Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Московский государственный технический университет имени Н.Э. Баумана»
(МГТУ им. Н.Э. Баумана)

Основы обеспечения информационной безопасности

Защита информации в телекоммуникационных сетях

Кафедра «Защита информации»

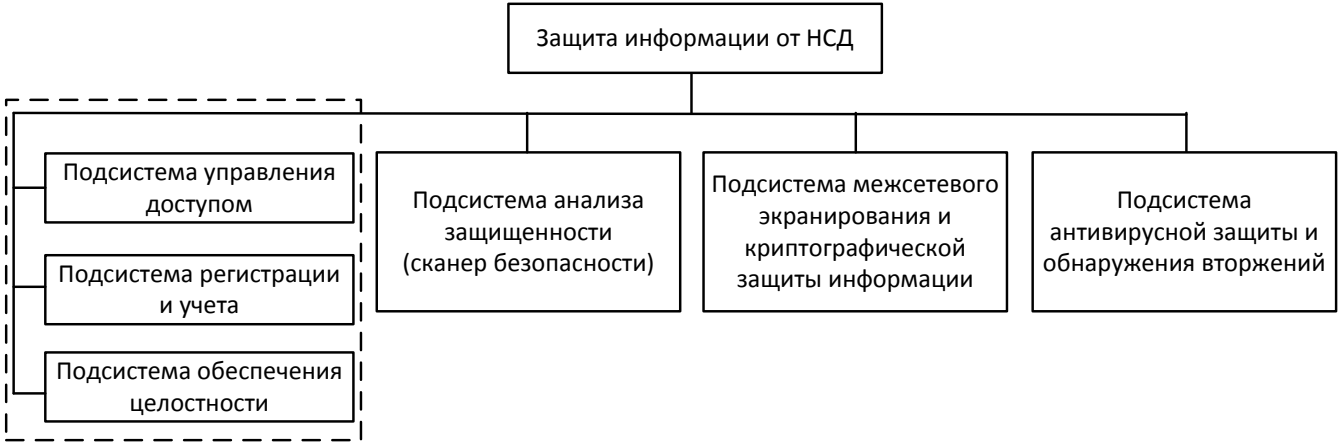
Информационно-телекоммуникационная сеть - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использов анием средств вычислительной техники.

При рассмотрении безопасности информационных систем обычно выделяют две группы проблем: безопасность компьютера и сетевую безопасность.

К безопасности компьютера относят все проблемы защиты данных, хранящихся и обрабатываемых компьютером, который рассматривается как автономная система. Эти проблемы решаются средствами операционных систем и приложений, таких как базы данных, серверы приложений и т.д., а так же встроенными аппаратными средствами компьютера.

Под сетевой безопасностью понимают все вопросы, связанные со взаимодействием устройств в сети. Это, прежде всего, защита данных в момент их передачи по линиям связи и защита от несанкционированного удаленного доступа в сеть.

Основные подсистемы защиты информации



Подсистема анализа защищенности. Должна обеспечивать анализ настроек и выявление уязвимостей объектов сетевой инфраструктуры, контроль изменений в конфигурациях элементов ИС, регистрацию в журнале аудита событий, нарушающих политику безопасности компонентов ИС.

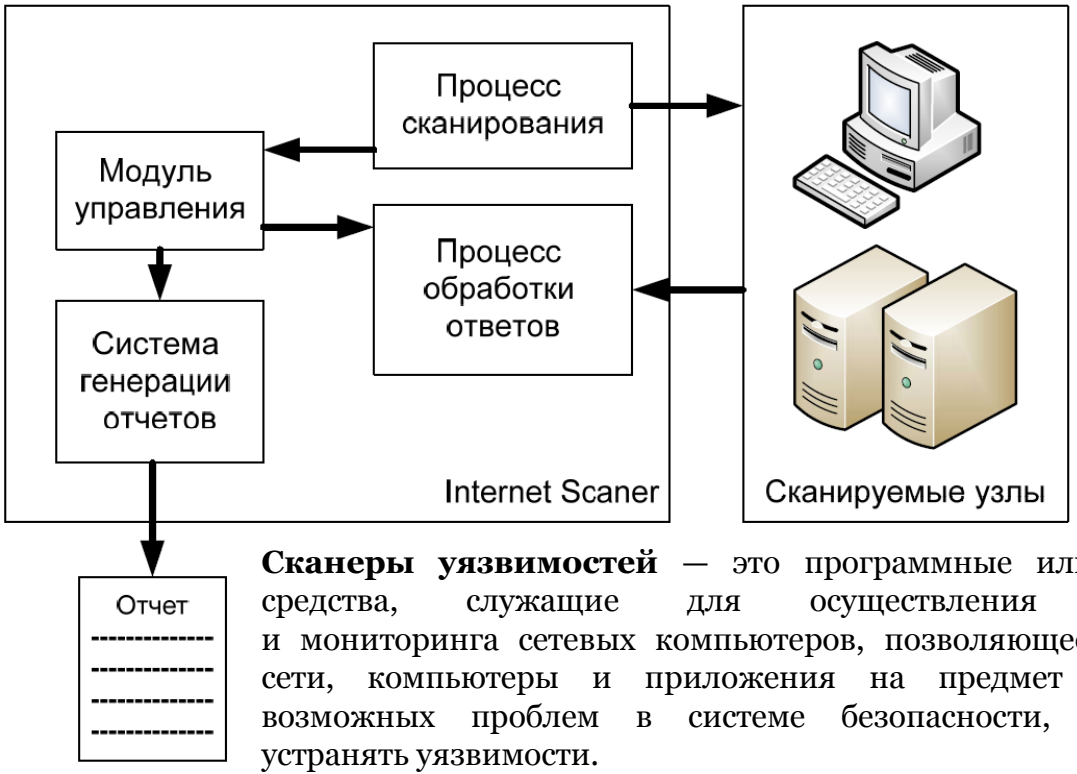
Подсистема антивирусной защиты. Должна обеспечивать надежный контроль над всеми потенциальными источниками проникновения вредоносных программ в ИС.

Подсистема обнаружения вторжений. Предназначена для выявления фактов неавторизованного доступа в компьютерную систему или сеть либо несанкционированного управления ими в основном через Интернет.

Подсистема межсетевого экранирования. Обеспечивает фильтрацию трафика.

Подсистема криптографической защиты. Подсистема, позволяющая усилить защиту информации от несанкционированного доступа посредством использования механизмов шифрования пользовательских данных.

Средства анализа защищенности сетей



Сканеры уязвимостей — это программные или аппаратные средства, служащие для осуществления диагностики и мониторинга сетевых компьютеров, позволяющее сканировать сети, компьютеры и приложения на предмет обнаружения возможных проблем в системе безопасности, оценивать и устранять уязвимости.

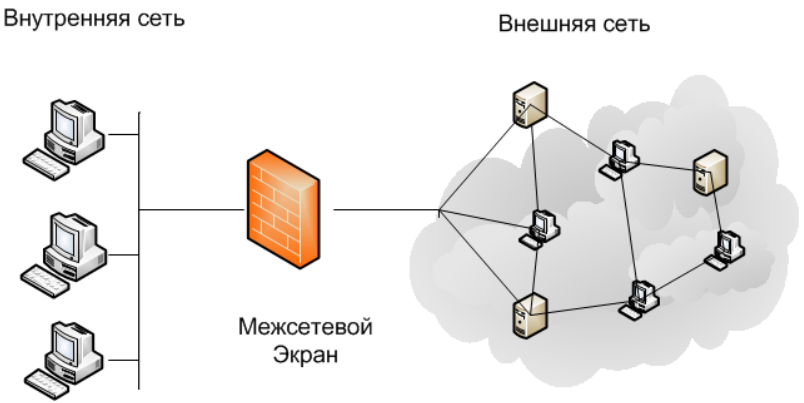
Средства обнаружения вторжений

Система обнаружения вторжений — программное или аппаратное средство, предназначенное для выявления фактов неавторизованного доступа в компьютерную систему или сеть либо несанкционированного управления ими в основном через Интернет. Системы обнаружения вторжений обеспечивают дополнительный уровень защиты компьютерных систем.

Обычно архитектура СОВ включает:

- сенсорную подсистему, предназначенную для сбора событий, связанных с безопасностью защищаемой системы
- подсистему анализа, предназначенную для выявления атак и подозрительных действий на основе данных сенсоров
- хранилище, обеспечивающее накопление первичных событий и результатов анализа
- консоль управления, позволяющая конфигурировать СОВ, наблюдать за состоянием защищаемой системы и СОВ, просматривать выявленные подсистемой анализа инциденты

Межсетевой экран (МЭ) - это локальное (однокомпонентное) или функционально - распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему и/или выходящей из информационной системы. МЭ обеспечивает защиту информационной системы посредством фильтрации информации, т.е. ее анализа по совокупности критериев и принятия решения о ее распространении на основе заданных правил.



Антивирусная программа — специализированная программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ и восстановления заражённых (модифицированных) такими программами файлов и профилактики — предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом.

Для защиты от вирусов используют три группы методов:

- Методы, основанные на *анализе содержимого файлов* (как файлов данных, так и файлов с кодами команд). К этой группе относятся сканирование сигнатур вирусов, а также проверка целостности и сканирование подозрительных команд.
- Методы, основанные на *отслеживании поведения программ* при их выполнении. Эти методы заключаются в протоколировании всех событий, угрожающих безопасности системы и происходящих либо при реальном выполнении проверяемого кода, либо при его программной эмуляции.
- Методы *регламентации порядка работы* с файлами и программами. Эти методы относятся к административным мерам обеспечения безопасности.