Информационные системы и информационная безопасность. Уязвимости беспроводных компьютерных сетей

Информационная система – совокупность программного обеспечения и технических средств, используемых для сбора, передачи, обработки, хранения и выдачи информации, с целью решения производственных задач подразделений организаций и предприятий. В организации/предприятии используются различные типы информационных систем для решения поисковых, управленческих, учетных, обучающих и других задач.

Информационные технологии – процессы, методы, алгоритмы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информационные ресурсы – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий.

Информационная безопасность – методы и способы защиты, обеспечивающие **конфиденциальность (секретность), целостность, доступность** информации.

Уязвимость систем и сетей – это слабое место в информационной системе, которое может привести к нарушению безопасности путем реализации некоторой угрозы.

Угрозы информационной безопасности

Угроза информационной безопасности — совокупность условий и факторов, создающих вероятность нарушения информационной безопасности.

Угрозы могут быть вызваны **непреднамеренными ошибками** персонала, неправильным функционированием технических средств, стихийными бедствиями или авариями (пожар, наводнение, отключение электроснабжения, нарушение телекоммуникационных каналов и т.п.), либо **преднамеренными злоумышленными действиями**, приводящими к нарушению информационных ресурсов Учреждения.

Информационные системы и информационная безопасность

УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

К основным угрозам безопасности информации и нормального функционирования информационных систем (ИС) относятся:

- утечка конфиденциальной информации;
- компрометация (разглашение) информации;
- несанкционированное использование информационных ресурсов;
- ошибочное использование информационных ресурсов;
- несанкционированный обмен информацией между абонентами;
- отказ от информации;
- нарушение информационного обслуживания;
- незаконное использование привилегий.

Уязвимости информационных систем и сетей

Уязвимость - это слабое место в информационной системе, которое может привести к нарушению безопасности путем реализации некоторой угрозы.

Причины уязвимости систем и сетей:

- **Отсутствие политики безопасности** (**Политика безопасности** – это формальное изложение правил, которым должны подчиняться лица, получающие доступ к корпоративной технологии и информации.)
- **Сложность конфигурирования.**
- **Игнорирование** разработчиками при проектировании сети Интернет **требований безопасности**.
- **Уязвимость сервисов TCP/IP.**
- **Легкость наблюдения за каналами и магистралями.**

Категории информационной безопасности

Конфиденциальность (информация доступна только тому кругу лиц, для кого она предназначена: ДСП, Секретно, Сов.секретно).

Целостность (информация получена в исходном виде).

Аутентичность (источником информации является именно то лицо, которое заявлено как ее автор).

Апеллируемость (можно будет доказать, что автором сообщения является именно заявленный человек).

Технические характеристики безопасности:

- **надежность** (вероятность того, что система ведет себя в штатном и аварийных режимах так, как заложено при ее проектировании) ;
- **контроль доступа** (гарантия того, что ограничения доступа постоянно выполняются);
- **контролируемость** (возможность проведения проверки любого компонента системы);
- **контроль идентификации** (вероятность того, что клиент, подключенный к системе, является именно тем, за кого себя выдает
- **устойчивость к умышленным сбоям** (вероятность сохранения работоспособности при внешнем воздействии).

Политика информационной безопасности

Политика информационной безопасности – комплекс взаимоувязанных руководящих принципов и разработанных на их основе правил, процедур и практических приемов, принятых в организации/предприятии для обеспечения их информационной безопасности.

Основные требования к политике информационной безопасности:

- ❖ быть реалистичной и выполнимой;
- ❖ быть краткой и понятной;
- ❖ не приводить к существенному снижению общей производительности подразделений предприятия;
- ❖ должна включать основные цели и задачи организации режима информационной безопасности;
- ❖ должна четко задавать области действия;
- ❖ указывать обязанности должностных лиц, касающиеся вопросов защиты информации.

Уровни политики безопасности

Политика безопасности охватывает следующие уровни (направления):

- политика выбора и использования паролей;
- политика допустимого использования ресурсов;
- антивирусная политика, инструкция по защите от компьютерных вирусов;
- политика установки обновлений программного обеспечения;
- политика резервного копирования, хранения и восстановления данных;
- правила работы пользователей в корпоративной сети;
- политика обеспечения безопасности удаленного доступа к ресурсам
- компьютерной сети;
- политика обеспечения безопасности при взаимодействии с сетью Интернет;
- политика безопасности периметра;
- правила предоставления доступа к ресурсам компьютерной сети;
- соглашение о соблюдении режима информационной безопасности, заключаемое со сторонними организациями; и др.

Разграничение доступа в информационных системах и сетях

Доступ к информации — ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение информации.

Уровни доступа — различаются несекретные, конфиденциальные (ДСП), **секретные** и **совершенно секретные** данные.

Объект доступа — единица информационного ресурса системы, доступ к которой регламентируется правилами разграничения доступа.

Субъект доступа — лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Правила разграничения доступа — совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Для каждого объекта существует **субъект-владелец**, который сам определяет тех, кто имеет доступ к объекту, а также разрешенные операции доступа.

Информационные системы и информационная безопасность

Ролевая модель контроля доступа в ИС

Ролевой метод управления доступом регламентирует доступ пользователей к информации на основе **типов их деятельности (активностей)** в системе (**ролей**). Под **ролью** понимается **совокупность действий и обязанностей**, связанных с определенным видом деятельности (администратор базы данных, менеджер, начальник отдела).

В ролевой модели с каждым объектом сопоставлен набор разрешенных операций доступа для каждой роли (а не для каждого пользователя). В свою очередь, каждому пользователю сопоставлены роли, которые он может выполнять. В некоторых системах пользователю разрешается выполнять несколько ролей одновременно, в других есть ограничение на одну или несколько не противоречащих друг другу ролей в каждый момент времени.

СПОСОБЫ ШИФРОВАНИЯ

Самым надежным механизмом защиты информации в компьютерных сетях является ее шифрование, т.е. использование криптографического преобразования конфиденциальных данных. При этом обеспечение защиты информации путем шифрования не должно нарушать работу сети в реальном масштабе времени, что возможно при выполнении шифрования со скоростью до 1 Гбит/с и выше.

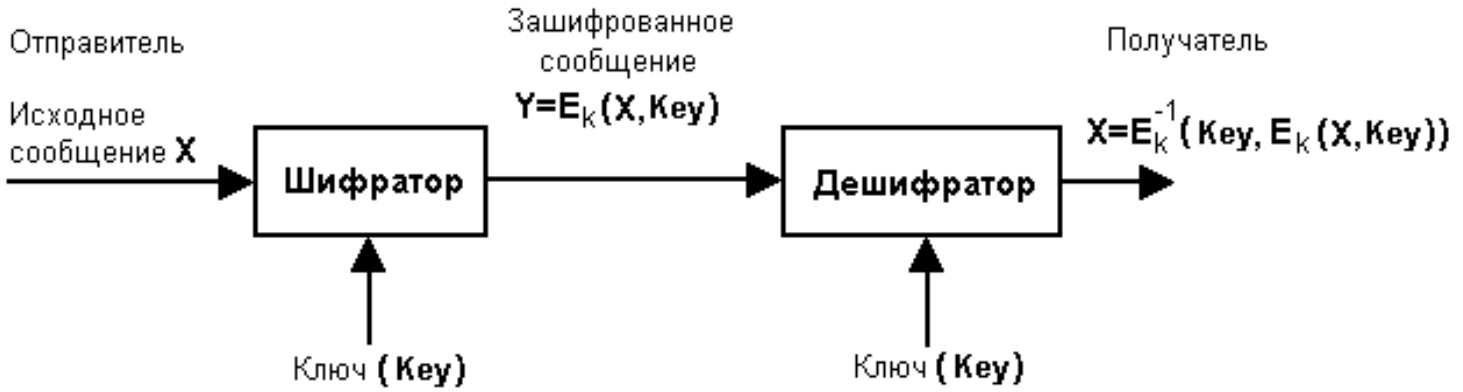
В зависимости от единицы кодирования все шифры можно разделить на две группы.

Потоковые шифры. Единицей кодирования при таком шифровании является один бит, а результат кодирования не зависит от прошедшего ранее входного потока. Схема применяется в системах передачи потоков информации, то есть в тех случаях, когда передача данных начинается и заканчивается в произвольные моменты времени и может случайно прерываться.

Блочные шифры. Единицей кодирования является блок из нескольких байтов (в настоящее время от 4-х до 32-х байтов). Результат кодирования зависит от всей совокупности байтов этого блока. Схема блочного шифрования применяется при пакетной передаче информации и кодировании файлов.

СИММЕТРИЧНЫЕ СПОСОБЫ ШИФРОВАНИЯ

В симметричных криптографических системах для шифрования и восстановления данных используется **один и тот же ключ Key.**



Все многообразие симметричных криптоалгоритмов базируется на следующих способах шифрования:

Моно- и **многоалфавитные подстановки**.

Перестановки.

Гаммирование.

СИММЕТРИЧНОЕ ШИФРОВАНИЕ

Моно- и **многоалфавитные подстановки** - Замена символов исходного текста на другие, того же алфавита, по более или менее сложному правилу.

Моноалфавитная подстановка - каждый символ исходного текста преобразуется в символ шифрованного сообщения по одному и тому же закону. При многоалфавитной подстановке **закон преобразования меняется** от символа к символу.

Перестановки. Способ шифрования заключается в перестановке местами символов исходного текста по некоторому правилу.

Гаммирование. Преобразование исходного текста, при котором символы входного текста складываются по модулю, равному мощности алфавита с символами псевдослучайной последовательности, вырабатываемой специальным генератором по определенному правилу.

СИММЕТРИЧНОЕ ШИФРОВАНИЕ

Моно- и **многоалфавитные подстановки. Шифр Цезаря.**

Гай Юлий Цезарь, римский император 100-44-й годы до н.э.

В шифре каждая буква замещается на букву, находящуюся k символами правее в алфавите по модулю, равному количеству букв в алфавите:

$$C_k(j)=(j+k)(\text{mod } n),$$

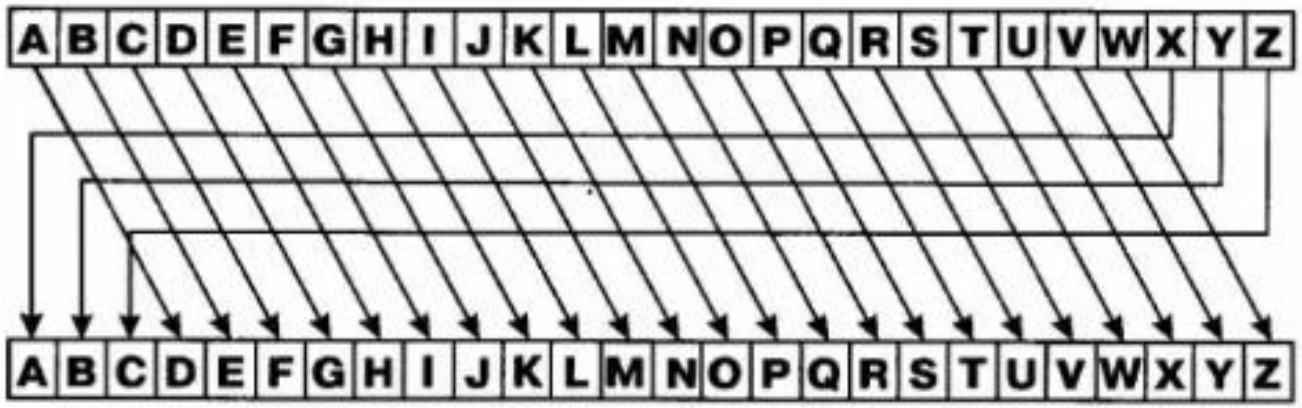
где j - порядковый номер буквы в алфавите, $C_k(j)$ – порядковый номер замещающей буквы, n – мощность входного алфавита (количество букв в используемом алфавите).

Таким образом, ключом шифрования здесь является число k, определяющее размер смещения. Дешифрование осуществляется по формуле

$$C_k^{-1}(j)=C_{n-k}=(j+n-k)(\text{mod } n)$$

СИММЕТРИЧНОЕ ШИФРОВАНИЕ.

Шифр Цезаря. Примеры шифрования.



Ключ: 3
Открытый текст:
P = HELLO CAESAR CIPHER
Зашифрованный текст:
C = KHOOR FDHVDU FLSKHU

Криптоаналитики – специалисты по дешифровке зашифрованной информации.
Криптоанализ шифра Цезаря – частотный анализ

СИММЕТРИЧНОЕ ШИФРОВАНИЕ

Квадрат Полибия

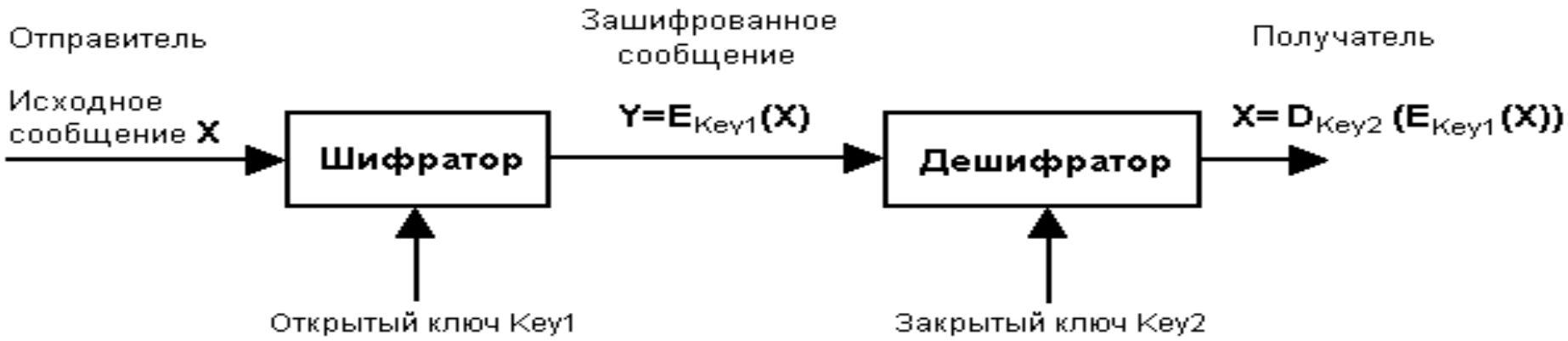
	А	Б	В	Г	Д	Е
А	А	Б	В	Г	Д	Е
Б	Ж	З	И	К	Л	М
В	Н	О	П	Р	С	Т
Г	У	Ф	Х	Ц	Ч	Ш
Д	Щ	Ъ	Ы	Ь	Э	Ю
Е	Я		.	,	-	:

Символ алфавита заменяется парой чисел или символов по определенному правилу.
Прямоугольник - доска Полибия.
Ключ: схема записи алфавита в таблицу.

представления букв В, Г, П, У будут АВ, АГ, ВВ, ГА

АСИММЕТРИЧНОЕ ШИФРОВАНИЕ

Асимметричные или двухключевые системы шифрования. Для шифрования и дешифрования данных применяются различные ключи, связанные между собой некоторой зависимостью.



Исходное сообщение **X шифруется открытым ключом Key1**, полученным от адресата. Затем это сообщение передается адресату. Зашифрованный текст **Y** в принципе не может быть расшифрован тем же открытым ключом. Дешифрование сообщения возможно только с использованием **закрытого ключа Key2**, который **известен лишь самому адресату**.

АСИММЕТРИЧНОЕ ШИФРОВАНИЕ

Открытый ключ передаётся по открытому (то есть незащищённому, доступному для наблюдения) каналу и используется для проверки электронной подписи (ЭП) и для шифрования сообщения.

Закрытый ключ расшифровки является секретным для всех — даже для отправителей сообщений.

Примерами использования асимметричных алгоритмов шифрования являются системы **RSA** (*Rivest-Shamir-Adleman*), **SSL** (*Secure Socket Layer*), **ГОСТ Р34.10-2001** и др.

АСИММЕТРИЧНОЕ ШИФРОВАНИЕ

Преимущества асимметричных шифров перед симметричными шифрами:

1) отсутствие необходимости предварительной передачи секретного ключа по надёжному каналу;

2) возможность хранения секретного ключа только на стороне получателя;

3) отсутствие необходимости частого обновления ключей;

4) меньшее число используемых ключей в больших сетях.

К **недостаткам** асимметричных систем шифрования относятся:

1) применение более длинных ключей по сравнению с симметричными системами;

2) процесс шифрования-расшифрования с использованием пары ключей проходит на два-три порядка медленнее, чем шифрование-расшифрование того же текста симметричным алгоритмом;

3) в чистом виде асимметричные криптосистемы требуют очень больших вычислительных ресурсов, поэтому на практике используются в сочетании с другими алгоритмами.

БЛОЧНОЕ ШИФРОВАНИЕ

Особенность блочных криптоалгоритмов - преобразование блока входной информации фиксированной длины в зашифрованный блок того же размера. Блочные шифры служат основой, на которой реализованы практически все криптосистемы.

Работа блочного шифра описывается двумя функциями:

Y=EnCrypt(X,Key) и X=DeCrypt(Y,Key)

Характерный признак большинства блочных алгоритмов — **многократное и косвенное** использование материала ключа и исходного блока информации. Это связано с требованием невозможности обратного декодирования при известных исходном и зашифрованном текстах.

Для решения такой задачи в приведенных выше преобразованиях чаще всего **используется не само значение ключа или его части, а некоторая, иногда необратимая, функция от материала ключа**.

Типичным представителем блочного шифрования является система **DES** (*Data Encryption Standard*), принципы построения которой определены американским стандартом криптографического закрытия данных, принятым в 1978 г.

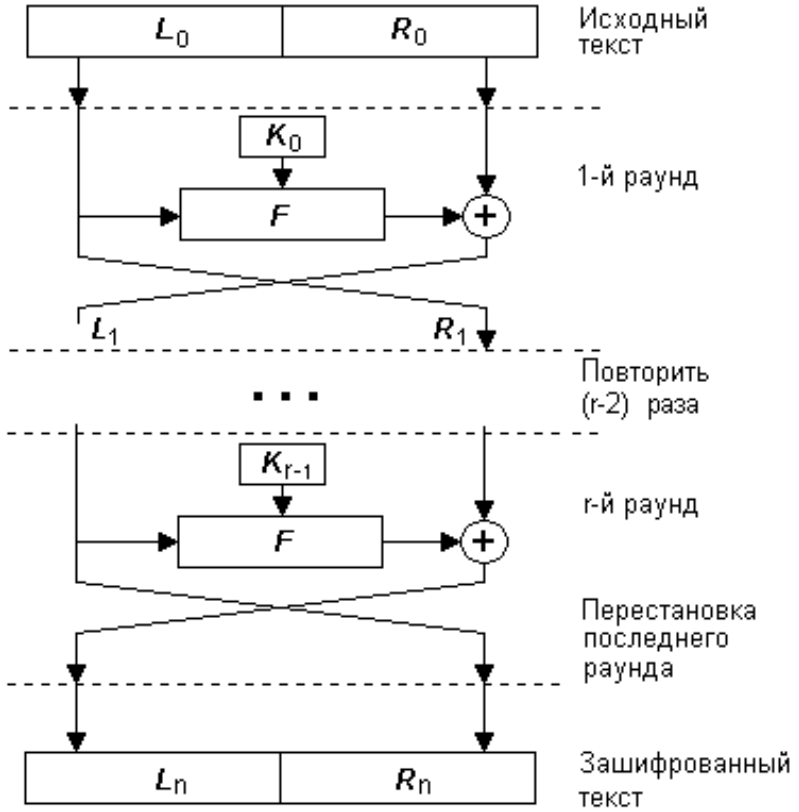
БЛОЧНОЕ ШИФРОВАНИЕ. СЕТЬ ФЕЙСТЕЛА.

1. Входной текст разбивается на блоки фиксированной длины с **четным числом символов**.
2. Выбранный блок делится на два равных подблока — «левый» (L_0) и «правый» (R_0). $L_i = R_{i-1} \oplus F(L_{i-1}, K_{i-1})$;
3. «Левый подблок» L_0 видоизменяется функцией $F(L_0, K_0)$ в зависимости от раундового ключа $\boldsymbol{K_0}$, после чего он складывается по модулю 2 с «правым подблоком» R_0.
4. Результат сложения присваивается новому левому подблоку L_1, а «левый подблок» L_0 присваивается без изменений новому правому подблоку R_1.

Операции 1-4 повторяется N_p–1 раз, при этом при переходе от одного этапа к другому меняются раундовые ключи (K_0 на K_1 и т. д.) по какому-либо математическому правилу, где N_p — количество раундов в заданном алгоритме.

Расшифровка закодированной информации происходит так же, как и шифрование, с той лишь разницей, что ключи поступают в обратном порядке, то есть не от первого к N_p-му, а от N_p-го к первому.

Одно из **преимуществ** рассмотренного способа шифрования – обратимость алгоритма независимо от используемой функции F, которая может быть сколь угодно сложной.



ПОТОКОВОЕ ШИФРОВАНИЕ

Потоковые шифры представляют собой разновидность гаммирования и преобразуют побитно открытый текст в шифрованный. Генератор ключевой последовательности выдает последовательность бит $k_1, k_2, \ldots, k_i \ldots$, которая складывается по модулю 2 (смешивается) с последовательностью битов исходного текста $x_1, x_2, \ldots, x_i, \ldots$ для получения шифрованного текста y:

$$y_i = x_i \oplus k_i .$$

На приемной стороне шифрованный текст складывается по модулю 2 с идентичной ключевой последовательностью, в результате чего получается исходный текст:

$$y_i \oplus k_i = x_i \oplus k_i \oplus k_i = x_i \ .$$

Потоковые шифры наиболее пригодны для шифрования непрерывных потоков информации, например, в сетях передачи данных.

Стойкость потоковой системы шифрования целиком зависит от внутренней структуры генератора ключевой последовательности. Чем ближе генерируемый поток по своим свойствам приближается к случайному, тем сложнее взломать шифр.

СПОСОБЫ ЗАЩИТЫ ОТ DOS И DDOS-АТАК

Действия и мероприятия по защите компьютерных сетей

Для предотвращения взлома компьютеров на начальной стадии атаки. следует выполнить следующие действия:

- ограничить использование отдельных служб;
- запретить выполнение неизвестных программ;
- установить модули обновления операционной системы и приложений;
- задать только минимально необходимые разрешения на использование каталогов и файлов.

СПОСОБЫ ЗАЩИТЫ ОТ DOS И DDOS-АТАК

Действия и мероприятия по защите компьютерных сетей

Для защиты от атак с использованием пакетов SYN целесообразно:

- *Увеличить размер очереди на установку соединений.*
- *Уменьшить период ожидания установки соединения.*
- *Регулярно использовать пакеты обновления программного обеспечения и защиты от потенциальных атак* SYN.
- *Использовать сетевые системы IDS.*
- *Использовать ОС с динамическим выделением ресурсов.*

Эффективным средством защиты является применение безопасного **протокола SSH в котором** весь передаваемый по нему трафик шифруется.

Способы борьбы с проникновением в сеть

Обнаружение нарушения безопасности сети

- На протяжении установленного промежутка времени обнаружено аномальное количество попыток аутентификации со стороны различных пользователей.
- Обнаружена аномально высокая активность в неурочное время (например, по выходным дням между 3 и 6 часами ночи).
- Зарегистрировано необычно большое количество несанкционированных попыток установки соединения с компьютерными системами.

Поведенческие методы обнаружения атак реализуются либо на основе анализа статистических параметров, либо при помощи нейросетей или экспертных систем.

ОБНАРУЖЕНИЕ ВТОРЖЕНИЙ НА ОСНОВЕ СИГНАТУРНОГО АНАЛИЗА

Сценарий вторжения - последовательность действий (*поведений*), описывающих атаку.

При использовании сигнатурных методов каждой разновидности атаки ставится в соответствие некий шаблон – ***сигнатура***.

В качестве сигнатуры могут применяться **строка символов**, **семантическое выражение** на специальном языке, **формальная математическая модель** и т. д.

Ряд разновидностей реализаций сигнатурных методов обнаружения атак:

- **метод анализа состояний** – сигнатура в виде последовательности переходов компьютерной системы из одного состояния в другое ;
- на основе экспертных систем;
- с использованием биологических моделей – **генетический** и **нейросетевой**.

ПРИМЕРЫ СИГНАТУР АТАК

Сигнатур атак, используемых при анализе трафика (заголовков сетевых пакетов):

1) В заголовке TCP пакета установлен **порт назначения 139** (вызывает зависание системы) и **флаг OOB** (Out of Band). Это является признаком атаки для WinNuke.

2) Установлены одновременно противоречащие друг другу флаги TCP пакета: **SYN и FIN**. Данная комбинация флагов используется во многих атакующих программах для обхода фильтров и мониторов, проверяющих только установку одиночного SYN флага.

3) Пример сигнатуры атаки, используемой при анализе контента:
"**GET . cgi-bin ./etc/passwd**". Наличие данной строки в области данных HTTP-пакета свидетельствует об использовании эксплойтов типа **phf, php** или **aglimpse**.

Недостатки сигнатурного анализа

- Невозможность обнаружения атак, сигнатуры которых пока не определены.
- Сложность обновления базы данных сигнатур в виду отсутствия общепринятого языка описания; добавление собственных сигнатур требует высокой квалификации.
- Необходимость затрат значительных временных ресурсов для обновления базы данных сигнатур при обнаружении нового типа атак.

Системы обнаружения вторжений (СОВ)

IDS (*Intrusion Detection Systems*).

Различают пассивные и активные IDS. ***Пассивные*** просто фиксируют факт атаки, записывают данные в файл журнала регистрации и выдают предупреждения. ***Активные*** *IDS* не только определяют, но и пытаются остановить атаку, а также могут провести ответное нападение на атакующего.

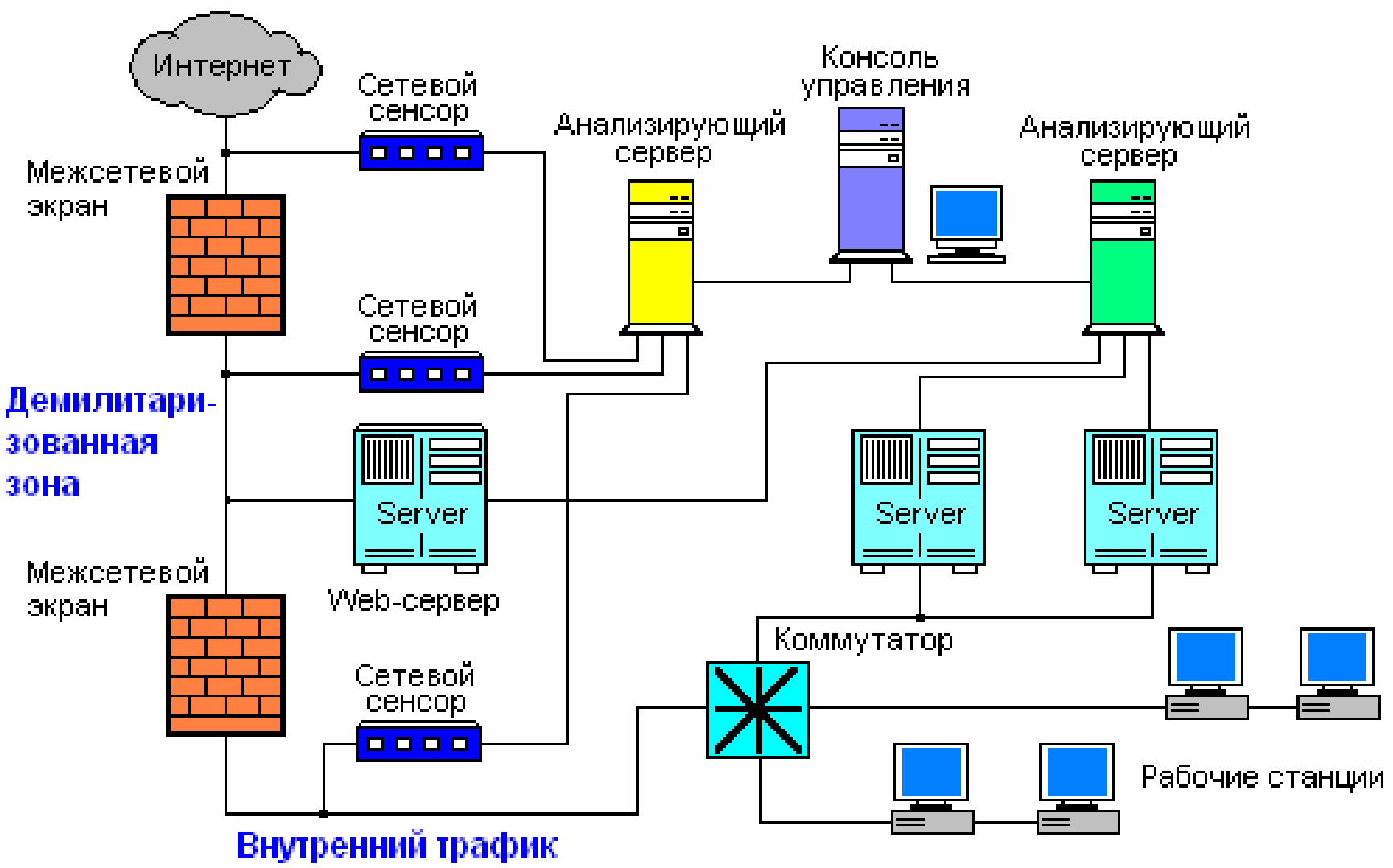
По способу выявления атаки: СОВ, основанные на **сигнатурах** либо на выявлении **аномалий**.

По уровню сбора информации об атаке: обнаружение на сетевом уровне, на рабочей станции и на уровне приложения.

По виду анализируемых файлов: **системы контроля целостности** файлов и **мониторы регистрационных файлов**.

Первые проверяют системные файлы с целью определения момента внесения в них изменений. **Мониторы регистрационных файлов** контролируют регистрационные файлы, создаваемые сетевыми сервисами и службами.

Системы обнаружения вторжений (СОВ)



Способы борьбы с проникновением в сеть

Демилитаризованная зона - DMZ

DMZ — технология обеспечения защиты информационного периметра, при которой серверы, отвечающие на запросы из внешней сети, или направляющие туда запросы, находятся в особом сегменте сети (который и называется DMZ).

Основное назначение DMZ — минимизировать последствия взлома сети, при этом взломщик получает (полный или частичный) контроль над серверами DMZ, но не имеет доступа к внутренним серверам или рабочим станциям.

Ключевая особенность DMZ — не только фильтрация трафика на внутреннем брандмауэре, но и требование обязательной мощной криптографии при взаимодействии между активным оборудованием внутренней сети и DMZ.