Қазақстан Республикасы Тәуелсіздігінің 30 жылдығына арналған «Сейфуллин оқулары – 17: «Қазіргі аграрлық ғылым: цифрлық трансформация» атты халықаралық ғылыми – тәжірибелік конференцияға материалдар = Материалы международной научно – теоретической конференции «Сейфуллинские чтения – 17: «Современная аграрная наука: цифровая трансформация», посвященной 30 – летию Независимости Республики Казахстан.- 2021.- Т.1, Ч.3 - С.11 – 15

ЗАЩИТА РЕЧЕВОЙ ИНФОРМАЦИИ

Ж.М. Байбулов,
Б.Ж. Медетов ,
Б.Е. Хамзина Б,
Е.Т.Шодыбаев

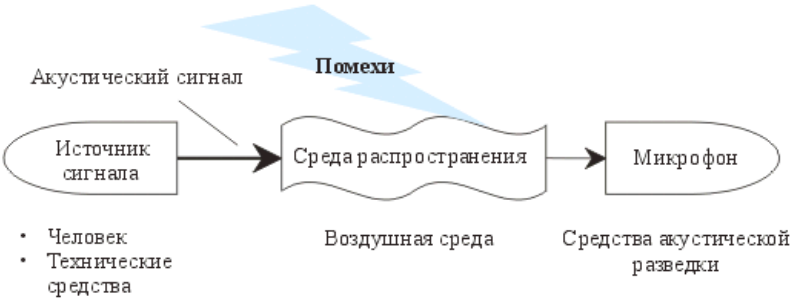
Статья посвящена сравнению и обзору существующих способов защиты речевой информации от утечки по акустическим каналам. Предложен способ защиты речевой информации с использованием комбинации маскирующих сигналов, состоящих из «белого» шума и речеподобных сигналов. Рассмотрены два основных направления технических мероприятий по защите информации с применением пассивных и активных способов.

Ключевые слова: шум, защита информации, речевая информация, акустический канал, маскирующий сигнал.

В процессе человеческой деятельности, в том числе и мышления, человек становится обладателем определенной информации, которая может быть конфиденциальной. Обладая определенной информацией, человек должен поделиться ею с определенным числом людей. При этом, как это часто бывает, первым типом такой информации является речевая информация. Особенностью защиты речевой информации является то, что она тесно связана с источником речи в виде акустических звуковых волн. Акустическая волна передает речевую информацию от источника к приемнику и одновременно воздействует на элементы ограждающих конструкций помещений. Это порождает вибрацию стеновых элементов, которая, распространяясь по всей конструкции здания, тем самым создавая акустический канал утечки, способствующий легко перехватить речевую информацию [1].

Существующие способы защиты информации при утечке по акустическим каналам, такие как уменьшение отношения сигнал/шума или увеличения уровня шума, которая не позволяет эффективно защитить нашу речевую информацию от возможности перехвата или непреднамеренного прослушивания. Из этого следует что необходим способ, который обеспечит закрытие каналов утечки речевой информации. С целью смоделировать иной способ, нами был проведен обзор и сравнение существующих способов защиты речевой информации от утечки по акустическим каналам.

Акустический канал утечки информации — это каналы, образованные за счет распространения акустических волн через среду между источником и приемником акустических волн и делится на два типа: прямой акустический канал, комбинированный акустический канал включающий распространение акустических волн в газовой, твердой и жидкой среде или различные их комбинации.



Акустический канал утечки информации

Защита акустической информации осуществляется пассивными и активными способами. [1]. Цель пассивного способа защиты акустической информации - максимально ослабить акустический сигнал от источника звука. Под пассивными способами понимается комплекс проектных и строительно-монтажных мероприятий, направленных на доработку: ограждающих конструкций помещения, систем инженерного и проводных систем различного назначения. Проводя вышеперечисленные работы, удается достигнуть соответствующих уровней звукоизоляции, виброизоляции, и понижения уровней опасных сигналов, возникающих за счет акустоэлектрических преобразований. В замкнутых пространствах звуковые волны отражаются от ограждающих конструктивных элементов, в результате формируется сложный рисунок звукового поля. Поглощение звуковой энергии является защитой не только конструкций помещений, но и воздуха. Потери энергии обусловлены вязкостью воздуха, теплопроводностью воздуха, а также молекулярным поглощением.

Наиболее частые каналы утечки акустических данных генерируются через вентиляционные отверстия, окна и двери. Рекомендуются установка резиновых прокладок на оконную раму и места примыкания стекла к раме для виброизолированния. Использовать не менее двух стеклопакетов, а также устанавливать звукопоглотители из стекловатного войлока или устанавливать поглотители на стенках вентиляционных каналов с использованием искусственных препятствий для изменения направления потока воздуха в вентиляционных отверстиях. Двери должны быть выполнены с тамбуром и плотным прилеганием дверного полотна к дверной раме. Бесспорными плюсами пассивных способов защиты информации являются отсутствие паразитных акустических шумов в защищаемом помещении, высокая временная надежность и стабильность параметров звуко- и виброизоляции, постоянная защищенность помещения в течение определенного времени, защищенность помещения не зависит от наличия

энергоснабжения, увеличения комфортности в помещениях (снижение общего уровня шума).

Активные способы защиты речевой информации основаны на создании дополнительных шумов на каналах утечки речевых данных, то есть на сокрытии сигнала, несущего речевые данные. Для реализации активной защиты используются специальные генераторы широкополосных электрических помех речевого диапазона частот, к которым подключаются излучатели различного типа, рассчитанные на создание помех в различных элементах строительных конструкций. Устройства активной защиты речевой информации состоят из генератора маскирующих сигналов и набора преобразователей электрических сигналов в акустические (электродинамические громкоговорители) или преобразователей электрических сигналов в механические сигналы.

При установке преобразователей на защищающие конструктивные элементы следует создавать силовое воздействие на ограждающие конструктивные элементы, вызывающее их вибрацию. В качестве вибропреобразователей широко используются пьезоэлектрические и электромагнитные преобразователи. [2]. Недостатком является сложность конструкции электромагнитного преобразователя для работы на высоких частотах (от 2000 до 8000 Гц). Пьезоэлектрические преобразователи не развивают необходимой силы для возбуждения колебаний ограждающих конструктивных элементов в диапазоне частот от 100 Гц до 500 Гц. Датчики, установленные на стенах, полу, потолке, оконных стеклах, издают акустические шумы, создавая неудобные условия в охраняемой зоне. Поэтому предлагается закрывать их звуконепроницаемыми колпачками и использовать автоматическое управление сигналами маскировки уровня в зависимости от уровня звукового давления защищаемой речи.

Эффективность технической защиты акустической информации зависит от правильного размещения преобразователей на защищающих конструктивных элементах. Рекомендуется, если здание выполнено из сборного железобетона, то преобразователи систем акустической защиты должны быть размещены на каждом элементе конструкции здания. Необходимость таких требований продиктована недостаточной устойчивостью акустических импедансов на стыках при эксплуатации здания. Указывается, что установка преобразователей должна производиться в геометрическом центре здания.

В настоящее время создано большое количество различных систем активной защиты информации и анализируя их можно выделить следующие плюсы и минусы. К преимуществу систем активного зашумления относится возможность точной настройки зашумляющих сигналов, снижающих паразитные шумы и возможность обеспечения защищенности практически любого помещения. Однако активным способам присущ ряд недостатков, среди них невозможность полного скрытия защитных мероприятий, а защищенность помещения обеспечивается только при нормальном энергоснабжение помещения.

Для защиты переговоров от прослушивания предлагаем использовать генераторы акустической шумовой помехи – «белый шум». Они позволяют замаскировать полезную информацию на фоне шума, формировавшиеся за счет теплового шума, полупроводника или другого естественного физического шума. Эти требования вытекают из необходимости избегания любой возможности перехвата акустических сигналов. Использование цифрового шума вместо "белого" шума создает риск того, что существует возможность применения шумоподавления. Речеподобные сигналы, генерируемые с помощью генератора случайных чисел, должны основываться на тепловых шумах в полупроводниковых приборах, а не на псевдослучайных последовательностях, генерируемых цифровыми приборами.

Нами выявлено, что эффективность устройств защиты речевой информации повышается при использовании речеподобных сигналов, генерируемых на основе аллофонов, с учетом вероятности продолжения слов и длинных предложений. Речеподобные сигналы формируются на основе аллофонов, работающих в охраняемой зоне, трудно отделить речевой формат и речеподобные сигналы благодаря чему обеспечивается закрытие каналов утечки речевой информации.

Так, в ходе нашего анализа и сравнения существующих способов защиты информации, нами была определилась модель защиты информации, которая позволит эффективно защитить нашу речевую информацию в помещениях и в линиях связи. Данная модель содержит устройства активной защиты речевой информации, формирующие маскирующие сигналы белого шума и шума с огибающей амплитудного спектра, подобные речевому сигналу. При этом, активная и пассивная защита речевой информации должна быть организована и осуществляться таким образом, чтобы не допустить распространения акустических колебаний, несущих речевую информацию за пределы охраняемой территории.

Разработка новых систем безопасности должна быть поставлена таким образом, чтобы, как только появятся предпосылки для создания новых средств нарушения защиты информации, необходимо начинать разработку мер по их противодействию. Эти разработки должны начаться не тогда, когда уже созданы новые средства нарушения информационной безопасности, а гораздо раньше, то есть, когда уже есть предпосылки для создания таких средств. Только при таких условиях система защиты информации может считаться эффективной. Тем не менее не стоит забывать о ряде других каналов утечки речевой информации, которые являются не менее опасными.

Список литературы

1. Administrative Management in Information // Protection Technical information protection// Administrative Management in Information. - С. 292.

2. Kazumasa Yamamoto, Seiichi Nakagawa. // Privacy Protection for Speech InformationJournal of information Assurance and Security. - № 5. - С. 284.

3. НЕЛК [Электронный ресурс]. Режим доступа: https://nelk.ru/catalogue/s92/s94%20 Дата обращения: 18.11.2020.

4. Техника СпецСлужб [Электронный ресурс]. Режим доступа: https://www.t-ss.ru/vibroacustik.htm Дата обращения: 19.11.2020.

5. Secandsafe.ru [Электронный ресурс] Режим доступа: https://secandsafe.ru/ stati/ zaschita_informacii/vibroakustichieskaia_zashchita_pomieshchienii%20. Дата обращения 18.11.2020.

6. Speech information security assessing in case of combined masking signalsSeitkulov, Y.N., BORANBAYEV, S.N., TASHATOV, N.N., DAVYDAU, H.V., PATAPOVICH, A.V.Journal of Theoretical and Applied Information Technology, 2020, 98(16), С. 3270–3281.

7. «Технические средства защиты информации». - Журнал "Специальная техника". -№14. - 2018.

8. Kondratev A.V. //Article Compromise of active and passive methods of vibroacoustic information protection. 2015. - С.76.

9. Technical surveillance counter measures (TSCM) [Электронный ресурс]. - Режим доступа: http://tscm/whatistscm.html. Дата обращения: 18.11.2020№

10. Special Equipment. - Germany: SIM Security & Electronic System GmbH, 2016.

11. Wahl G. Minispione-Schaltungstechnik. - Baden-Baden: Verl. fur Technik und Handwerk (vth-Fachbuch). Bd. 2. Oszillatoren fur Minispione; Passive Minispione; UKW-Leistungssender;Video-Modulatoren; Minispione-Abwehrgerate; Verzeichnis handelslieblicher Uberwachungs- und Abwehrgerate. - 4. Aufl. - 2012. – С. 45.

12. WA Technology: product Catalogue. - China, BSWA Technology Co., Ltd, 2014. -– С. 145.

13. Хореев А.А. Техническая защита информации. Том 1. Технические каналы утечки информации. М.: НПЦ «Аналитика», 2008. – С. 22.