, приведенному ниже.

ДОКУМЕНТ ЗАЩИЩЕН АВТОРСКИМ ПРАВОМ

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Опубликовано в Швейцарии

Содержание

Страница

Предисловие

Международная организация по стандартизации (ISO) и Международная электротехническая комиссия (IEC) создали специализированную систему всемирной стандартизации. Национальные организации, являющиеся комитетами-членами ISO или IEC, участвуют в разработке международных стандартов через технические комитеты, учрежденные соответствующей организацией для того, чтобы заниматься отдельными областями технической деятельности. Технические комитеты ISO и IEC сотрудничают в областях, представляющих взаимный интерес. Другие правительственные и неправительственные международные организации, сотрудничающие с ISO и IEC, также принимают участие в этой работе. В области информационной технологии ISO и IEC учредили Совместный Технический комитет ISO/IEC JTC1.

Проекты международных стандартов разрабатываются согласно правилам, привёденным в Директивах ISO/IEC, Часть 2.

Основной задачей технических комитетов является подготовка международных стандартов. Проекты международных стандартов, принятые техническими комитетами, рассылаются комитетам-членам на голосование. Для публикации в качестве международного стандарта требуется одобрение не менее 75 % комитетов-членов, принявших участие в голосовании.

Следует иметь в виду, что, возможно, некоторые элементы настоящего документа могут быть объектом патентных прав. ISO не несет ответственность за определение некоторых или всех таких патентных прав.

ISO/IEC 18043 подготовлен Совместным Техническим комитетом ISO/IEC JTC1, *Информационные технологии,* Подкомитетом SC 27, *Методы защиты в Информационных технологиях.*

Официальное уведомление

Национальный Институт Стандартов и Технологии (NIST) настоящим предоставляет ISO/IEC неисключительную лицензию на использование Специальной публикации NIST по Системам обнаружения вторжения (SP800-31) при разработке Международного стандарта ISO/IEC 18043. Однако NIST сохраняет право на использование, копирование, распространение или модификацию SP800-31, когда он посчитает это необходимым.

Введение

Организации должны не только знать когда, где и как произошло вторжение в их сеть, систему или приложение, они также должны знать какое слабое место было использовано и какие меры безопасности или соответствующие опции обработки рисков (т.е. перенос риска, приемлемая степень риска, исключение риска) должны быть реализованы, чтобы предотвратить подобное вторжение в будущем. Организации должны также распознавать и отражать кибернетические проникновения. Это требует анализа хост и сетевого трафика и/или контрольного следа для сигнатур атаки или специфичного шаблона, которые обычно указывают злонамеренные или подозрительные намерения. В середине 1990 годов организации начали использовать Системы Обнаружения Вторжения (IDS) для осуществления этих потребностей. Общее применение IDS продолжает расширяться с более широким набором продуктов IDS, которые стали доступны для удовлетворения возрастающего уровня запросов организаций в повышенных возможностях обнаружения вторжения.

Для организации в порядке вещей извлекать максимальные выгоды от IDS, поэтому процесс выбора IDS, ввод в действие и операции должны тщательно планироваться и реализовываться надлежащим образом подготовленным и опытным персоналом. В случае, когда этот процесс успешно выполняется, продукты IDS могут помочь организации получить информацию о вторжении и могут использоваться как важное предохранительное средство в общей инфраструктуре информационной и коммуникационной технологии (ICT).

Данный международный стандарт обеспечивает руководящие принципы для эффективного выбора IDS, ввода в действие и эксплуатацию, а также основные сведения об IDS. Он также пригоден для тех организаций, которые рассматривают привлечение соисполнителей для реализации возможностей обнаружения вторжения. Информацию по соглашениям на уровне услуг внешних соисполнителей можно найти в процессах Менеджмента услуг в Информационных технологиях (ITSM) на базе ISO/IEC 20000.

Информационные технологии. Методы защиты. Выбор, применение и операции систем обнаружения вторжения

1 Область применения

В данном международном стандарте предусматриваются руководящие принципы для помощи организациям в использовании Системы Обнаружения Вторжения (IDS). В частности, в стандарте обращается внимание на выбор, применение и операции IDS. Он также содержит дополнительную информацию, на основании которой эти руководящие принципы были получены.

Данный международный стандарт может быть полезен:

a) организации в удовлетворении следующих требований ISO/IEC 27001:

- Организация должна реализовать процедуры и другие управляющие воздействия, способные к быстрому обнаружению и ответным действиям при инцидентах защиты.
- Организация должна выполнять процедуры мониторинга и анализа и другие управляющие воздействия для надлежащего распознавания неудавшихся и успешных нарушений защиты и инцидентов.

b) организации в реализации средств управления, которые удовлетворяют следующим целям защиты ISO/IEC 17799.

– Обнаружить несанкционированные действия при обработке информации.

– Системы должны отслеживаться, и события информационной безопасности должны регистрироваться. Должны использоваться операторские журналы регистрации и журналы регистрации неисправностей для идентификации проблем информационной системы..

– Организация должна соблюдать все соответствующие юридические требования, применимые к действиям по мониторингу и регистрации.

– Должен использоваться мониторинг системы для проверки эффективности принятых средств управления и проверки соответствия модели стратегии доступа.

Организация должна признать, что использование IDS не является единственным и/или исчерпывающим решением для удовлетворения и соответствия вышеназванным требованиям. Более того, данный международный стандарт не предназначен быть критерием для оценок соответствия любого вида, например, для сертификации как Системы Менеджмента Защиты Информации (ISMS), сертификации продуктов и услуг IDS.

2 Термины и определения

Применительно к данному документу применяются следующие термины и определения.

2.1
атака
attack
попытки разрушить, подвергнуть воздействию, изменить или вывести из строя Информационную систему и/или информацию в ней или иные нарушения политики безопасности

2.2
сигнатура атаки
attack signature
последовательность компьютерных действий или изменений, которые использовались при атаке и которые используются также IDS для обнаружения атаки и часто определяются путем проверки сетевого трафика или журналов хост- машины

ПРИМЕЧАНИЕ Она может рассматриваться также как шаблон атаки.

2.3
удостоверение
attestation
вариант шифрования открытым ключом, который позволяет программам и устройствам IDS аутентифицировать их идентичность с удаленными участвующими сторонами

ПРИМЕЧАНИЕ См. Раздел 2.21, Удаленное удостоверение.

2.4
мост
bridge
сетевое оборудование, которое прозрачно соединяет локальную сеть (LAN) на уровне 2 OSI к другой локальной сети, которая использует тот же протокол

2.5
криптографическое значение хэш-функции
cryptographic hash value
математическое значение, которое присваивается файлу и используется для последующего “тестирования” этого файла, чтобы проверить не изменились ли предумышленно данные, содержащиеся в этом файле

2.6
отказ от обслуживания при атаке
DoS (Denial-of-Service) attack
предотвращение санкционированного доступа к ресурсам системы или задержка операций или функций системы

[ISO/IEC 18028-1]

2.7
демилитаризованная зона
Demilitarized Zone DMZ
логическое и физическое сетевое пространство между маршрутизатором периметра и внешним брандмауэром

ПРИМЕЧАНИЕ 1 DMZ может быть между сетями и подвергаться тщательному наблюдению, но не быть им.

ПРИМЕЧАНИЕ 2 Ими обычно являются незащищенные области, содержащие защищенные хост-машины, которые предоставляют услуги общего пользования.

2.8
использовать
exploit
определенный способ прорвать защиту Информационной системы через слабое место

2.9
брандмауэр
firewall
тип защитного шлюза или барьера, размещенного между сетевыми средами – состоящий из

специализированного устройства или составной из нескольких компонентов и методов – через который проходят все трафики из одной сетевой среды в другую, и разрешается пропускать только санкционированный трафик

[ISO/IEC 18028-1]

2.10
ошибочный допуск
false positive
предупреждение IDS, когда нет атаки

2.11
ошибочный отказ
false negative
нет предупреждения IDS, когда происходит атака

2.12
хост
host
адресуемая система или компьютер в сетях на базе TCP/IP, аналогичных Интернету

2.13
злоумышленник
intruder
субъект, который проводит или провел вторжение или атаку на хост, сеть, сайт или организацию

2.14
вторжение
intrusion
несанкционированный доступ к сети или системе, подсоединенной к сети, т.е. предумышленный или случайный доступ несанкционированный доступ к информационной системе для включения злонамеренного действия против системы, или несанкционированное использования ресурсов в информационной системе

2.15
обнаружение вторжения
intrusion detection
формальный процесс обнаружения вторжений, обычно характеризующийся получением знаний о ненормальном использовании шаблонов, а также какого рода, как и какое слабое место было использовано, включая как и когда это произошло

2.16
система обнаружения вторжения
intrusion detection system
IDS
информационная система, используемая для определения того, была ли попытка вторжения, оно происходит или произошло, а также ответного действия в Информационной системе и сетях

2.17
система предотвращения вторжения
intrusion prevention system
IPS
вариант систем обнаружения вторжения, который специально разработан для обеспечения возможности активного ответного действия

2.18
приманка
honeypot
обобщающий термин для ложной системы, используемой для обмана, отвлечения, отвода и поощрения нарушителя затратить время на информацию, которая появляется как ценная, но фактически сфабрикована и не представляет интереса для законного пользователя

2.19
проникновение
penetration
несанкционированный акт обхода механизмов защиты Информационной системы

2.20
инициализация
provisioning
процесс удаленного поиска новых обновлений программ с веб-сайта поставщика и загрузка обновлений в установленном порядке

2.21
удаленное удостоверение
remote attestation
процессы использования цифровых сертификатов для обеспечения идентичности, а также технической и программной конфигурации IDS и безопасной передачи этой информации в доверенный цент службы эксплуатации

2.22
ответное действие (ответ на событие или ответ на вторжение)
response (incident response or intrusion response)
действия, принимаемые для защиты и восстановления нормальных рабочих условий Информационной Системы и хранимой в ней информации, когда происходит атака или вторжение

2.23
маршрутизатор
router
сетевое устройство, используемое для установления и контроля потока данных между различными сетями, которое само может базироваться на различных сетевых протоколах, путем выбора путей или маршрутов на основе механизмов или алгоритмов протокола маршрутизации

ПРИМЕЧАНИЕ Информация по маршрутизации хранится в таблице маршрутов.

[ISO/IEC 18028-1]

2.24
сервер
server
компьютерная система или программа, которая предоставляет услуги другим компьютерам

2.25
соглашение об уровне сервиса
Service Level Agreement
контракт, который определяет техническую поддержку или требуемые профессиональные рабочие характеристики, включая функционирование и последствия при неисправности, которые провайдер может предоставить своим клиентам

2.26
сенсор
sensor
компонент/агент IDS, который собирает данные о событиях из Информационной Системы или сети, находящейся под наблюдением

ПРИМЕЧАНИЕ Указывается также как монитор.

2.27
подсеть
subnet
часть сети, в которой совместно используется компонент общих адресов

2.28
переключатель
switch
устройство, которое обеспечивает возможность соединения между устройствами, объединенными в сеть, с помощью внутренних механизмов переключения

ПРИМЕЧАНИЕ Переключатели отличаются от других устройств межкомпонентного соединения в локальной сети (например, от концентратора), поскольку технология, используемая в переключателях, устанавливает соединения на двухточечной основе. Это гарантирует, что сетевой трафик рассматривается только адресуемыми сетевыми устройствами и дает возможность при маршрутизации иметь несколько соединений одновременно.

[ISO/IEC 18028-1]

2.29
контрольные точки доступа
Test Access Points
TAP
обычно пассивные устройства, которые не устанавливают служебные данные на пакете, они также повышают уровень защиты, поскольку они делают интерфейс сбора данных невидимым в сети, когда переключатель может еще поддерживать информацию уровня 2 о порте. TAP предоставляет также функциональные возможности для многих портов, поэтому проблемы сети могут отлаживаться без потери возможностей IDS

2.30
троянский конь
trojan horse
злоумышленная программа, которая выдает себя за благоприятное приложение

3 Предварительные данные

Назначение Системы Обнаружения Вторжения (IDS) состоит в пассивном мониторинге, обнаружении и регистрации несоответствующих, неправильных, подозрительных или ненормальных действий, которые могут представлять собой вторжение, и обеспечении предупреждения, когда такие действия обнаруживаются. На персонале Обеспечения безопасности Информационной Системы лежит ответственность за активный просмотр журналов регистрации IDS и принятие решения по последующим действиям при любой попытке несоответствующего доступа.

Когда организации необходимо быстро обнаруживать вторжения в ее Информационную систему и быстро реагировать на них, организация должна рассмотреть применение IDS. Организация может развернуть IDS путем приобретения программного обеспечения и/или аппаратных изделий или путем привлечения внешних возможностей IDS у провайдера услуг IDS.

Существует много коммерчески доступных или открытых продуктов и услуг IDS, которые основаны на различных технологиях и подходах. Кроме того, IDS не является технологией “включай и работай”. Поэтому когда организация готовится к использованию IDS, она должна быть, как минимум,

ознакомлена с руководящими принципами и информацией, приводимой в данном стандарте.

Основные сведения о IDS представлены, главным образом, в Приложении А. В этом Приложении поясняются различные характеристики двух основных типов IDS: IDS на базе хост- машины (HIDS) и IDS на базе сети (NIDS), а также двух основных подходов при анализе во время обнаружения, т.е. Подход на основе злоупотребления и Подход на основе аномалии.

Для HIDS источником информации для обнаружения является одна хост- машина, в то время как NIDS извлекает ее из трафика на сегменте сети. В подходе на базе злоупотребления атаки на Информационные системы моделируются как характерные сигнатуры атаки, система систематически сканируется на появление этих сигнатур атаки. Процесс включает специальное кодирование предшествующего поведения и действий, которые считались вторжениями или злоумышленными. Подход на базе аномалий пытается обнаружить вторжения путем фиксации значительных отклонений от нормального поведения. Он функционирует в предположении, что атаки отличаются от нормальной/законной работы и, следовательно, могут быть обнаружены системами, которые идентифицируют эти различия.

Организация должна понимать, что источник информации и различные подходы к анализу имеют как достоинства, так и недостатки или ограничения, которые могут повлиять на способность или неспособность обнаружить атаки и на степень сложности, связанный с установкой и поддержанием IDS.

4 Общие положения

Функции и ограничения IDS, представленные а Приложении А, указывают на то, что организация должна комбинировать подходы на базе хост- машины (включая мониторинг приложений) и на базе сети для достижения достаточно полного охвата возможных вторжений. Каждый тип IDS имеет свою силу и ограничения; вместе они могут лучше обеспечить охват событий защиты и анализ тревожных сигналов.

Объединение технологий IDS зависит от наличия механизма взаимосвязи в системе управления предупреждениями. Ручное соединение предупреждений HIDS и NIDS может привести к перегрузке оператора IDS без какой-либо дополнительной пользы, и результат может быть хуже, чем при выборе наиболее подходящих выходных данных IDS одного типа.

Процесс выбора, применения и эксплуатации IDS в рамках организации показан на Рисунке 1 вместе с указанием раздела, в котором описываются основные шаги в этом процессе.

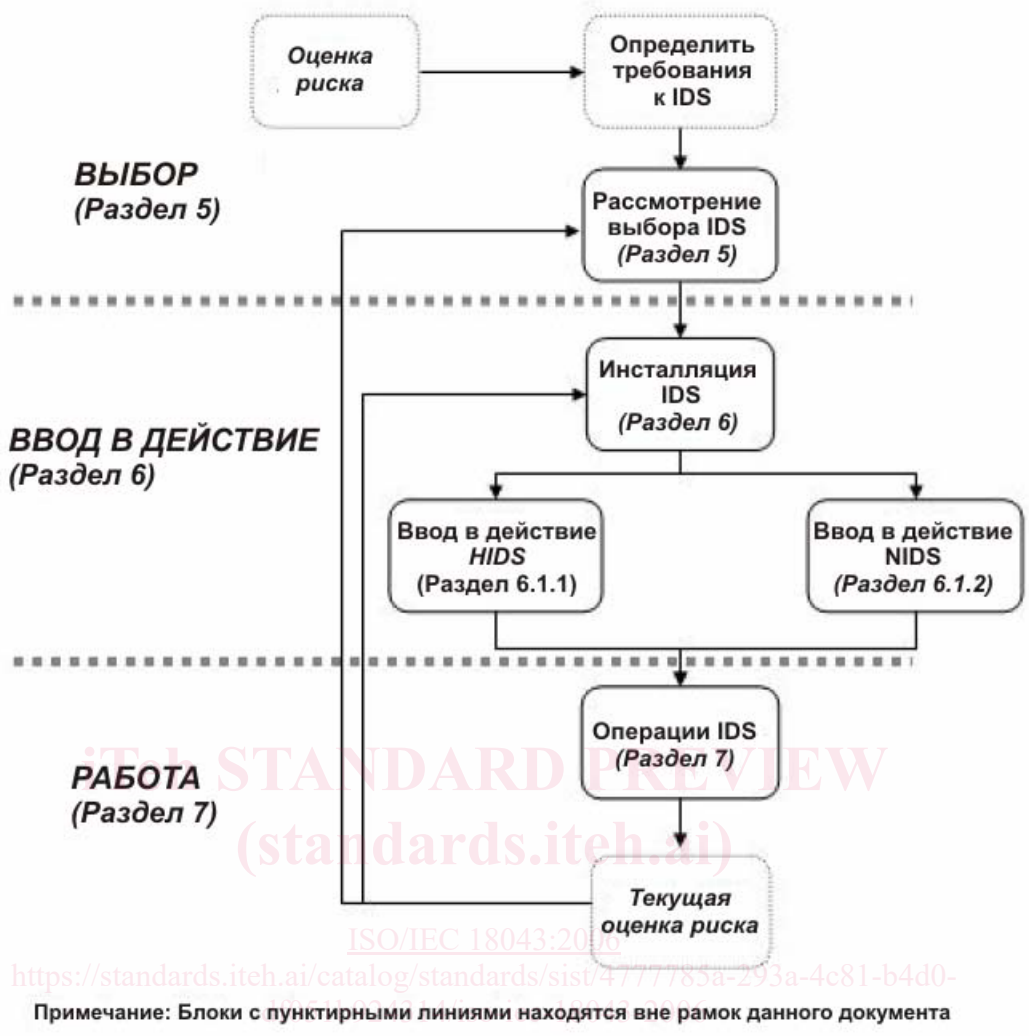

Рисунок 1 - Выбор, ввод в действие и операции IDS

5 Выбор

Существует много доступных продуктов IDS и семейств этих продуктов. Они колеблются от рыночных предложений свободно распространяемого ПО, которые могут применяться на недорогих хост – машинах, до очень дорогостоящих коммерческих систем, требующих наличия самых последних технических средств. Поскольку при выборе существует много различных продуктов IDS, процесс выбора IDS, который наилучшим образом подходил бы к потребностям организации, достаточно трудный. Более того, может быть ограниченная совместимость между различными продуктами IDS, предлагаемыми на рынке. Кроме того, при слияниях и возможном широком географическом распространении организации, эти организации могут быть вынуждены использовать различные IDS, и может потребоваться объединение этих различных IDS.

В брошюре поставщика может не описываться, как хорошо IDS может обнаруживать вторжения и как сложно вводить их в действие, эксплуатировать и поддерживать в рабочей сети со значительным объемом трафика. Поставщики могут указать, какие атаки могут быть обнаружены, но без доступа к сетевому трафику организации очень трудно описать, как хорошо IDS работать, и исключать ошибочные отказы в доступе и ошибочные допуски. Следовательно, полагаться на предоставляемую поставщиком информацию о возможностях IDS не достаточно и не рекомендуется.

Для оценки IDS может использоваться стандарт ISO/IEC 15408 (все части). В этом случае документ с названием “Security Target (Целевой объект защиты)” может содержать более точное и надежное описание характеристик IDS, чем брошюры поставщика. Организация должна использовать этот

документ в процессе выбора.

В следующих пунктах описываются основные факторы, которые следует учитывать в процессе выбора IDS.

5.1 Оценка риска информационной безопасности

Перед выбором IDS организация должна выполнить оценку риска информационной безопасности с целью определения атак и вторжений (угроз), при которых конкретная Информационная система организации может быть уязвима с учетом таких факторов как характер используемой информации в системе и как ее необходимо защищать, типов используемых систем связи и других рабочих факторов и факторов окружения. При рассмотрении этих потенциальных угроз в контексте их конкретных целей информационной безопасности организация может определить элементы управления, которые обеспечат экономически целесообразное уменьшение рисков. Определенные элементы управления обеспечили бы основу требований к функциям, предусмотренным в IDS.

Примечание Управление рисками информационной безопасности будет предметом будущего международного стандарта (ISO/IEC 13335-2).

После установки IDS следует организовать действенное текущее управление рисками, чтобы периодически оценивать эффективность элементов управления при изменениях операций системы и фактических угроз.

5.2 IDS на базе хост- машины и сети

Применение IDS должно основываться на организационной Оценке Риска и приоритетах защиты ресурсов. При выборе IDS должен быть изучен наиболее эффективный метод контроля событий. IDS на базе хост- машины (HIDS) и на базе сети (NIDS) могут применяться в тандеме. Если выбран такой метод мониторинга IDS, организация должна реализовать его поэтапно, начиная с NIDS, поскольку они обычно более простые в установке и обслуживании, затем следует использовать HIDS на ответственных серверах.

Каждый вариант имеет свои достоинства и недостатки. Например, в случае, когда IDS применяется за пределами внешнего брандмауэра, IDS может генерировать большое число тревожных сигналов, которые не требуют тщательного анализа, поскольку при сканировании может определяться большое число событий с предупреждениями, которые эффективно предотвращаются внешним брандмауэром.

5.2.1 IDS на базе хост- машины

Выбор HIDS требует идентификации целевых хост- машин. Поскольку полномасштабное применение HIDS на каждой хост- машине достаточно дорогостоящее, в организации обычно HIDS используется только на ответственных хост- машинах. Поэтому применение HIDS должно иметь приоритеты в соответствии с результатами анализа риска и учета затрат – выгод. Организация должна применять IDS, способные к централизованному управлению с функциями регистрации, если HIDS используется на всех или значительном числе хост -машин.

5.2.2 IDS на базе сети

При использовании NIDS основной вопрос состоит в том, где разместить сенсоры системы. Вариантами являются:

- Внутри внешнего брандмауэра;
- За пределами внешнего брандмауэра;
- На главной сетевой магистрали;
- В ответственных подсетях.

5.3 Обсуждение

5.3.1 Окружение системы

Организация на основе оценки риска безопасности должна сначала определить, в порядке приоритетов, какие ресурсы должны защищаться и после этого приспособить IDS к этому окружению. Как минимум, следующая информация о системном окружении должна собираться для достижения этой цели:

- Сетевые графики и карты, определяющие число и расположение хост- машин, точки входа в сети и подключения к внешним сетям;
- Описание системы управления сетями предприятия;
- Операционные системы каждой хост- машины;
- Число и типы сетевых устройств, таких как маршрутизаторы, мосты и переключатели;
- Число и типы серверов и коммутируемых соединений по телефонной линии;
- Дескрипторы любых сетевых серверов, включая типы, конфигурации, прикладное программное обеспечение и версии режима на каждом;
- Подсоединение к внешним сетям, включая номинальную пропускную способность и поддерживаемые протоколы;
- Пути возврата документов, отличные от входящего соединительного пути, т.е. ассиметричный поток данных.

5.3.2 Обеспечение безопасности

После документирования технических характеристик окружения системы должны быть определены установленные в настоящее время механизмы обеспечения секретности. Необходима, как минимум, следующая информация:

- Демилитаризованная Зона (DMZ)
- Число, типы и размещение брандмауэров и фильтрующих маршрутизаторов;
- Идентификация серверов аутентификации;
- Кодирование данных и связей;
- Пакеты MALWARE/Антивирус;
- Средства управления доступом;
- Специализированные технические средства защиты, такие как шифровальное оборудование;
- Виртуальные частные сети;
- Любые другие установленные механизмы защиты.

5.3.3 Политика безопасности IDS

После идентификации системных и общих условий безопасности должна быть определена для IDS политика безопасности. Для определения политики, как минимум, требуется ответить на следующие основные вопросы: