УДК 681.3.067

ОДИН ИЗ АСПЕКТОВ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ В ТЕЛЕКОМУНИКАЦИОННЫХ СИСТЕМАХ

Олег Степанов

Военный институт Национального технического университета Украины «КПИ»

Анотація: **Стаття присвячена розробці методу захисту інформації шляхом сполучення персональної електронно-обчислювальної машини з існуючою спецапаратурою лінійного шифрування.**

Summary: **The article is devoted to development a method of a protection of information, by reciprocation of the personal computer to existing special instrumentation of linear encoding.**

Ключові слова: інформаційна безпека, канал засекреченого зв`язку.

Важность проблемы информационной безопасности сейчас уже очевидна для всех. Даже небольшого размышления достаточно, чтобы понять её проблемы, сложность, проистекающую как из сложности и разновидности современных информационных систем, так и из необходимости комплексного подхода к безопасности с привлечением законодательных, административных и програмно-технических мер.

Информационной безопасностью занимаются давно. Первоначально это было прерогативой государственных организаций, имеющих дело с секретной информацией или отвечающих за обеспечение режима секретности (армия, служба безопасности и т.п.), для защиты военных, государственных и дипломатических тайн при помощи шифров. Поэтому, и люди, и методы, которые они разрабатывали и применяли, были очень специфическими, секретными, громоздкими, а потому и недоступными обыкновенному пользователю.

В настоящее время наблюдается всплеск интереса к информационной безопасности, который объясняется, в первую очередь, широким использованием электронно вычислительной техники в армии, промышленности, управлении, связи, научных исследованиях, в комерческой и банковской сфере. Компьютерная техника во многом вытеснила средства связи, прежде всего удобством пользования, возможностью разработки документов любого вида и передачи инфомации по каналам связи.

Всё это привело к тому, что пявилось очень много различных несертифицированных програмных продуктов, програмно-аппаратных средств защиты информации, которыми могут пользваться все, кроме государственных структур и, в частности, Вооружённых сил.

Поэтому, исходя из всего вышесказанного я считаю необходимым, предложить несколько методов обьединения персональной электро-вычислительной машины (ПЭВМ) с каналом засекреченной связи гарантированной стойкости, который бы обеспечил безопасность информации при передаче её между ПЭВМ, расположенными на значительном удалении друг от друга.

Прежде чем перейти к изложению вариантов сопряжения ПЭВМ с каналом засекреченой связи, рассмотрим тракт прохождения сигнала в этой системе.

Для упрощения, покажем только половину тракта, вторая половина аналогична первой.

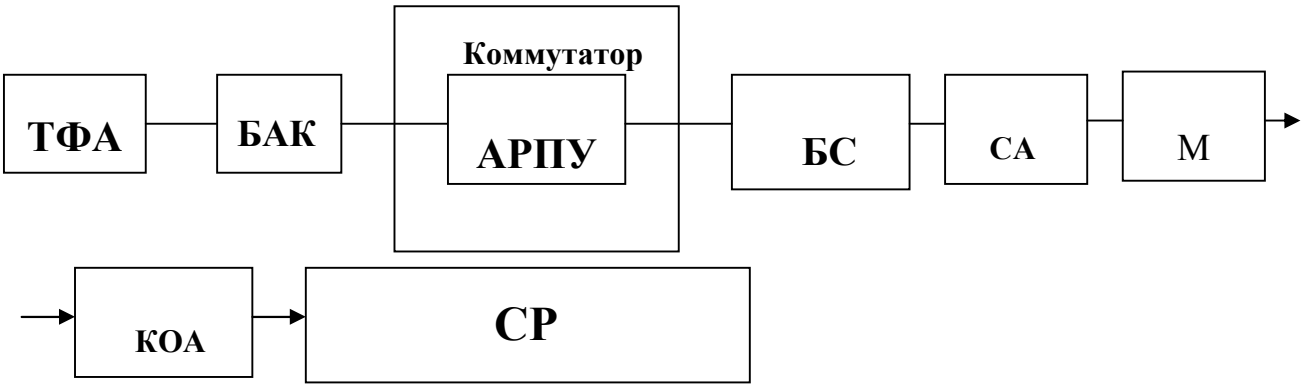

Рисунок 1 - Схема соединения телефонного аппарата с засекреченым каналом связи

На рисунке 1 обозначено: АРПУ – автоматическое распределительное устройство, БАК – блок абонентской комутации, БС – блок сопряжения, СА – спец аппаратура, КОА – канало-образующее устройство, ТФА – телефонный аппарат, М – модем, СР – среда распространения.

Исследуя тактико-технические характеристики (ТТХ) АРПУ и модема можно сделать вывод о том, что и АРПУ и модем имеют одинаковые скорости работы, рабочий диапазон частот, входное и выходное сопротивления. И самое главное то, что гребёнка полосовых фильтов анализатора АРПУ, перекрывает полосу частот, с какой модем работает в линию.

Поэтому, подключив модем паралельно телефонному апарату, можно предположить, что анализатор АРПУ, сигналы, поступающие от модема, будет воспринимать как речь, а следовательно и преобразовывать эти сигналы как речевые, к виду, удобному для засекречивания. Тогда схема сопряжения ПЭВМ с каналом засекреченой связи будет иметь вид:

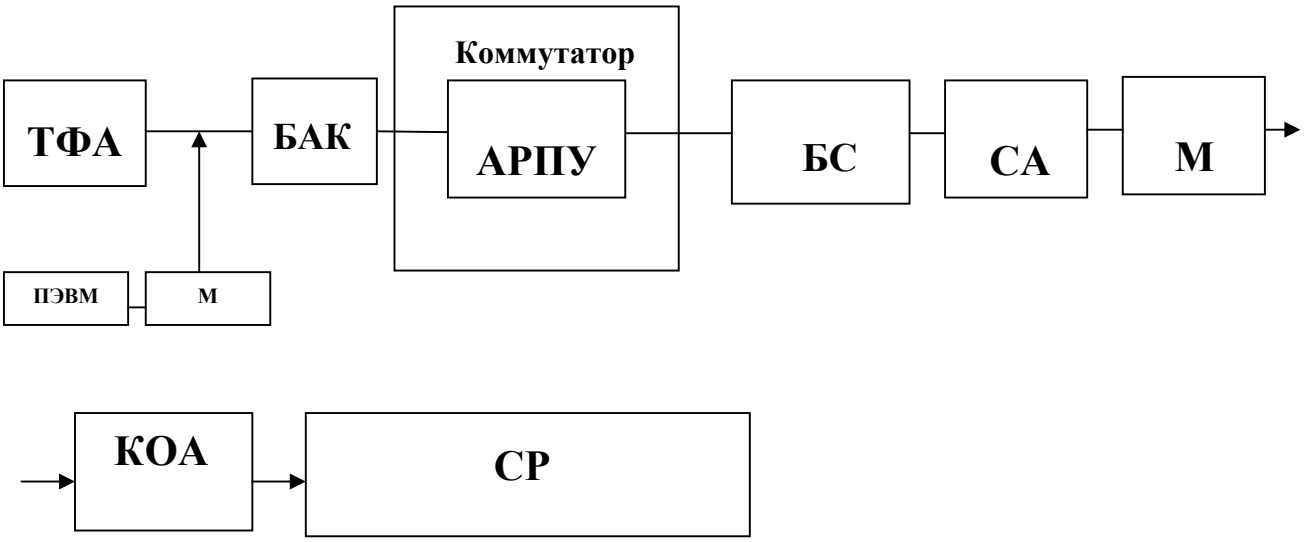

Рисунок 2 - Схема сопряжения ПЭВМ через модем с каналом засекреченой связи

Достоинством такого подключения ПЭВМ к сети засекреченой связи есть то, что:

1. Реализация даного метода не требует никаких дополнительных затрат материальных средств, обучения обслуживающего персонала.
2. Любой из абонентов сети засекреченной связи может произвести обмен информацией с любым абонентом сети засекреченой связи, имеющим аналогичный модем.

Недостатком этого метода можно считать то, что:

1. Телефонистка, обслуживающая коммутатор, должна будет сделать переключение режима работы блока шнуровых комплектов, из режима “4пр” в режим “4\2пр”. Это связано с тем, что модем имеет 2-х проводное окончание а канал засекреченной связи 4-х проводное.
2. Модем должен передавать информацию, используя только частотную модуляцию сигнала.

Анализируя недостатки этого метода сопряжения ПЭВМ с каналом засекреченной связи, можно сделать вывод о том, что эти недостатки можно устранить, если заменить модем в схеме на рис.2 на устройство сопряжения (УС) ПЭВМ с АРПУ.

УС соединяется с ПЭВМ через последоватьльный порт COM 2 и имеет 4-х проводный выход.

Структурная схема данного УС представлена на рисунке 3. На этом рисунке обозначено:

Вх Ус - входной усилитель, ПФ - полосовой фильтр, Исх Ус – исходящий усилитель, Г – генератор, ОУ операционный усилитель, Л1 – приёмная линия, Л2 – передающая линия, ЭИ – элемент индикации, ОУ – устройство управления, ТР – трансформатор.

Сигналы COM порта RS – 232: RX, DTR, RTS, GMD, TxD, DSR, CTS, DSD.

Запитывать данное устройство можно с линии, при этом необходимо использовать преобразователь напряжения. Подключается данное устройство паралельно к телефонному аппарату засекреченной связи в 4-х проводном режиме. В остальном схема включения УС и взаимодействия с остальными элементами тракта такая же, как представлена на рисунке 2, только вместо модема будет использоваться устройство сопряжения.

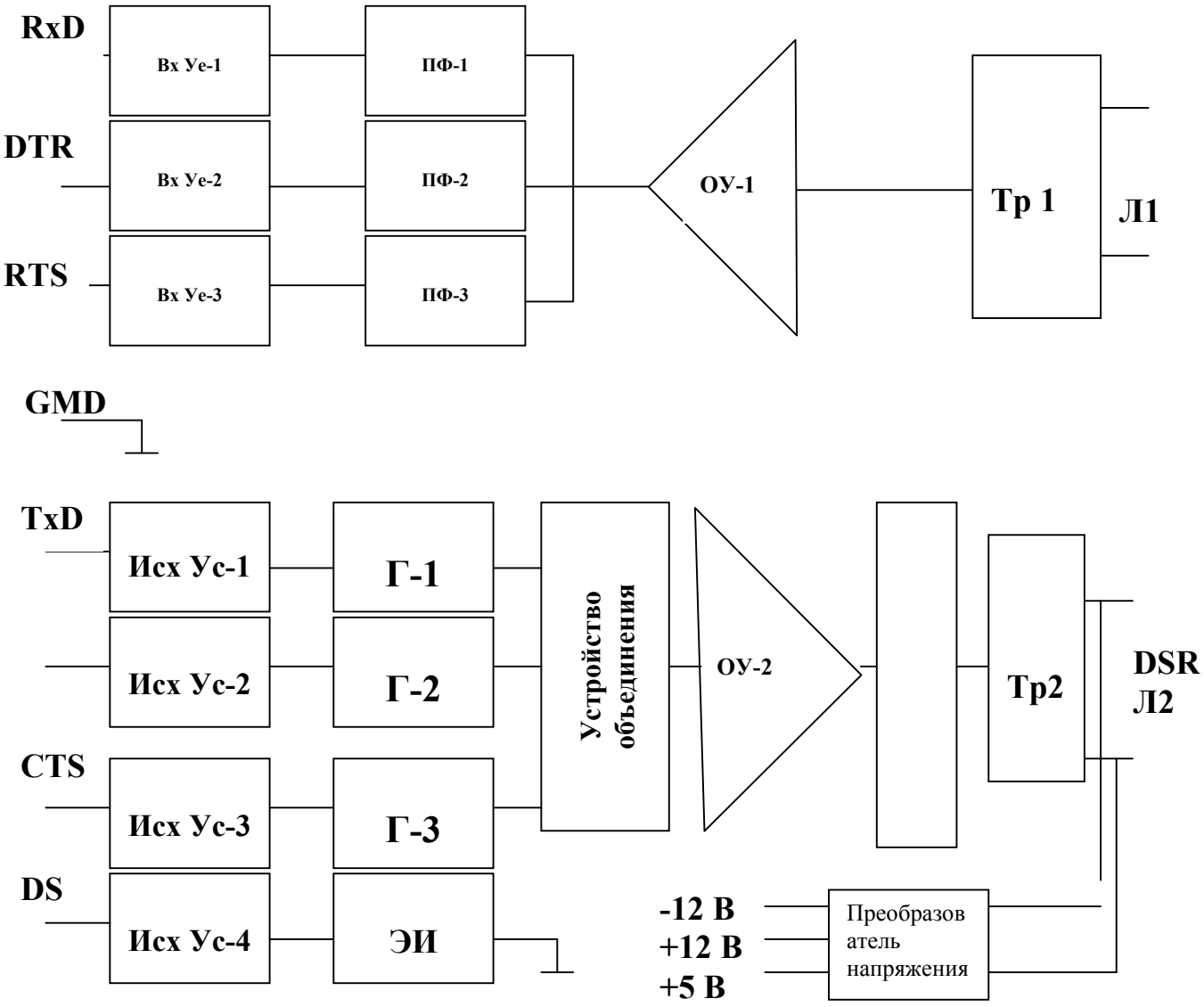

Рисунок 3 - Структурная схема устройства сопряжения ПЭВМ с каналом засекреченой связи

Всё вышеизложенное даёт возможность сделать вывод о том, что на данном этапе целесообразно рекомендовать использование этого метода сопряжения ПЭВМ с аппаратурой гарантированного линейного засекречивания для обеспечения безопасности передачи информации с помощью ПЭВМ в Вооружённых силах Украины. Большое количество преобразований выходного сигнала ПЭВМ компенсируется простотой реализации данного метода, и минимальными затратами.