Тема 5

Методы защиты информации на физическом уровне

Содержание темы

- Классификация методов защиты информации.
- Методы защиты информации на физическом уровне модели OSI.
- Модели информационной безопасности.
- Триада «Конфиденциальность, доступность, целостность».
- Гексада Паркера.
- Модель STRIDE.
- Особенности беспроводной среды передачи.
- Множественный доступ с кодовым разделением каналов (CDMA).

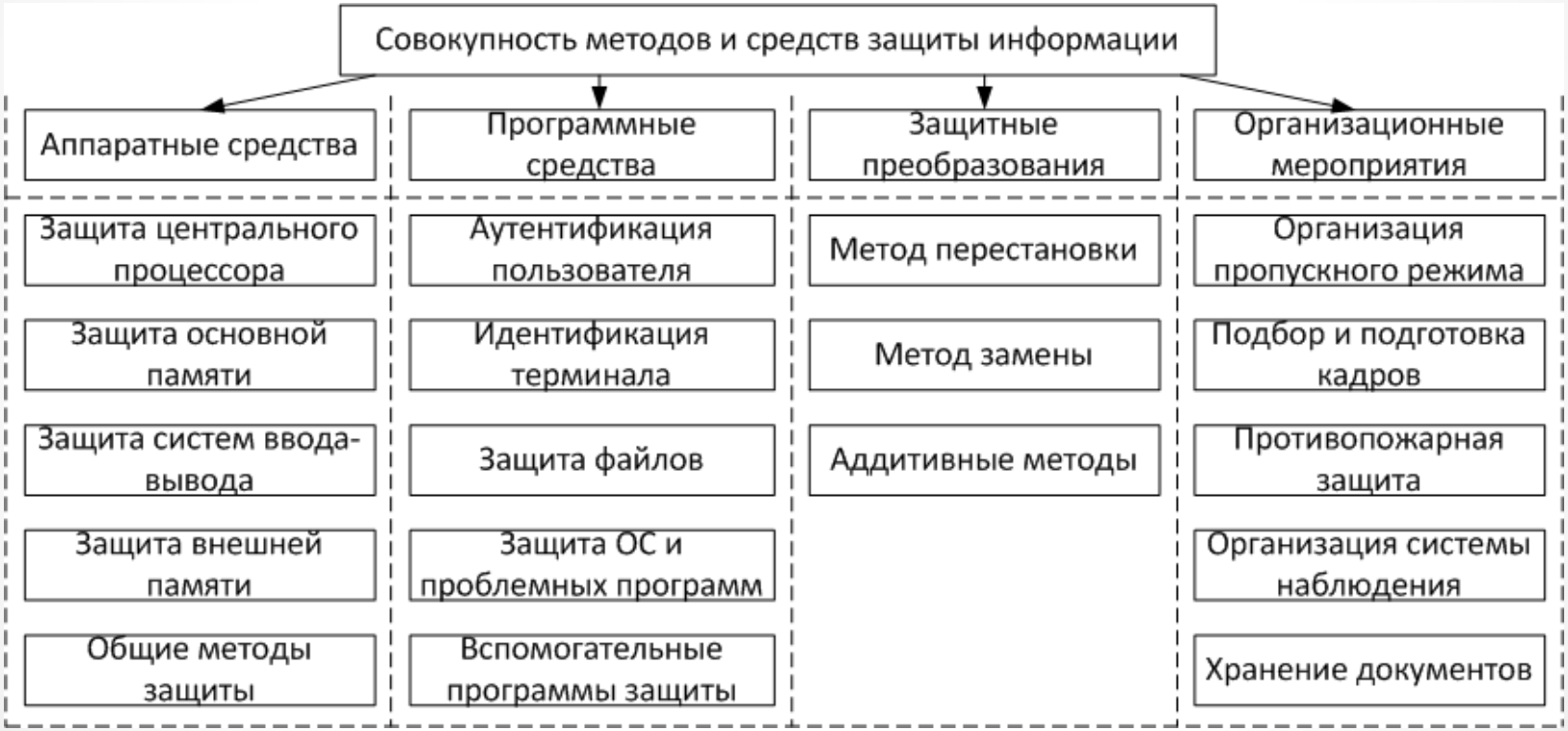
Классификация методов защиты информации

Методы и средства защиты информации являются технической основой системы защиты информации.

Совокупность защитных методов и средств включает в себя:

- программные методы;
- аппаратные средства;
- защитные преобразования;
- организационные мероприятия.

Классификация методов защиты информации



Аппаратные методы ЗИ

Сущность **аппаратной** или **схемной защиты** состоит в том, что в устройствах и технических средствах обработки информации предусматривается наличие специальных технических решений, обеспечивающих защиту и контроль информации.

К аппаратным методам защиты информации относятся:

- электронный замок;
- электро-магнитный экран и т. п.

Программные методы ЗИ

Программные методы защиты – это совокупность алгоритмов и программ, обеспечивающих разграничение доступа и исключение несанкционированного использования информации.

К программным методам защиты информации относятся:

- антивирусная программа;
- программный брандмауэр и т. п.

Методы защитных преобразований

Сущность **методов защитных преобразований** состоит в том, что информация, хранимая в системе и передаваемая по каналам связи, представляется в некотором коде, исключающем возможность ее непосредственного использования.

К методам защитных преобразований относятся:

- методы замены;
- методы перестановки и т. п.

Организационные мероприятия по ЗИ

Организационные мероприятия по защите включают в себя совокупность действий по подбору и проверке персонала, строгое регламентирование процесса разработки и функционирования информационной системы.

К организационным мероприятиям по защите информации относятся:

- организация пропускного режима в здание;
- система видеонаблюдения и т. п.

Классификация методов защиты информации

Методы защиты на физическом уровне

Основные угрозы на физическом уровне – это:

- **физический доступ к носителям информации**;
- **угроза оборудованию**;
- **Угроза кабельной системе**;
- **возможность съема информации за счет различного рода излучений, электромагнитных наводок**;
- и т. п.

Методы защиты на физическом уровне

Уровни защиты:

- защита территории;
- доступа к оборудованию и носителям;
- защита кабельной системы;
- электроснабжения;
- средства архивирования.

Методы защиты на физическом уровне

Защита помещения и аппаратуры осуществляется с помощью охранных систем: систем датчиков и сбора сигналов.

Датчики:

- традиционные (на замыкание-размыкание);
- ультразвуковые;
- прерывание луча;
- телевизионные;
- радиолокационные;
- микроволновые;
- пневматические;
- магнитные.

Методы защиты на физическом уровне

Утечка информации по техническим каналам:

- **электромагнитный высокочастотный прямой канал** – излучение системных блоков, дисплеев, линий связи;
- **электромагнитный низкочастотный прямой канал** – поля с сильной магнитной составляющей (катушки, трансформаторы);
- **электромагнитный косвенный канал** – наводки на металлические проводящие предметы;
- наводки на шины заземления;
- акустический канал;
- акусто-электрический канал – преобразование звуковых сигналов в электрические.

Методы защиты на физическом уровне

Средства защиты: активные и пассивные

Пассивные – локализация излучений и развязывание информационных сигналов.

- **Локализация**: экранирование и заземление средств вычислительной техники, звукоизоляция помещений.
- **Развязывание**: установка специальных устройств, электрических вставок.

Активные – пространственные зашумления:

- электромагнитные зашумления или создание прицельных помех;
- уничтожение закладных устройств.

Модели информационной безопасности

Информационная безопасность - это процесс обеспечения конфиденциальности, доступности, целостности и информации.

Триада «**конфиденциальность**, **доступность**, **целостность**» только одна из существующих моделей информационной безопасности.

Эта популярная до сих пор модель была предложена Джери Зальцером и Майком Шредером в 1975 году.

Модели информационной безопасности

Обеспечение конфиденциальности

Служба конфиденциальности обеспечивает секретность информации. Правильно сконфигурированная, эта служба открывает доступ к информации только аутентифицированным пользователям.

Служба конфиденциальности должна учитывать различные способы представления информации – в виде распечаток, файлов или пакетов, передающихся по сетям.

Механизмы обеспечения конфиденциальности	Контроль физической безопасности
	Контроль доступа к файлам на компьютере
	Шифрование файлов
Требования к конфиденциальности файлов	Идентификация и аутентификация
	Правильная настройка компьютерной системы
	Правильное управление ключами при использовании шифрования

Обеспечение доступности

Служба обеспечения доступности информации поддерживает ее готовность к работе, позволяет обращаться к компьютерным системам, хранящимся в этих системах данным и приложениям.

Для сохранения важной информации самым простым способом является создание ее резервных копий и размещение их в безопасном месте.

Обеспечение целостности

Служба обеспечения целостности следит за правильностью информации.

При должном уровне организации эта служба дает пользователям уверенность в том, что информация является верной, и ее не изменил никто из посторонних.

Способы защиты бумажных документов от подделки: подпись на каждой странице, подшивка документов в папки, изготовление нескольких копий документа.

Основным способом защиты целостности электронных документов или файлов является контроль над доступом к ним на компьютере.

Модели информационной безопасности

Гексада Паркера – одна из наиболее известных альтернатив триаде КДЦ. Она появилась в 1998 году.

Аутентичность – это состояние системы, при котором пользователь не может выдать себя за другого, а документ всегда имеет достоверную информацию об его источнике.

Владение – это состояние системы, при котором физический контроль над устройством или другой средой хранения информации предоставляется только тем, кто имеет на это право.

Полезность – это такое состояние информационной системы, при котором обеспечивается удобство практического использования информации и связанных с ней процедур.

Модели информационной безопасности

Модели информационной безопасности

Модель STRIDE – альтернатива триаде КДЦ и гексаде Паркера. Она используется компанией Microsoft для разработки безопасного программного обеспечения.

В соответствии с этой моделью информационная система находится в безопасности, если она защищена от следующих видов нарушений информационной безопасности:

Spuffing	Подмена данных
Tampering	Изменение данных
Repudiation	Отказ в ответственности
Information Disclosure	Разглашение сведений
Denial of Service	Отказ в обслуживании
Elevation of Privilege	Захват привилегий

Беспроводная среда передачи

Отказ от проводов и обретение мобильности приводит к высокому уровню помех в беспроводных линиях связи.

Если интенсивность битовых ошибок (BER) в проводных линиях связи равна 10^{-9}-10^{-10}, то в беспроводных линиях связи она достигает величины 10^{-3}.

Методы повышения качества радиосигналов

Техника расширенного спектра разработана специально для беспроводной передачи. Она позволяет повысить помехоустойчивость кода для сигналов малой мощности, что очень важно в мобильных приложениях.

Выделяют следующие методы расширения спектра сигнала:

- **расширение спектра скачкообразной перестройкой частоты** (**Frequency Hopping Spread Spectrum**, **FHSS**);
- **прямого последовательного расширения спектра** (**Direct Sequence Spread Spectrum**, **DSSS**).

Совместно с FHSS и DSSS может использоваться метод **множественного доступа с кодовым разделением** (**Code Division Multiplexing Access**, **CDMA**).

FHSS

Идея метода **расширения спектра скачкообразной перестройкой частоты** (**Frequency Hopping Spread Spectrum**, **FHSS**) возникла во время Второй мировой войны, когда радио широко использовалось для секретных переговоров и управления военными объектами.

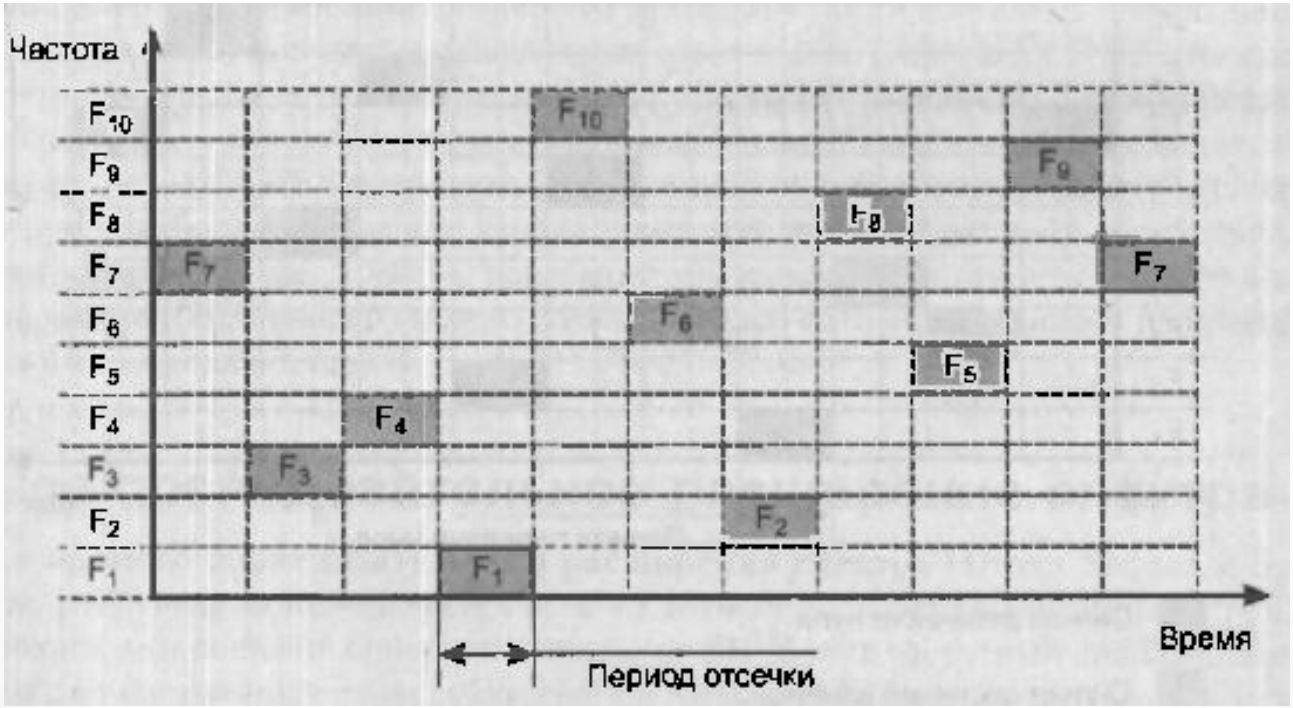
Для того чтобы радиообмен нельзя было перехватить или подавить узкополосным шумом, было предложено вести передачу с **постоянной сменой несущей** в пределах **широкого диапазона частот**.

В результате мощность сигнала распределялась по всему диапазону, и прослушивание какой-то определенной частоты давало только небольшой шум.

FHSS

Последовательность перестройки частот:

$$F_7 - F_3 - F_4 - F_1 - F_{10} - F_6 - F_2 - F_8 - F_5 - F_9$$



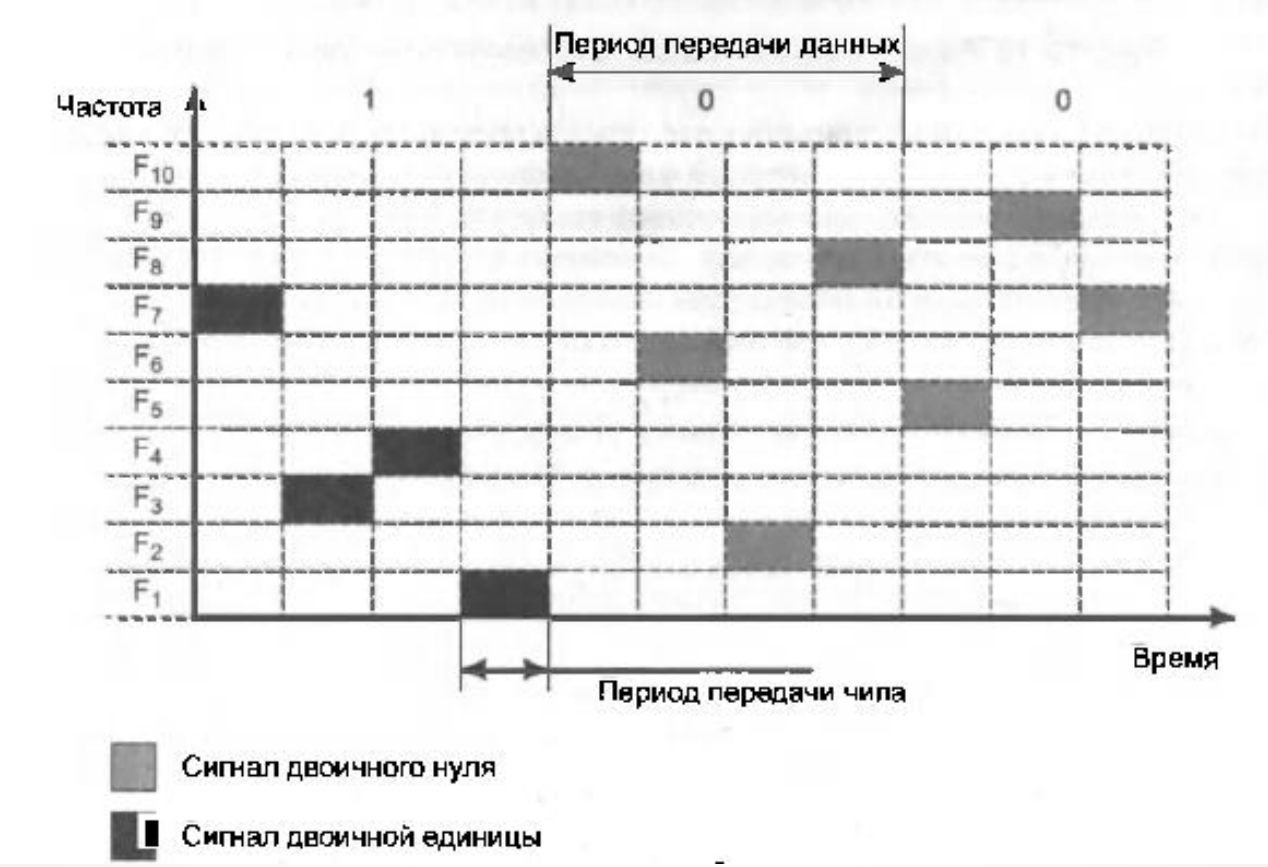
Методы FHSS применяют в беспроводных технологиях IEEE 802.11 и Bluetooth.

FHSS

Медленное расширение спектра (частота смены подканалов **ниже**, чем скорость передачи данных в канале)

FHSS

Быстрое расширение спектра (частота смены подканалов **выше**, чем скорость передачи данных в канале)



DSSS

В методе **прямого последовательного расширения спектра** (**Direct Sequence Spread Spectrum**, **DSSS**) также используется весь частотный диапазон, выделенный для одной беспроводной линии связи.

Однако в отличие от FHSS весь частотный диапазон занимается не за счет постоянных переключений с частоты на частоту, а за счет того, что каждый **бит информации** заменяется ***N* битами**, поэтому тактовая скорость передачи сигналов увеличивается в ***N* раз**.

А это, в свою очередь, означает, что спектр сигнала также расширяется в ***N* раз**.

DSSS

Цель кодирования методом **DSSS** та же, что методом **FHSS** - **повышение помехоустойчивости**.

Узкополосная помеха будет искажать только **определенные частоты спектра сигнала**, так что приемник с **большой степенью вероятности** сможет правильно распознать передаваемую информацию.

DSSS

Код, которым заменяется двоичная единица исходной информации, называется **расширяющей последовательностью**, а каждый бит такой последовательности - **чипом**.

Соответственно, скорость передачи результирующего кода называют **чиповой скоростью**.

Двоичный нуль кодируется **инверсным значением расширяющей последовательности**.

Примером расширяющей последовательности является ***последовательность Баркера***, которая состоим из 11 бит:

10110111000.

Последовательность Баркера

1 – 10110111000;
0 – 01001000111.

110 – 10110111000 10110111000 01001000111;
111 – 10110111000 10110111000 10110111000;
000 – 01001000111 01001000111 01001000111.

Последовательность Баркера позволяет приемнику **быстро синхронизироваться с передатчиком**, то есть надежно выявлять начало последовательности.

CDMA

Кодирование методом **DSSS** позволяет мультиплексировать несколько каналов в одном диапазоне.

Техника такого мультиплексирования называется **множественным доступом с кодовым разделением** (**Code Division Multiplexing Access**, **CDMA**).

CDMA широко используется в сотовых сетях.

CDMA

В **CDMA** каждая станция может при передаче все время пользоваться **полным спектром частот**.

В **CDMA** применения теории кодирования (**коды Уолша**), что делает его **более терпимым к помехам**, а также позволяет нескольким сигналам от различных пользователей **совместно** использовать общий диапазон частот.

В CDMA каждый битовый интервал разбивается на ***m*** коротких периодов (чипов). Обычно в битовом интервале помещаются 64 или 128 элементарных сигналов.

Каждой станции соответствует уникальный *m*-битный код, называющийся **элементарной последовательностью**.

CDMA

Например, если $m = 8$ и если станции A соответствует последовательность:

$$(-1\ -1\ -1\ +1\ +1\ -1\ +1\ +1),$$

то она может послать бит «1», передав элементарную последовательность:

$$(-1\ -1\ -1\ +1\ +1\ -1\ +1\ +1),$$

а бит «0», передав:

$$(+1\ +1\ +1\ -1\ -1\ +1\ -1\ -1),$$

Здесь +1 и -1 - сигналы с такими уровнями напряжения.

CDMA

Чтобы увеличить количество информации, которое необходимо передавать (чтобы скорость составила ***b*** бит/с, нужно отправлять ***m×b*** элементарных сигналов в секунду), необходимо увеличить в ***m*** раз пропускную способность канала связи.

Таким образом, для CDMA нужна в ***m* раз большая пропускная способность**, чем для станции не применяющей CDMA, если никаких изменений в методах модуляции и кодирования не производится.

CDMA

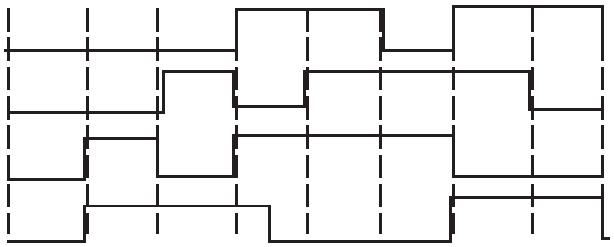
$A = (-1\ -1\ -1\ +1\ +1\ -1\ +1\ +1)$

$B = (-1\ -1\ +1\ -1\ +1\ +1\ +1\ -1)$

$C = (-1\ +1\ -1\ +1\ +1\ +1\ -1\ -1)$

$D = (-1\ +1\ -1\ -1\ -1\ -1\ +1\ -1)$

а



б

$S_1 = C = (-1\ +1\ -1\ +1\ +1\ +1\ -1\ -1)$

$S_2 = B+C = (-2\ \ 0\ \ 0\ \ 0\ +2\ +2\ \ 0\ -2)$

$S_3 = A+\overline{B} = (\ 0\ \ 0\ -2\ +2\ \ 0\ -2\ \ 0\ +2)$

$S_4 = A+\overline{B}+C = (-1\ +1\ -3\ +3\ +1\ -1\ -1\ +1)$

$S_5 = A+B+\overline{C}+D = (-4\ \ 0\ -2\ \ 0\ +2\ \ 0\ +2\ -2)$

$S_6 = A+B+\overline{C}+D = (-2\ -2\ \ 0\ -2\ \ 0\ -2\ +4\ \ 0)$

в

$S_1 \bullet C = [1+1-1+1+1+1-1-1]/8 = 1$

$S_2 \bullet C = [2+0+0+0+2+2+0+2]/8 = 1$

$S_3 \bullet C = [0+0+2+2+0-2+0-2]/8 = 0$

$S_4 \bullet C = [1+1+3+3+1-1+1-1]/8 = 1$

$S_5 \bullet C = [4+0+2+0+2+0-2+2]/8 = 1$

$S_6 \bullet C = [2-2+0-2+0-2-4+0]/8 = -1$

г

Последовательности CDMA

а) - двоичные элементарные последовательности для четырех станций; *б)* - биполярные элементарные двоичные последовательности; *в)* - шесть примеров передачи; *г)* - восстановление сигнала станции С.

CDMA

Когда две или более станции пытаются осуществить одновременную передачу, их биполярные сигналы линейно складываются.

$$A = (-1\ -1\ -1\ +1\ +1\ -1\ +1\ +1)$$
$$B = (-1\ -1\ +1\ -1\ +1\ +1\ +1\ -1)$$
$$C = (-1\ +1\ -1\ +1\ +1\ +1\ -1\ -1)$$
$$D = (-1\ +1\ -1\ -1\ -1\ -1\ +1\ -1)$$

Например, если при передаче одного элементарного сигнала три станции послали +1, а одна послала -1, то в результате получится +2. Можно рассматривать это как сложение напряжений: три станции имеют на выходе +1 В, а одна имеет на выходе -1 В. В результате сложения получаем +2 В.

Все элементарные последовательности должны быть попарно **ортогональны**.

$$S_1 = C = (-1\ +1\ -1\ +1\ +1\ +1\ -1\ -1)$$
$$S_2 = B+C = (-2\ \ 0\ \ 0\ \ 0\ +2\ +2\ \ 0\ -2)$$
$$S_3 = A+\overline{B} = (\ 0\ \ 0\ -2\ +2\ \ 0\ -2\ \ 0\ +2)$$
$$S_4 = A+\overline{B}+C = (-1\ +1\ -3\ +3\ +1\ -1\ -1\ +1)$$
$$S_5 = A+B+\overline{C}+D = (-4\ \ 0\ -2\ \ 0\ +2\ \ 0\ +2\ -2)$$
$$S_6 = A+B+\overline{C}+D = (-2\ -2\ \ 0\ -2\ \ 0\ -2\ +4\ \ 0)$$

CDMA

Чтобы восстановить исходный битовый поток каждой из станций, приемник должен заранее знать элементарные последовательности всех передатчиков, с которыми он работает.

$$A = (-1\ -1\ -1\ +1\ +1\ -1\ +1\ +1)$$
$$B = (-1\ -1\ +1\ -1\ +1\ +1\ +1\ -1)$$
$$C = (-1\ +1\ -1\ +1\ +1\ +1\ -1\ -1)$$
$$D = (-1\ +1\ -1\ -1\ -1\ -1\ +1\ -1)$$

Восстановление осуществляется путем вычисления нормированного скалярного произведения принятой последовательности (то есть линейной суммы сигналов всех станций) и элементарной последовательности той станции, чей исходный сигнал восстанавливается.

$$S_1 \bullet C = [1+1-1+1+1+1-1-1]/8 = 1$$
$$S_2 \bullet C = [2+0+0+0+2+2+0+2]/8 = 1$$
$$S_3 \bullet C = [0+0+2+2+0-2+0-2]/8 = 0$$
$$S_4 \bullet C = [1+1+3+3+1-1+1-1]/8 = 1$$
$$S_5 \bullet C = [4+0+2+0+2+0-2+2]/8 = 1$$
$$S_6 \bullet C = [2-2+0-2+0-2-4+0]/8 = -1$$