Литература

1. Induction Heating. Industrial Applications / Ed. by S. Lupi. Paris, U.I.E., 1992. – 142 p.
2. Румак, Н. В. Экономичный бесконтактный нагрев энергией переменного магнитного поля / Н. В. Румак, В. Л. Ланин, И. Н. Чернышевич // Весці АН Беларусі. Сер. фіз.-тэхн. навук. – 1994. – № 2. – С. 94–96.

АНАЛИЗ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ ВЫДЕЛЕННОГО ПОМЕЩЕНИЯ ОТ УТЕЧКИ ПО АКУСТОЭЛЕКТРИЧЕСКИМ КАНАЛАМ

П. А. Пакуш, И. А. Врублевский

Белорусский государственный университет информатики и радиоэлектроники, г. Минск

Статья посвящена анализу защищенности акустоэлектрических каналов, которые возникают при преобразовании звуковых волн в электрические сигналы (например, в телефонных линиях или из-за вибраций оконных стекол) и представляют угрозу утечки информации ограниченного распространения. Подробно рассмотрены методы защиты окон как слабого звена с точки зрения виброакустической безопасности. На основе анализа данных о звукоизоляции различных типов остекления обосновывается необходимость применения систем активной защиты с вибродатчиками и генераторами шума.

Ключевые слова: защита информации, система активной защиты, вибродатчик.

PROTECTION OF SPEECH INFORMATION OF THE PROTECTED ROOM FROM LEAKAGE VIA ACOUSTOELECTRIC CHANNELS

P. A. Pakush, I. A. Vrubleuski

Belarusian State University of Informatics and Radioelectronics, Minsk

The article is devoted to the security analysis of acousto-electric channels, which arise from the conversion of sound waves into electrical signals (e.g., in telephone lines or due to window pane vibrations) and pose a threat of leaking classified information. Methods for protecting windows as a vulnerable point from the perspective of vibroacoustic security are examined in detail. Based on the analysis of sound insulation data for various types of glazing, the necessity of using Active Protection Systems (APS) with vibration sensors and noise generators is substantiated.

Keywords: information security, active protection system, vibration sensor.

Актуальность задач защиты речевой информации от утечки по акустическим каналам, связанных с источником речи человека, занимает важное место в области безопасности информации. Современные системы связи и переговоры могут сопровождаться риском утечки информации ограниченного распространения. Одним из таких каналов утечки является акустоэлектрический канал – передача звуковой информации через вибрации, электромагнитные наводки и другие физические эффекты, которые могут быть зафиксированы злоумышленниками. Для предотвращения рисков потери информации необходимо предпринять ряд мероприятий организационного и технического характера, направленных на построение системы защиты речевой информации защищаемого помещения от утечки по акустоэлектрическим каналам.

Акустоэлектрические каналы возникают из-за преобразования звуковых волн в электрические сигналы, которые могут передаваться по проводам или другим электрическим каналам. Эти каналы являются уязвимыми для перехвата или подслуши-

вания электрических сигналов. Уязвимость акустоэлектрических каналов связана с тем, что электрические сигналы могут быть перехвачены или прослушаны.

Акустоэлектрический канал утечки в основном используется в целях перехвата конфиденциальной речевой информации в помещении. Для того чтобы подключиться к линии телефонного аппарата, установленного в контролируемом помещении, злоумышленники могут использовать специальные устройства – низкочастотные усилители или аппаратуру «высокочастотного навязывания». Используя эти средства, перехват информации может быть осуществлен через соединительные линии ВТСС, которые обладают микрофонным эффектом [1].

Для обеспечения безопасности переговорной комнаты необходимо применять технические решения, которые позволяют предотвратить утечки конфиденциальной информации. К активным видам защиты относятся генераторы шума, которые будут зашумлять линию, выходящую за пределы контролируемой зоны во время проведения переговоров. По сравнению с пассивными средствами защиты основным недостатком данного метода защиты является его дороговизна, а невозможность удостовериться в работоспособности самого устройства защиты. Следует также отметить, что также помеха может быть отфильтрована злоумышленником. К активным способам защиты можно также отнести и уничтожение средств прослушивания или их «выжигание». При использовании такого способа в линию подается высоковольтные импульсы (до 1500 вольт), приводящие к выходу из строя технических средств злоумышленника. Однако применение такого способа является как опасным, так и не совсем эффективным. Опасен он тем, что во время процесса «выжигания» к линии может быть подключено другое оконечное устройство, которое будет выведено из строя. А его недостаточная эффективность вытекает из того, что злоумышленник может подключиться к линии уже во время проведения переговоров, и его техника останется цела. Помимо этого, существуют также различные технические средства, с помощью которых можно извлекать информативные сигналы из линии, не имея к ней прямого гальванического подключения, а только находясь рядом с ней.

К пассивным средствам защиты линий, выходящих за пределы контролируемой зоны можно отнести ограничители сигналов малой амплитуды, которые позволяют практически полностью ограничить прохождение полезных сигналов в линию. К недостаткам способа защиты ограничителями можно отнести его незначительное влияние на линию, к которой он подключен. Это связано с тем, что помимо информативных акустических сигналов, он также может отфильтровать сигналы, необходимые для работы технического средства, установленного в помещении. Размыкатели, как понятно из названия, размыкают линию, и злоумышленник уже не сможет получить информацию от устройства, которое находится в помещении. Они могут быть выполнены как в виде простого ключа, так и автоматического прибора, который отключает аппарат от линии при положенной трубке. Такой способ защиты является самым надежным и требующий дополнительных средств защиты только для комфортного исполнения. Но и у него есть определенные недостатки, например, невозможность использования технических средств в момент проведения переговоров.

Исходя из приведенных способов защиты, можно сделать вывод, что, говоря о полной защите помещения от канала утечки акустоэлектрических преобразований, можно говорить лишь об отключении технических средств от линий, выходящих за пределы контролируемой зоны. Решить такую задачу может расширение границ контролируемой зоны с возможностью отсутствия подключение к таким линиям злоумышленника, а также отказ от технических средств в помещениях для проведения переговоров.

К дополнительным мерам по противодействию утечкам информации через акустический, оптический и электрический каналы можно отнести: установку генератора белого шума, использование акустических панелей и средств затемнения для защиты от акустических утечек, а также фильтрацию электромагнитных помех и шифрование данных для защиты от электрических утечек. Такие технические решения, интегрированные в общую структуру безопасности, обеспечивают надежную защиту информации ограниченного распространения в переговорной комнате, обеспечивая высокий уровень безопасности и конфиденциальности важных бизнес-процессов и переговоров.

Организация системы защиты с использованием САЗ должна производиться при оптимальном соотношении защиты и удобства использования. В любом помещении наиболее уязвимыми с точки зрения перехвата информации являются двери и окна. Переговорная комната с окнами в пол – современное дизайнерское решение, обеспечивающее максимальное естественное освещение и визуальное расширение пространства. Однако такие окна создают определенные вызовы с точки зрения безопасности и акустики. Большие стеклянные поверхности хуже поглощают звук, способствуя его отражению и распространению. Кроме того, стекло может передавать вибрации, способствуя акустоэлектрическим утечкам. Оконные стекла сильно вибрируют под давлением акустической волны.

В таблице представлены результаты исследований звукоизоляции различных типов остекления. Данные таблицы наглядно показывают, что окна обладают слабыми изолирующими качествами.

Значения звукоизоляции различных типов остекления

Схема остекления	Звукоизоляция (дБ) на частотах, Гц					
	125	250	500	1000	2000	4000
Одинарное остекление:						
Толщина 3 мм	17	17	22	28	31	32
Толщина 4 мм	18	23	26	31	32	32
Толщина 6мм	22	22	26	30	27	25
Двойное остекление с воздушным промежутком						
57 мм (3 мм)	15	20	32	41	49	46
90 мм (3 мм)	21	29	38	44	50	48
57 мм (4 мм)	21	31	38	46	49	35
90 мм (4 мм)	25	33	41	47	48	36

Можно также отметить, что увеличение числа стекол не всегда приводит к увеличению звукоизоляции на частотах речевого сигнала. Это связано с тем, что могут наблюдаться резонансные явления в воздушных промежутках (между стеклами) и эффектах волнового совпадения. Отсюда следует, что разумным выбором для защиты окон от виброакустического канала утечки является установка системы активной защиты – генератора шума и вибродатчиков. Учет физических характеристик речевого сигнала имеет ключевое значение для оптимизации системы активной защиты. Поскольку длина волны основных частот речи варьируется от 8,6 см (4000 Гц) до 1,37 м (250 Гц), зона максимальной амплитуды вибраций стекла будет сосредоточена в его центральной части. Именно в этой области происходит формирование

стоячих волн и наблюдается наибольшая виброакустическая активность при воздействии речевого сигнала. Следовательно, размещение вибродатчиков в центре стеклянных панелей является наиболее эффективным. Такая локация позволяет:

– охватить весь спектр речевых частот, обеспечивая шумоподавление как коротких (высокочастотных), так и длинных (низкочастотных) волн;

– получить максимальное зашумление информативного сигнала, предотвращая возможность его последующего детектирование.

Таким образом, установка датчиков в центральных зонах стекол является оптимальным решением для создания эффективной системы противодействия утечкам информации через виброакустический канал. Оптимизация активной защиты заключается в правильном размещении датчиков на стеклах и в тщательной настройке АЧХ источника шумового сигнала. Уменьшить паразитный шум можно увеличением количества вибродатчиков и уменьшением на них мощности помехи [2].

Методы оптимизации:

1. Вибродатчики необходимо размещать только на стеклах. Связано это с тем, что попытки установки вибродатчиков на рамы окон приводят к недопустимому уровню акустических шумов при выполнении норм защищенности.

2. Дать рекомендации по количеству необходимых для размещения вибродатчиков на одном стекле практически невозможно – многое зависит от условий. Заключение выводится экспертным методом, исходя из пробных замеров и опыта. В среднем, оптимально размещать на 1 $м^2$ стекла 2 датчика (одиночное стекло), а при остеклении стеклопакетом – до 4 датчиков.

3. Серьезная оптимизация достигается при индивидуальной настройке мощности каждого датчика. Данный метод оптимизации возможен только при использовании генераторов системы активной защиты, имеющих регуляторы АЧХ.

Важным элементом является проведение оценки эффективности системы активной защиты. После оптимизации системы активной защиты необходимо удостовериться в том, что выполняются требования защищенности. Для этого выбираются контрольные точки на плоскости стекла, с которых снимаются показания уровней шума и сигнала/шума. Выбор контрольных точек является достаточно сложным, но с уверенностью можно сказать, что оценка показаний одной контрольной точки не показывает эффективность системы защиты.

В настоящее время руководящими документами не определено, какая из нескольких имеющихся поверхностей остекления (внешняя или внутренняя) наиболее опасна для вибрационного канала утечки информации при применении средств дистанционного съема информации. В связи с этим, опасны все поверхности, и, следовательно, должна оцениваться защищенность для каждой из них. Если выполняются условия защищенности на внутренних поверхностях окна (внутреннем стекле), то они будут выполняться и на внешних. Связано это с тем, что отраженный сигнал от внешней поверхности модулирован более слабым информативным сигналом, и кроме того, уровень шума на них значительно больше, чем на внутренних поверхностях.

Проведенный анализ позволяет сделать вывод, что акустоэлектрические каналы утечки информации, возникающие как в линиях связи, так и на вибрирующих ограждающих конструкциях, в особенности на таких поверхностях как окна, представляют собой серьезную угрозу для конфиденциальности переговоров.

Надежная защита речевой информации требует комплексного подхода, сочетающего пассивные и активные методы. Наиболее эффективным из пассивных средств защиты линий связи является их физическое размыкание на время проведения переговоров. Однако для защиты от дистанционного съема информации через

вибрации оконных стекол пассивных методов звукоизоляции недостаточно. Увеличение количества стекол в стеклопакете не гарантирует адекватного подавления речевого сигнала на всех частотах из-за резонансных явлений. Таким образом, ключевым элементом безопасности для помещений с большими окнами становится применение оптимизированных систем активной защиты (САЗ). Их эффективность напрямую зависит от корректного размещения вибродатчиков на поверхности стекол и точной настройки амплитудно-частотной характеристики (АЧХ) генераторов шума для каждого конкретного окна. Оценка защищенности должна проводиться по контрольным точкам на всех поверхностях остекления.

Достижение максимального уровня безопасности возможно только при интеграции организационных мер (расширение контролируемой зоны) с техническими решениями, где пассивная защита линий связи дополняется активной виброакустической защитой ограждающих конструкций, образуя эшелонированную систему предотвращения утечек информации.

Литература

1. Кутузов, В. И. Повышение эффективности защиты информации от утечек информации через окна по акустическому и виброакустическому каналу при использовании средств активной защиты / В. И. Кутузов. – URL: https://journalpro.ru/articles/povyshenie-effektivnosti-zashchity-informatsii-ot-utechek-informatsii-cherez-okna-po-akusticheskomu (дата обращения: 19.09.2025).
2. Нуриев, С. А. Защищенность речевой информации в научных организациях от утечки по техническим каналам / С. А. Нуриев, И. Н. Карцан // Современные инновации, системы и технологии. – 2023. – № 3. – С. 349–361.

ОДНОКОНТУРНЫЙ ПОЗИЦИОННЫЙ ЭЛЕКТРОПРИВОД

К. А. Хаджинова, М. К. Хаджинов

Белорусский государственный университет информатики и радиоэлектроники, г. Минск

Рассмотрена разработка одноконтурных позиционных электроприводов, способных конкурировать с традиционными трехконтурными системами. Предложены два варианта: с ПДД-регулятором в прямой цепи и с ПД-регулятором в обратной связи. Оба обеспечивают астатизм и высокую устойчивость, демонстрируя конкурентоспособность по длительности переходной характеристики при одинаковом периоде дискретизации.

Ключевые слова: одноконтурные позиционные электроприводы, трехконтурные системы управления, ПДД-регуляторы, ПИ-регуляторы, астатизм по возмущениям, устойчивость к изменениям параметров, малогабаритные устройства.

SINGLE-LOOP POSITION ELECTRIC DRIVE

K. A. Khadzhinova, M. K. Khadzhinov

Belarusian State University of Informatics and Radioelectronics, Minsk

This paper examines the development of single-loop positional electric drives capable of competing with traditional three-loop systems. Two designs are proposed: one with a PDD controller in the feedforward loop and one with a PD controller in the feedback loop. Both provide astatic behavior and high stability, demonstrating competitiveness in terms of transient response duration with the same sampling period.

Keywords: single-loop positional electric drives, three-loop control systems, PDD controllers, PI controllers, astatic behavior, stability to parameter changes, compact devices.