УДК004.056.53

**Джурунтаев Д.З,**
*Д.т.н., профессор Казахского национального технического исследовательского университета имени К.И. Сатпаева г. Алматы, Республика Казахстан*
**Амиргалиев Е.Н.,**
*Д.т.н., профессор Университет имени Сулеймана Демиреля*
**Заурбек А.**
*Казахский национальный технический исследовательский университет имени К.И. Сатпаева*

# ЗАЩИТА РЕЧЕВОЙ ИНФОРМАЦИИ ОТ СКРЫТОЙ ЗВУКОЗАПИСИ И ЕЁ УТЕЧКИ ПО АКУСТИЧЕСКОМУ КАНАЛУ

**Аннотация.** Данная работа относится к области обеспечения информационной безопасности переговоров в кабинете руководителя организации или служебном помещении от скрытой звукозаписи и перехвата их с помощью виброакустического зашумления оптического канала связи на акустических частотах и может быть использована в системах защиты конфиденциальной речевой информации.

В работе рассматриваются вопросы защиты речевой информации от скрытой звукозаписи (посредством диктофонов) и от утечки по акустическому и оптико-электронному (лазерному) каналам. В статье предлагается электрическая схема генератора псевдослучайной последовательности импульсов с активным фильтром низких частот, которая на основе создания акустического шума позволяет предотвратить скрытую звукозапись речевой информации и её утечки по акустическим и оптико-электронным каналам.

**Ключевые слова:** утечка речевой информации, виброакустический и оптический технические каналы утечки информации, диктофоны, генератор псевдослучайной последовательности импульсов, активный фильтр низких частот.

Актуальность данного исследования состоит в том, что задача защиты речевой информации от утечки по различным техническим каналам занимает одно из ведущих мест в решении общей проблемы информационной безопасности.

В настоящее время немалую часть передаваемых по техническим каналам связи данных составляет речевая информация. Человеческая речь является универсальным средством общения, обладает уникальными свойствами эффекта присутствия, информационной избыточностью, поэтому широко используется во многих системах связи и передачи информации.Речевая информация может содержать сведения, составляющие конфиденциальную информацию о деятельности предприятия, коммерческую тайну, персональные данные о личной жизни работника государственного сектора, политика, бизнесмена.В этой связи задача защиты речевой информации от утечки по различным каналамзанимаетодно из ведущих мест в решении общей проблемы информационной безопасности.

Для нелегального сьема(прослушивания) речевой информации злоумышленники могут использовать широкий набор технических средств(закладные устройства, диктофоны, магнитофоны, лазерные акустические локационные устройства, направленные

микрофоны и т. д.) и с их помощью перехватывать речевую информацию по акустическому, виброакустическому иоптико-электронному каналам.

Следует отметить, что при проведении практических работ по защите речевой информации от утечки из помещений по акустическим и виброакустическим каналам не достаточно выполнение только пассивных мер защиты, например: усиление звукоизоляции и виброизоляции конструкций, введение звукопоглощения и вибропоглощения в тракты утечки речевых сигналов, применение обнаружителей диктафонов: металлодетекторов, нелинейных локаторов и т. д.[1-3].Кроме того, дорогостоящие предварительные проверки помещений на наличие звукозаписывающих и подслушивающихустройств, оказываются бесполезными, если эти устройства попадают в помещение накануне проведения конфиденциальных переговоров или вносится непосредственно участниками этих переговоров.В таких случаях для гарантированной защиты целесообразно использование активных мер защиты речевой информации путем создания дополнительных акустических и вибрационных маскирующих помех. При этом для эффективного воздействия помехи на устройство перехвата речевой информации, уровень помехи должен в несколько раз, а иногда и на порядок превосходить уровень речевого(полезного) сигнала в канале передачи. Для того, чтобы устройству перехвата было сложнее отфильтровать помеху, ее спектр должен находиться как можно ближе к речевому спектру(диапазону частот от 300 Гц до 3400 Гц).В результатемаскирования речевого сигнала шумовой помехой,«злоумышленники» в своих приемниках (научниках) слышат вместо полезной речевой информации шумы.

В данной статье рассматривается вопрос защиты речевой информации от скрытой звукозаписи с применением диктофонов. Современные диктофоны (аналоговые или цифровые) не только являются микроминиатюрными по габаритным размерам, но и они позволяют вести запись информации (на микрокассету или флеш-память) больших обьемов. Некоторые аналоговые диктофоны позволяют осуществить запись на микрокасету до 6 часов непрерывной работы,другие диктофоны снабжены беззвучным автостопом, системой VOX (автоматического включения записипри появлении акустического сигнала) и системой дистанционного включения/выключения[1,4].Однако самыми удобными для несанкцио-нированной записи речевой информации являются цифровые диктофоны, которые имеют микроминиатюрные размеры, отличаются высоким качеством записи (на микрочипы, карты:SmartMedia, MemoryStick и др) и воспроизведения.

Диктофоны бывают встроенными (стационарными) и переносными (носимыми) и их выбор зависит от разных факторов, в частности от условий, при которых приходится вести звукозапись. Встроенные диктофоны должны быть компактными и иметь относительно малые размеры для обеспечения их скрытности. Однако при этом их возможности по времени непрерывной работы для ведения скрытой звукозаписи речевой информации существенно ограничиваются. На практике более широко применяются переносные диктофоны. Переносной диктофон хорошо комуфлируется под любой элемент личных вещей посетителя-«злоумышленника»(в виде пуговицы на костюме или рубашке, колпачка от авторучки и т. д.), поэтому его не сложно пронести вкабинет руководителя организации или помещение, где будут проходить важные деловые переговоры или совещание.

Обнаружение у посетителя руководителя организации или участника совещания диктофона с применением металлодетектора в принципе не представляет особой трудности. Однако проведение такого мероприятия (открытого досмотра лиц и носимых ими предметов: портфеля, кейсов, сумок и т. д.) перед важным совещанием как правило не

желательно, так как может вызвать отрицательную реакцию посетителя переговоров или участника совещания. Для контроля за проносом диктофона можно использовать нелинейные локаторы («детекторы нелинейных переходов»), которые позволяют обнаруживать звукозаписывающие устройства на относительно больших расстояниях, чем металлодетекторы при входе в помещение.Однако при этом необходимо учитывать безопасность руководителя организации, в кабинете которого будет находиться и эксплуатироваться нелинейный локатор (с относительно высокимуровнем ВЧ-излучения)в течение относительно длительного времени.

Таким образом, для защиты от скрытой звукозаписи с помощью диктофонов целесообразно применение активных мер защиты речевой информации, т. е. целесообразно использование генераторов акустического шума[1,5-7], которые своими колебаниями маскируют звуковые сигналы. При этом для эффективного маскирования эти колебания (шумовые помехи) должны иметь структуру речевого сообщения, т. е. по своему спектральному составу должны быть близкими звуковому сигналу.

Для маскирования речевых сигналов, т. е. для защиты переговоров от скрытой звукозаписи на диктофон, прослушивания с помощью радиозакладки и перехвата их по оптико-электронному каналу в работе предлагается электрическая схема генератора псевдослучайной последовательности импульсов, которая создает акустическое и виброакустическое зашумление (рисунок 1). В состав генератора псевдослучайной последовательности импульсов входят пятиразрядный последовательный(сдвигающий) регистр на триггерах D-типа, мультивибратор (генератор тактовых импульсов), логические элементы: «исключающее ИЛИ», «И» и «ИЛИ», с помощью которых осуществляется обратная связь, и активный фильтр низких частот второго порядка на операционном усилителе (ОУ). Сигнал обратной связи У одновременно подается на входы сдвигающего регистра и активного фильтра низких частот[8].

Рассмотрим принцип действия схемы генератора акустического шума для защиты речевой информации. 0-ое состояние сдвигающего регистра, когда триггеры всехразрядов находятся в состоянии логического 0 (выходные сигналы триггеров $Q_1 = Q_2 = Q_3 = Q_4 = Q_5 = 0$) является не рабочим. Для исключения 0-ого состояния регистра в схему вводится логический элемент (ЛЭ)«И», на входы которого подаются сигналы с инверсных выходов триггеров всех разрядов регистра.

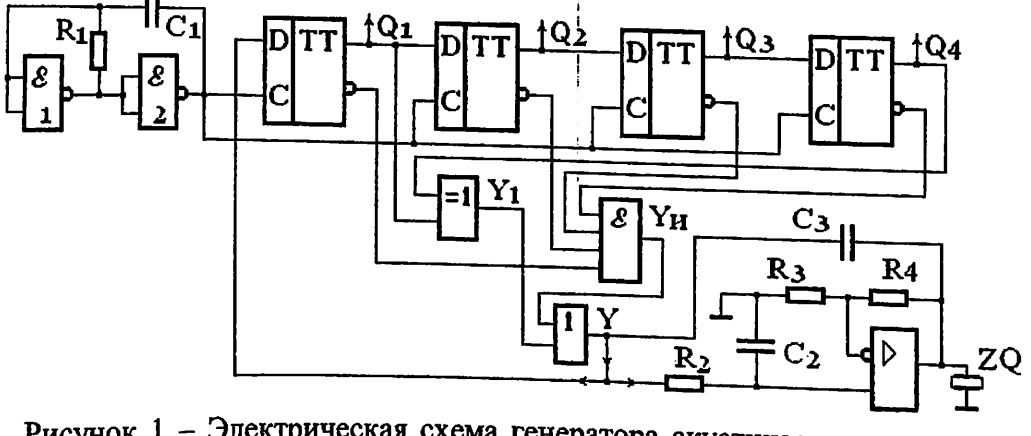


Рисунок 1 – Электрическая схема генератора акустического шума для защиты речевой информации

При 0-ом состоянии регистра на выходе ЛЭ «исключающее ИЛИ»будет сигнал логического 0($У_1 = 0$), а на выходе ЛЭ«И» - логическая 1($У_и = 1$) и этот единичный сигнал

через элемент «ИЛИ» по цепи обратной связи (У = 1) поступает на вход сдвигающего регистра. Следует отметить, что сигнал логической 1 на выходе ЛЭ«И» ($У_И$ = 1) будет только при 0-ом состоянии регистра, а в остальных случаях сигнал $У_И = 0$.

После поступления первого тактового импульса мультивибратора сигнал У = 1 с выхода генератора записывается в триггер первого разряда регистра и одновременно с этим содержимое регистра сдвигается на один разряд вправо. При этом в регистре будет число 1 ($Q_1$ =1, $Q_2 = Q_3 = Q_4 = Q_5 = 0$), а сигнал обратной связи У(он же является выходным сигналом логического элемента «ИЛИ» и генератора псевдослучайной последовательности импульсов) будет равен логическому 0, так как $У = У_1 + У_И = 0 + 0 = 0$. Поэтому после подачи второго тактового импульса в триггер первого разряда записывается сигнал логического 0, а содержимое регистра вновь сдвигается вправо на один разряд и в регистре будет число2 ($Q_1 = 0, Q_2 = 1, Q_3 = Q_4 = Q_5 = 0$). Сигнал обратной связи У будет равен 1(У = 1). Этот 1-чный сигнал записывается в триггер первого разряда после подачи 3-го тактового импульса и после сдвига содержимого регистра в нем будет число 5. Далее после подачи последующих тактовых импульсов мультивибратора состояние разрядных триггеров и содержимое регистра (число в регистре) будут меняться в соответствии с таблицей состояний 1 генератора псевдослучайной последовательности импульсов. Как видно из таблицы состояний 1 после 31-го тактового импульса мультивибратора в регистре будет число 16 ($Q_1 = Q_2 = Q_3 = Q_4 = 0, Q_5 = 1$), а сигнал У = 1, поэтому 32-й тактовый импульс возвращает регистр (генератор) в начальное состояние, соответствующее числу 1($Q_1$ =1, $Q_2 = Q_3 = Q_4 = Q_5 = 0$), У = 1. Состояние регистра, когда все триггеры находятся в состоянии логического 0 ($Q_1 = Q_2 = Q_3 = Q_4 = Q_5 = 0$), как отмечено выше, исключается как нерабочее. Далее генератор будет генерировать псевдослучайные импульсы с длиной (периодом повторения), равным 31 в той же последовательности, как указано в таблице состояний 1.

В общем случае при n-разрядном сдвигающем регистре можно генерировать m - кодовые последовательности псевдослучайных импульсов, где $m = 2^n - 1$. Псевдослучайная последовательность кодов чисел(импульсов) отличается от истинно случайной периодичностью, хотя внутри периода ничем не отличается от истинно случайной. Последовательность 10110101100100011111010110010000, соответствующую $m = 2^n - 1$ можно снять с выхода триггера любого разряда сдвигающего регистра, так как та же самая последовательность поступает с временным сдвигом с выхода триггера каждого разряда. При относительно большом значении nпсевдослучайная последовательность практически не отличается от случайной последовательности.

Таблица 1 - Таблица пятиразрядного генератора псевдослучайной последовательности импульсов

| № тактовых импульсов | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Число в Рг / Вых. сигналы | 0 | 1 | 2 | 5 | 10 | 21 | 11 | 23 | 14 | 29 | 27 | 22 | 12 | 24 | 17 | 3 |
| $Q_1$ | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 |
| $Q_2$ | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 1 |
| $Q_3$ | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 0 |
| $Q_4$ | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 0 |
| $Q_5$ | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 0 |
| Y | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 |
| $Q_1$ | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 |
| $Q_2$ | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 |
| $Q_3$ | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 |
| $Q_4$ | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 0 |
| $Q_5$ | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 |
| Y | 1 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 |

Акустический шум, создаваемый генератором псевдослучайной последовательности импульсов обеспечивает также защиту от прослушивания (с помощью закладных устройств) переговоров в кабинете руководителя организации или переговоров, проводимых в специально выделенных для этой цели помещениях. Для создания акустического шума к выходу генератора псевдослучайной последовательности импульсов подключается активный фильтр низких частот (ФНЧ) второго порядка на основе операционного усилителя, нагрузкой которого является пьезокерамический преобразователь ZQ (рисунок 1). Операционный усилитель включен по схеме неинвертирующего усилителя (повторителя). Активный ФНЧ, частота среза которого мала по сравнению с частотой тактовых импульсов мультивибратора, осуществляет преобразование цифрового шума(псевдослучайной последовательности импульсов) в аналоговый. Цифровой шум представляет собой временной случайный процесс, близкий по своим свойствам к процессу физических шумов и поэтому называется «псевдослучайным процессом». Схема активного ФНЧ второго порядка, называемая также схемой Саллена-Ки (рисунок 1) позволяет реализовать большую крутизну спада амплитудно-частотной характеристики по сравнению со схемой активного ФНЧ первого порядка[6,8]. Следует отметить, что акустическое зашумление помещения обеспечивает эффективную защиту информации в нем, если акустический генератор расположен к акустическому приемнику злоумышленника ближе, чем источник информации. Например, когда подслушивание возможно через дверь или, когда перехват речевой информации осуществляется через оконное стекло с помощью лазерного устройства, то акустический генератор целесообразно прикрепить к двери или разместить на подоконнике, вблизи от зашумляемого оконного стекла. Если местонахождение акустического приемника злоумышленника (например, закладного устройства) неизвестно, то размещение акустического генератора между

говорящими людьми не гарантирует надежную защиту информации. Кроме того, повышение уровня шума вынуждает собеседников к более громкой речи, что создает дискомфорт и снижает эффект от зашумления. Оптимизация режима работы генератора акустического зашумления позволит снизить уровень шумов и обеспечить большую комфортность ведения разговоров в защищаемом помещении.

При использовании лазерного устройства в направлении источника звука (кабинета руководителя организации или комнаты, где ведутся важные переговоры конфиденциального характера) посылается зондирующий луч. Возникающие при разговоре акустические волны, распространяясь в воздушной среде. воздействуют на оконное стекло и вызывают его колебания в диапазоне частот, соответствующих речевому сообщению. Оконное стекло вибрирует под действием окружающих звуков и модулируют своими колебаниями лазерный луч. Таким образом, лазерное излучение, падающее на внешнюю поверхность оконного стекла, в результате виброакустического преобразования речевого сообщения оказывается промодулированным сигналом. Отраженный модулированный сигнал принимается оптическим приемником лазерного устройства, в котором осуществляется восстановление речевой информации из кабинета руководителя организации.

Предложенную в работе схему генератора псевдослучайной последовательности импульсов можно использовать также для защиты речевой информации от прослушивания лазерным микрофоном. Пьезокерамический вибратор генератора псевдослучайной последователь-ности импульсов, прикрепляемый (приклеиваемый) к поверхности оконного стекла, вызывает его колебание по случайному закону с амплитудой, превышающей амплитуду колебаний стекла от акустической волны речевого сигнала. При этом на приемной стороне возникают трудности в детектировании речевого сигнала.

Данная работа относится к области обеспечения информационной безопасности переговоров в кабинете руководителя организации или служебном помещении, выделенном для этой цели, с помощью акустического зашумленияна частотах звуковых сигналов и может быть использовано в системах защиты конфиденциальной речевой информации. Следует отметить также, что генераторы псевдослучайных последовательностей импульсов на сдвигающих регистрах с обратными связями можно использовать для защиты телефонных разговоров, а также в криптографии для создания алгоритмов поточного шифрования[2,7]. Вместе с тем следует отметить, что программная реализация алгоритмов функционирования генераторов псевдослучайных последовательностей импульсов на базе линейных сдвиговых регистров представляет собой достаточно сложную задачу.

**Список литературы**

1 Андрианов В. И., Соколов А.В. Шпионские штучки. Устройства длязащиты объектов и информации: справ. пособие. – СПб.: Лань, 1996. - 254 с.

2 Хорев А.А. Техническая защита информации. Т.1: Технические каналы утечки информации. – М.: НПЦ «Аналитика», 2008. – 436 с.

3 Герасименко В.Г., Лаврухин Ю.Н., Тупота В.И. Методы защиты акустической речевой информации от утечки по техническим каналам. – М.: РЦИБ «Факел», 2008. – 258 с.

4 Дворянкин С.В., Мишуков А.А. Маскирование речевой информации:

Перспективные методы и средства. – М.: журнал «Спецтехника и связь», №3, 2009. – С. 46-51.

5 Горбатов В.С. Контроль защищенности речевой информации впомещениях. – М.: НИЯУ МИФИ, 2014. – 248 с.

6 Горшков Ю.Г. Анализ и маскирование речи. Учебное пособие. – М.:МГТУ им. Н.Э. Баумана, 2006. – 58 с.

7 Адамян А. Защита речевой информации руководителя организации от скрытой записи посетителем. http://daily.sec.ru, 17.08.2007.

8 Джурунтаев Д.З. Схемотехника. Учебник. – Алматы: Эверо, 2005. – 276 с.

**Джурунтаев Д.З.**
*т.ғ.д., Қ. И. Сатпаев атындағы Қазақ Ұлттық Зерттеу Университетінің профессоры, Алматы, Қазақстан*
**Әмірғалиев Е.Н.**
*Сулейман Демирель атындағы университет, Қаскелен, Қазақстан*
**Заурбек А.**
*Қ. И. Сатпаев атындағы Қазақ Ұлттық Зерттеу Университетінің профессоры, Алматы, Қазақстан*

## СӨЙЛЕУ АҚПАРАТЫН ЖАСЫРЫН ЖАЗЫЛЫМ ЖӘНЕ ОНЫҢ АКУСТИКАЛЫҚ АРНА АРҚЫЛЫ ЖОҒАЛУЫНАН ҚОРҒАУ

**Аңдатпа.** Мақалада жасырын дауыс жазу (диктофон арқылы) және акустикалық және оптикалы электронды арналар (лазерлік) арқылы ақпарат жоғалуынан сөйлеу ақпараттарын қорғау мәселелері қарастырылады.

**Кілт сөздер:** сөйлеу ақпаратының жоғалуы, акустика, ақпарат жоғалудың ақпараттың тербеліс акустикалық және оптикалық техникалық арналары,диктофондар, импульстің жалған кездейсоқ генераторы, төменгі жиіліктің белседі фильтрі

**Zhuruntayev D.Z.,**
*Doctor of technical sciences, Professor, Kazakh National Technical Research Unniversity after K. I. Satpayev, Almaty Kazakhstan*
**Amirgaliyev Y.N.,**
*Doctor of technical sciences, Professor, Suleyman Demirel University, Kaskelen, Kazakhstan*
**Zaurbek A.**
*Kazakh National Technical Research Unniversity after K. I. Satpayev, Almaty Kazakhstan*

## THE PROTECTION OF SPEECH INFORMATION FROM HIDDEN RECORDING AND ITS LEAK THROGH ACOUSTIC CHANNEL

**Abstract.** This work relates to the field of information security talks in the office of the head of the organization or the back room of hidden recording and intercepting them by a vibro-acoustic noise optical channel acoustic frequencies and can be used to protect sensitive voice information systems. We consider the protection of the speech information of the hidden recording (by audio recorders) and leakage on acoustic and optical-electronic (laser) channels. The article provides an electric diagram of a pseudo-random sequence of pulses with an active low-pass filter, which is based on the creation of acoustic noise prevents hidden recording of voice data and its leakage through acoustic and optical-electronic channels.

**Key words:** leakage of voice information, acoustic, vibro-acoustic and optical technical channels of information leakage, dictaphone, the pseudo-random sequence of pulses, the active low-pass filter.