АКУСТИЧЕСКИЕ АСПЕКТЫ МОДЕЛИ УГРОЗ УТЕЧКИ ИНФОРМАЦИИ ПО СРЕДСТВАМ МОДУЛЯЦИИ ВИДИМОГО СВЕТА

ACOUSTIC THREAT OF INFORMATION LEAKAGE BY MEANS OF MODULATION OF VISIBLE LIGHT

B. Shvyrev
D. Timonov

Summary. The article discusses a new type of leakage of acoustic information by means of modulating the visible light generated by the LEDs of lighting devices due to the microphone effect or deliberately inserted bookmarks. The sound of human speech is distributed in the room with the absorbing coating without taking into account the reflections. The main method of hiding information processed in the meeting room in accordance with the current regulations is to install vibration-acoustic generators in potentially vulnerable areas. The tactics of their location is based on the model of the threat of information leakage on the means of using radio waves. In the work, the calculation of the signal-to-noise ratio for different heights of the room. The existence of information security vulnerabilities due to the transmission of voice information available without interference at the ceiling level with lighting LEDs is shown. The choice of information security tools does not take into account the threat of information leakage by means of modulation of visible light.

Keywords: leakage channel of acoustic information, modulation of visible light, signal-to-noise ratio, information leakage threat.

Швырев Борис Анатольевич
К.ф.-м.н., в.н.с., ФКУ Научно-исследовательский институт ФСИН России
bor2275@yandex.ru
Тимонов Дмитрий Александрович
Начальник лаборатории, Краснодарское высшее военное училище имени генерала армии С. М. Штеменко
dmitrii-timonov@bk.ru

Аннотация. В статье рассматривается новый вид утечки акустической информации по средствам модуляции видимого света, создаваемого светодиодами осветительных приборов за счет микрофонного эффекта или сознательно заложенной закладки. Звук речи человека распространяется в помещении с поглощающим покрытием без учета пере отражений. Основным способом сокрытия информации, обрабатываемой в переговорном помещении в соответствии с действующими регламентами, является установка на потенциально уязвимых участках вибро-акустических генераторов. Тактика их расположения основывается на модели угроз утечки информации по средствам использования радиоволн. В работе выполнен расчет величины отношения сигнал/шум для различных высот помещения. Показано существование уязвимости информационной безопасности за счет передачи речевой информации доступной без помех на уровне потолка с осветительными светодиодами. В выборе средств защиты информации не учитывается угроза утечки информации по средствам модуляции видимого свету.

Ключевые слова: канал утечки акустической информации, модуляция видимого света, отношение сигнал/шум, угроза утечки информации.

В настоящее время защита акустической информации на объекте реализуется путем использования ряда административных и технических мер. Основная техническая методика, препятствующая утечке речевой информации по акустическому и виброакустическому каналу основана на уменьшении отношения «сигнал/шум». В [1–3] авторы определяют пассивные и активные методы защиты.

Пассивные методы направлены на уменьшение уровня информативного сигнала за счет улучшения звуко-и виброизоляции инженерных конструкций и установки фильтрующих устройств в проводных коммуникациях.

Защита помещений для конфиденциальных переговоров реализуется с помощью основных двух групп технических средств: Инженерно-технические средства защиты помещений, Технические средства защиты от перехвата речевой информации.

Инженерно-технические средства защиты помещений включают в себя: инженерные конструкции и материалы вносящие значительное затухание в поле звуковой волны распространяющейся наружу контролируемого объекта, технические средства зашумления строительных конструкций акустическим и виброакустическим шумом.

Технические средства защиты от перехвата речевой информации включают в себя объемное зашумление помещения в близи от места источника речевой информации [1–3]. Обычно в соответствии с действующими методиками зашумление выполняется в звуковом диапазоне, реже в ультразвуковом. Конечно, целесообразно использование зашумления и в диапазоне электромагнитных волн, но такое решение подразумевает неустранимое наличие негласного радиопередатчика или мобильного телефона. Конечно наличие негласных радиопередатчиков имеет организационную ком-

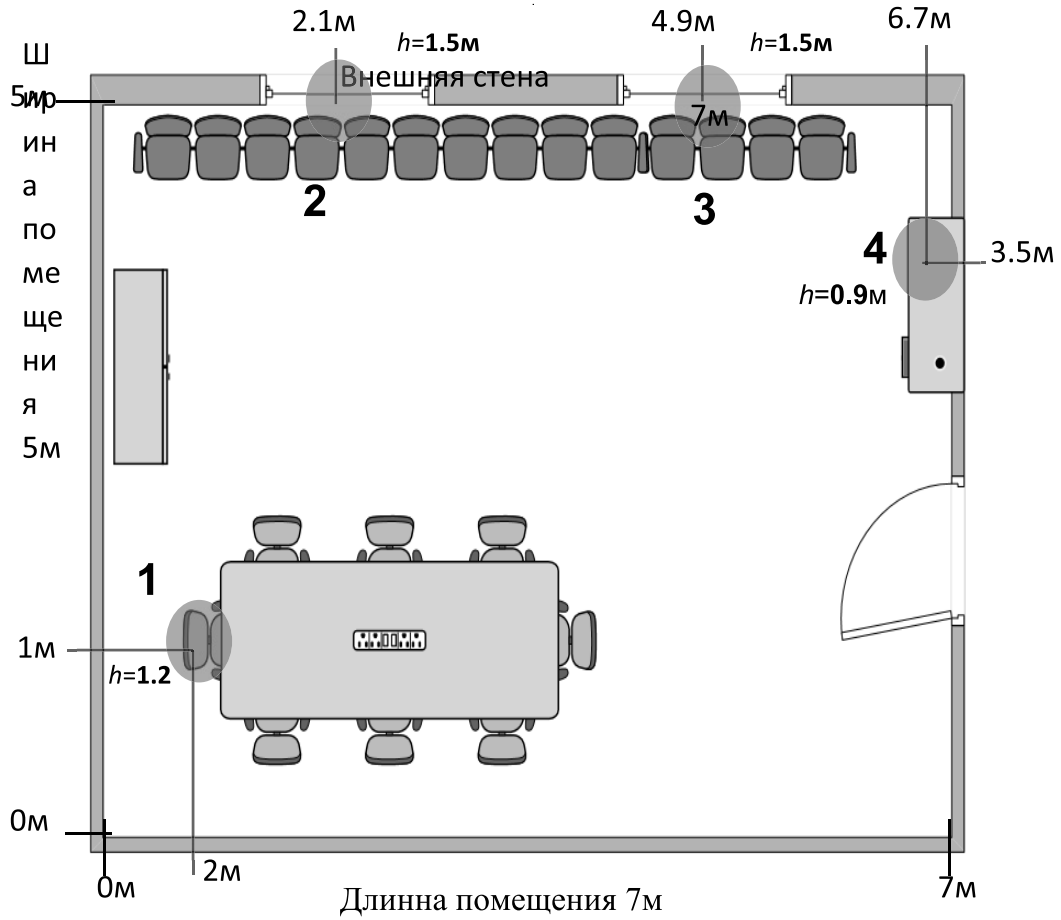

Рис. 1. Схема комнаты для переговоров с указанием источников звука: 1 –диктора с уровнем 55дБ, 2 и 3 – генераторы шума 20 дБ, 4 – генератор шума 40 дБ.

поненту контроля и при реализации комплекса мероприятий в принципе может быть минимизирована, что нельзя сказать в отношении сотовых телефонов. При этом для важных конфиденциальных переговоров использование генератора шума в радиодиапазоне будет оправданным и уместным.

При расположении радиомикрофона в близости от источника речевой информации и последующего преобразования видимого света светодиодов освещения в соответствии с передаваемым сообщением возникает надежный канал утечки речевой информации, который в настоящее время недостаточно изучен и мало представлен в отечественной литературе. Наиболее вероятным местом размещения специального технического средства (СТС), использующего модуляцию видимого света на объекте является потолок.

Найдем минимальные граничные значения уровня речевого сигнала диктора, который может быть зарегистрирован на потолке переговорного помещения с учетом помех и высоты потолков.

При неизменной частоте громкость звука растет с увеличением интенсивности. При одинаковой интенсивности наибольшей громкостью обладают звуки в диапазоне частот 700–6000 Гц. Нулевой уровень громкости звука соответствует звуковому давлению 20 мкПа и силе звука 10› Вт/м при частоте 1 кГц. Считается, что человек слышит в диапазоне 0–120дБ [3].

Уровень звука постоянного шума в помещениях определяется в ГОСТ 12.1.036–81 и СН 2.2.4/2.1.8.562–96 «Шум на рабочих местах, в помещениях жилых, общественных зданий и на территории жилой застройки» [4]. Уровень 30 дБ соответствует тихому разговору, 100 дБ сильному крику. Одним из наиболее важных параметров при расчете уровня звукового давления является уровень шума. Установлено, что человек способен (слышать) улавливать звуки с уровнем 1дБ (20мкПа, 10–12 Вт/м2), который называется порогом слышимости. Но это возможно только при хорошем слухе и в отсутствии шума. Так как в реальных условиях, шум всегда присутствует, то различить полезную (звуковую) информацию на фоне шума можно при условии, что уровень звука превышает

уровень шума, как минимум на 3 дБ (в 2 раза). Для хорошей разборчивости данная разница должна составлять минимум 6дБ (в 4 раза). В нормативной же документации данный запас составляет 15дБ.

По мере удаления расчетной точки (слушателя) от звукового источника, звуковое давление в этой точке, уменьшается по логарифмическому закону. Зависимость в виде формулы:

$$P = 20\ lg\ (L), \quad (1)$$

где P — звуковое давление, дБ; L — расстояние от источника звука до расчетной точки, м.

Интерпретацию данной зависимости называют правилом шести децибел: При каждом удвоении удаления от источника звука (громкоговорителя), звуковое давление уменьшается на 6дБ!

Зная звуковое давление источника звука P_0, можно определить звуковое давление в расчетной точке P_i, находящейся на расстоянии L от этого источника:

$$P_i = P_o\ - 20\ lg\ (L) \quad (2)$$

Используя минимально допустимые значения уровня звукового давления, создаваемого диктором и системами генерации акустического шума рассчитаем распределение звукового давления в помещении для переговоров на рис. 1 и рис. 2.

Информативное поле, создаваемое диктором, значительно затухает при удалении и его уровень перекрывается звуковым полем, создаваемым генераторами акустического шума. Выбор средств защиты определяется тактикой защиты помещения для переговоров и установкой оборудования исходя из модели угроз в местах наиболее уязвимых для несанкционированного доступа к акустической информации. Внешняя стена помещения с двумя оконными проемами является самым уязвимым местом и входная дверь из не выделенного помещения. Другие две стены являются капитальными и содержат инженерные средства зажиты. Такое расположение

Интенсивность звукового давления, создаваемого диктором на потолке помещения в его проекции, обладает наибольшим вкладом в звуковое поле. На потолке отмечается незначительный уровень шумового звукового поля, создаваемого генераторами. Интенсивность звукового поля диктора на уровне потолка значительно затухает по мере удаления от источника звука. Можно отметить, что звуковое давление на потолке создастся преимущественно диктором, что определяет уязвимость утечки информации через СТС, расположенные на потолке помещений. Расположение СТС, использующих радиодиапазон для передачи информации за пределы контролируемого помещения, на потолке не рассматривается как вероятная модель угрозы, но может иметь место, если имеется подвесной потолок скрывающий систему вентиляции. Использование СТС радиодиапазона на потолке не обеспечивает значительной дальности передачи и в связи с этим маловероятен. Совсем иначе обстоит дело при использовании модуляции видимого света, создаваемого светодиодами осветительных приборов помещений. Осветительные светодиодные приборы располагаются на поверхности потолка или ниже при использовании люстр и потенциально обладают наименьшим расстоянием до говорящих и максимальным расстоянием до генераторов шума. Что обеспечивает хорошие условия для перехвата звукового поля говорящего и отсутствии влияния шумового поля от генераторов шума акустического диапазона. Расположение управляемых осветительных светодиодов на потолке позволяет регистрировать звуковое поле диктора без значительных помех и передачи его по средствам модуляции видимого света.

Для большей информативности рассчитаем отношение сигнал/шум по мощности на разных высотах помещения для переговоров. Отношение сигнал/шум (ОСШ, англ. SNR, Signal-to-Noise Ratio) является безразмерной величиной и удобно для проведения сравнительных оценок:

$$SNR(dB) = 10\lg\left(P_{signal}/P_{noise}\right) =$$

$$= 10\ lg\left(P_{signal}\right) - 10\lg(P_{noise})$$

Для расчета P_{noise} и P_{signal} воспользуемся выражением 2.

Основные контрмеры могут быть разделены на два типа: процедурные и технические мероприятия.

Процедурные контрмеры включают в себя запрет на использование видеокамер в офисе, закрытие светодиодов, использование более инерционных ламп накаливания или энергосберегающих неоновых ламп, а также экранирование окон. Отдельно необходимо контролировать соблюдение введенных административных ограничений и регулярно их проверять.

Запрет на использование осветительных светодиодных ламп легко реализуется, но приводит к увеличению расходов на электроэнергию. Стоит отметить, что для организации офисных рабочих мест часто используются помещения типа «опен-эйр» которые подразумевают отделение рабочих мест только перегородками или использование стеклянных стен и перегородок все это позволяет камерам видеонаблюдения наблюдения полу-

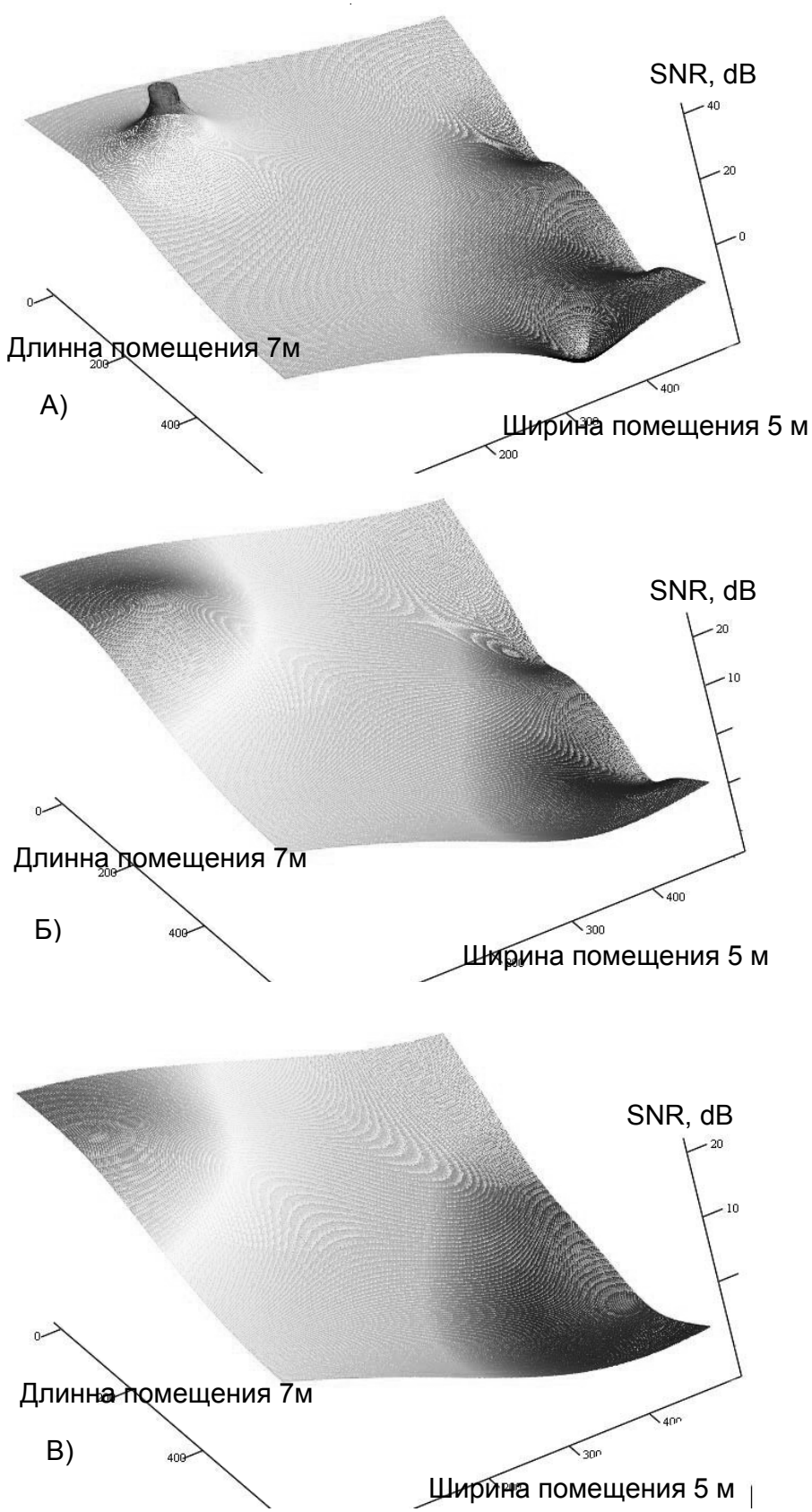

Рис. 2. Распределение отношения сигнал/шум в помещении для переговоров для высот:
А – 1.2 м, Б – 2 м, В – 2.7 м.

чать оптический сигнал от светодиодов осветительной техники и компьютеров. Следовательно, необходимо предусмотреть экранирование вычислительной техники от попадания в поле зрения систем видеонаблюдения [5–7].

Целесообразно использовать технические системы противодействия, включающие мониторинг состояния светодиодов с помощью программного или оптического метода. Обнаружение использование светодиодов для передачи сообщений внешними датчиками является идеальным методом, не сообщая злоумышленнику никакой информации о выполняемых мерах обеспечения защиты информации. Такой мониторинг является пассивный и не обнаруживаемый злоумышленником. Внешнее обнаружение передачи обычно по видимому свету весьма информативно, однако для высокой вероятности обнаружения необходимо знать частотный диапазон и вид модуляции и кодирования передаваемого сообщения. Стоит признать, что рассмотренные скрытые оптические каналы утечки информации относятся к маловероятным, но все же они остаются трудно обнаруживаемыми. Ситуация обусловлена мало изученностью технологии передачи информации по средствам модуляции видимого света и отсутствии официальных регламентов и оборудования и методик выявления и противодействия утечки информации по скрытым оптическим каналам по средствам модуляции видимого излучения светодиодов [8–12]. Таким образом, актуальным является угроза утечки акустической информации по средствам модуляции видимого света, и нуждается во всестороннем исследовании.

ЛИТЕРАТУРА

1. Зайцев А. П. Технические средства и методы защиты информации: Учебник для вузов / Зайцев А. П., Шелупанов А. А., Мещеряков Р. В. и др.; под ред. А. П. Зайцева и А. А. Шелупанова.— М.: ООО «Издательство Машиностроение», 2009–508 с.
2. Колебания и волны. Введение в акустику, радиофизику и оптику. Горелик Г. С. Издательство: Физико-математической литературы. 1959
3. Gary Davis, Ralph Jones. «Sound Reinforcement Handbook». Copyright 1987, 1989 Yamaha Corporation of America and Gary Davis & Associative.
4. ГОСТ 12.1.036–81 и СН 2.2.4/2.1.8.562–96 «Шум на рабочих местах, в помещениях жилых, общественных зданий и на территории жилой застройки».
5. ГОСТ Р 51275–99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. (Принят и введён в действие Постановлением Госстандарта России от 12 мая 1999 г. № 160).
6. Clark, L., and Algaier, W.E., Surveillance Detection, The Art of Prevention. Cradle Press LLC, 2007, 197 pp.
7. Управление информационной безопасностью, управление рисками [Текст]: монография / Швырев Б. А., Тимонов Д. А.— М., 2018.— 170 с.
8. Основные понятия национальной кибербезопасности государств, входящих в Северо-Атлантический альянс [Текст]: монография / Б. А. Швырев.— М., 2018.— 114 с.
9. Политические и стратегические цели национальной кибербезопасности [Текст]: монография / Б. А. Швырев.— М., 2018.— 131с.
10. "Comprehensive Summary of Modulation Techniques for LiFi | LiFi Research". www.lifi.eng.ed.ac.uk. Retrieved 2018–01–16.
11. Harald Haas. "Harald Haas: Wireless data from every light bulb". ted.com. Archived from the original on 8 June 2017.
12. "Archived copy". Archived from the original on 2 February 2016. Retrieved 2 February 2016.

Журнал «Современная наука: актуальные проблемы теории и практики»