

# КАНАЛ УТЕЧКИ АКУСТИЧЕСКОЙ ИНФОРМАЦИИ ПОСРЕДСТВОМ МОДУЛЯЦИИ ВИДИМОГО СВЕТА

*В статье рассматривается принципиальная возможность формирования канала утечки акустической информации посредством изменения параметров испускаемого светового потока светодиодными осветительными приборами под воздействием звуковых колебаний. Проводится обзор акустических каналов утечки информации для определения места рассматриваемого канала в существующих классификациях. Показано, что акустооптический канал по определению включает рассматриваемый в статье канал утечки и может быть дополнен каналом утечки посредством модуляции видимого света.*

*Ввиду частичного соответствия рассматриваемого канала утечки двум видам, имеющимся в сложившейся классификации каналов утечки акустической информации, – акустооптическому и акустоэлектрическому (параметрическому), и существования уточняющих отличий в использовании видимого некогерентного излучения, формируются предпосылки к уточнению классификации и добавлению в нее акустического канала утечки информации посредством модуляции видимого света.*

*Приводится определение рассматриваемого канала утечки. Его существование стало возможным с появлением малоинерционных осветительных полупроводниковых приборов. Научное подтверждение этого факта заключается в наличии коммуникационной технологии связи посредством модуляции видимого света, которая получила название Light Fidelity, или Li-Fi.*

*Исходя из анализа, автор отмечает важность исследований как технических, так и административных мер по противодействию утечки информации.*

**Ключевые слова:** акустический канал утечки информации, модуляция видимого света, Li-Fi.

Shvyrev B. A., Timonov D. A.

# ACOUSTIC INFORMATION LEAKAGE CHANNEL BY MEANS OF VISIBLE LIGHT MODULATION

*The article discusses the fundamental possibility of forming a leakage channel of acoustic information by means of changing the parameters of the emitted light flux by LED lighting devices, under the influence of sound vibrations. An overview of the acoustic channels of information leakage is conducted to determine the location of the channel in question in the existing classifications. It is shown that the acousto-optic channel, by definition, includes the leakage channel considered in the article and can be supplemented by a leakage channel by means of modulation of visible light.*

*In view of the partial correspondence of the leakage channel under consideration to two types existing in the current classification of leakage channels of acoustic information — acousto-optic and acoustoelectric (parametric), and having a clarifying difference in the use of visible non-coherent radiation creates prerequisites for clarifying the classification and adding in her acoustic channel information leakage by means of modulation of visible light.*

*The definition of the leakage channel in question is given. Its existence became possible with the advent of a little inertial semi-conductor lighting fixtures. Scientific confirmation of this fact lies in the existence of communication technology communication by means of modulation of visible light, which was called Light Fidelity or Li-Fi.*

*Based on the analysis, the author notes the importance of research, both technical and administrative measures to counter information leakage.*

**Keywords:** *acoustic channel of information leakage, modulation of visible light, Li-Fi.*

Защита информации – это сложная, многогранная проблема, решение которой требует привлечения комплекса организационных, технических, правовых и иных мер.

Для ее реализации создается соответствующая система защиты. Одним из основных принципов ее построения является системность, учитывающая все слабые и наиболее уязвимые места систем обработки (обсуждения) информации, а также характер, возможные объекты и направления атак на систему со стороны нарушителя, пути проникновения в распределенные системы и несанкционированные действия, примененные к информации, включая ее перехват по техническим каналам утечки.

Общеизвестно, что информация, как обрабатываемая средствами вычислительной техники, так и обсуждаемая, содержится в информативных сигналах. И в зависимости от вида источника их образования способом получения информации злоумышленником служат технические каналы утечки информации.

Все больший интерес с точки зрения образования каналов утечки информации представляют различные бытовые электронные приборы. Общей тенденцией в их развитии является использование высокочастотных беспроводных радиоинтерфейсов, а также сверхъярких светодиодов. Последние годы характеризуются интенсивным освоением оптического диапазона для передачи данных. Такая ситуация обусловлена высокой информационной емкостью светового поля как носителя информации, высокой скоростью передачи данных по информационным каналам и принципиальной легкостью осуществления математических операций с двумерными световыми полями. Одним из способов создания таких полей является модуляция видимого света, создаваемого яркими и свер-

хъяркими светодиодами осветительных приборов. Модуляция реализуется путем управления параметрами тока, протекающего через светодиод. Управление током осуществляет микроконтроллер.

Модуляция светового потока возникает за счет воздействия акустических колебаний, создаваемых преимущественно голосовым аппаратом человека на параметрические элементы микроконтроллера источника освещения, под воздействием которых они изменяют свои величины. Такое преобразование акустического сигнала в световой возможно при условии существования микрофонного эффекта в схеме контроллера светодиода или наличия миниатюрного микрофона в контроллере, выступающего как элемент закладки.

Рассмотрим существующие классификации акустических каналов для определения места расположения в них канала утечки посредством модуляции видимого света.

Акустический канал утечки речевой информации является одним из самых ранних способов несанкционированного доступа к звуковой информации. Так, звуковой сигнал может приниматься непосредственно ухом человека или с использованием различных инженерных устройств, позволяющих увеличить дальность приема звукового сигнала или выделить полезный сигнал на фоне помех или незначимых сигналов с другими угловыми координатами. Звуковые колебания, являясь продольной механической волной, распространяются в воздухе и жидкости. При этом скорость распространения имеет прямую зависимость от упругих свойств среды. В твердых телах, таких как строительные конструкции, помимо продольных, могут существовать поперечные звуковые волны, или волны сдвига. Оба типа волн одинаково хоро-

шо передают звук. Продольные волны распространяются всегда быстрее поперечных. По твердому телу могут распространяться поверхностные звуковые волны, поддерживаемые силой упругости.

Известны различные классификации акустического канала [1, 2]. По своей структуре акустический канал можно представить следующим образом (табл. 1).

Следующая классификация, представленная в таблице 2, выделяет каналы по количеству преобразований исходного звукового поля [5].

Акустический канал утечки по природе формирования передачи информации на значительное расстояние, состоящий из преобразованных акустических колебаний в электромагнитные волны различных диапа-

Таблица 1

**Структура акустического канала утечки**

Структура акустического канала утечки		
Источник акустического сигнала	Среда распространения акустического сигнала	Приемник акустического сигнала
Речь человека	Воздушное пространство	Микрофон
Технические и радиоэлектронные устройства звуковоспроизведения	Строительные конструкции (упругие среды)	Стетоскоп
Функциональные звуки механических и электронных узлов технических средств	Жидкости	Акселерометр
Функциональные звуки механических средств		Гидрофон
		Геофон

Акустическим каналом утечки информации можно назвать процесс естественного или искусственного происхождения передачи информации, первоначально находящейся в виде акустического сигнала, несанкционированной стороне. В зависимости от дальнейших трансформаций акустического сигнала и используемого физического принципа или диапазона электромагнитных волн различают следующие разновидности акустиче-

зонов, можно классифицировать как низкочастотного диапазона, радиодиапазона, сверхвысокочастотного диапазона, инфракрасного диапазона, оптического когерентного (лазерного) излучения. Использование исключительно механизма преобразования акустического первичного поля в вибрационный процесс обуславливает несравнимо малое расстояние передачи информации, что в предыдущей классификации не учитывалось.

Таблица 2

**Классификация акустических каналов утечки информации**

Акустические каналы утечки информации	
Одноканальные	Составные
Акустический (воздушный)	Акустоэлектрический
Гидроакустический	Акусто-электромагнитный
Вибрационный	Акустооптический (лазерный)
Микросейсмический	Параметрический
Виброакустический	

ского канала утечки информации: воздушный, акустоэлектрический, акусто-электромагнитный, виброакустический, параметрический радиоволновой, оптико-электронный, или лазерный, акустический инфракрасный [3, 4].

Таким образом, исходя из рассмотренных классификаций акустического канала видна эволюция развития технических средств, отраженная в выделении отдельных видов каналов утечки акустической информации в отдельные группы. Это обусловлено значитель-

ным заделом по каждой группе, выделенной в самостоятельную. Стоит отметить акустооптический канал, охватывающий исключительно единственный механизм преобразования акустического сигнала в видимый диапазон посредством переотражения лазерного луча от стеклянных и/или иных отражающих сред, находящихся под воздействием интересующего акустического поля. В данном виде не рассматривается модуляция видимого света как процесс, использующий некогерентное излучение осветительных приборов для передачи сообщений на большие расстояния, хотя преобразование видимого света современных ламп, основанных на использовании сверхъярких светодиодов, используется для передачи данных в компьютерных сетях.

Наличие в схеме управления осветительными диодами микроконтроллеров выявляет массив скрытых потенциальных угроз возникновения канала утечки посредством модуляции видимого света от светодиодных осветительных приборов. Механизмы модуляции видимого света могут быть как естественного происхождения, за счет возникновения микрофонного эффекта из-за использования как минимум конденсаторов в схеме управления, так и искусственного, за счет сознательного размещения в контроллере микрофонов высокой чувствительности.

Стоит отметить, что применение специальной аппаратуры приема промодулированного светового сигнала и последующего детектирования, цифровой обработки и выделения полезного сигнала обеспечивает формирование канала утечки информации, по своим физическим свойствам схожего с акустоэлектрическим (параметрическим) в видимом диапазоне электромагнитного излучения каналом утечки речевой информации, а по используемому диапазону – с акустооптическим каналом.

Ввиду частичного соответствия рассматриваемого канала утечки двум видам, существующим в сложившейся классификации каналов утечки акустической информации, – акустооптическому и акустоэлектрическому (параметрическому), и с учетом уточняющего отличия в использовании видимого некогерентного излучения, создаются предпосылки к внесению соответствующих поправок в классификацию и добавлению в нее акустического канала утечки информации посредством модуляции видимого света. В настоящий момент можно сформулировать опреде-

ление рассматриваемого канала следующим образом: акустический канал утечки информации посредством модуляции видимого света — это канал передачи акустической информации несанкционированной стороне посредством изменения яркости и длительности свечения светодиодных источников света или модуляции излучения в оптическом диапазоне электромагнитных волн.

Существование такого канала утечки стало возможным с появлением малоинерционных осветительных приборов, основным световым элементом которых являются яркие и сверхъяркие светодиоды. Научное подтверждение этого факта заключается в существовании коммуникационной технологии связи посредством модуляции видимого света, которая получила название Light Fidelity, или Li-Fi [6]. Термин «Li-Fi» был предложен профессором Харальдом Хаасом [7] на конференции TED Global Talk 2011 года, где он представил идею «беспроводных данных из каждого источника» [8]. Технологию, которая использует среду передачи во многом подобно Wi-Fi, относят к классу коммуникаций в видимом спектре света. Для организации передачи данных используются обычные осветительные светодиоды. Белый свет светодиодов может формироваться излучателями различных диапазонов частот видимого спектра. Существуют тетрахроматические, дихроматические и трихроматические светодиодные источники, используемые для генерации белого света [9]. Наиболее часто применяются в осветительных приборах светодиоды на основе люминофора. Тетрахроматические и трихроматические светодиодные источники обладают несравнимо большей полосой пропускания, сложностью реализации модуляции и небольшой дальностью передачи сообщений [9,10].

Для передачи бинарных данных достаточно включать и выключать светодиод, тем самым кодируя информацию на физическом уровне. При уменьшении интервала переключений до 1 мкс человек не заметит мерцания, а возможность переключения между режимами с разной яркостью потенциально увеличивает пропускную способность. Передаваемая информация может кодироваться разными режимами включения/выключения светодиода. В аппаратуре приема сигнала используется чувствительный фотодиод, который путем прямого детектирования преобразует видимый сигнал. Сигнал с фотоприем-

ника поступает на устройство декодирования и обработки, позволяющее сформировать передаваемое сообщение.

Формирование канала утечки информации посредством видимого света включает установку устройства преобразователя акустического сигнала в изменение интенсивности яркости светодиода, которое реализуется в контроллере светодиода. Кроме того, целесообразно использовать оптические системы, позволяющие наблюдать за изменением светимости или яркости доступных для наблюдения участков контролируемых помещений, и высокочувствительный фотоприемник. Такими участками могут быть окна, щели дверных проемов, открытые окна и фрамуги и непосредственно сам светодиод. Способом использования световых волн для перехвата информации также является такая их особенность распространения, как вторичная, или отраженная,

светимость. Дальность перехвата видимого оптического сигнала ограничивается только светосилой оптических систем наблюдения и может быть сколь угодно большой.

Канал утечки акустической информации посредством модуляции видимого света является сравнительно новым каналом утечки и в настоящее время недостаточно освещен в литературе, что определяет актуальность исследования. Также возникает необходимость проработки как технических, так и административных мер по противодействию утечки информации. Как в отечественной доктрине информационной безопасности, так и стратегиях развития кибербезопасности иностранных государств отмечается важность своевременного реагирования на новые виды угроз и предупредительной разработки комплекса мер, направленных на их нейтрализацию и уменьшение возможных потерь [11–14].

---

## Литература

1. Садовская Т.Г., Хорев А.А. Средства и методы обеспечения безопасности бизнеса. Технические каналы утечки информации: учеб. пособие. – М.: Изд. МГТУ им. Н.Э.Баумана, 2009. – 80 с.
2. Хорев А.А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации: учеб. пособие. – М.: Гостехкомиссия РФ, 1998. – 320 с.
3. 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.
4. Хорев А.А. Способы и средства защиты информации: учеб. пособие. – М.: МО РФ, 1998. – 316 с.
5. Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3-х т. Т. 1. Технические каналы утечки информации. – М.: НИЦ «Аналитика», 2008. – 436 с.
6. «Comprehensive Summary of Modulation Techniques for LiFi. LiFi Research». [www.lifi.eng.ed.ac.uk](http://www.lifi.eng.ed.ac.uk). Retrieved 2018-01-16.
7. Harald Haas. «Harald Haas: Wireless data from every light bulb». [ted.com](http://ted.com). Archived from the original on 8 June 2017.
8. «Archived copy». Archived from the original on 2 February 2016. Retrieved 2 February 2016.
9. E.F. Schubert, T. Gessmann, J.K. Kim. Light Emitting Diodes, Wiley Online Library, 2005.
10. A. Zukauskas, M.S. Shur, R. Gaska. Introduction to Solid-state Lighting, J. Wiley, United States, 2002.
11. Указ Президента РФ от 05.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СЗ РФ. – 2016. – №50. – Ст. 7074.
12. Управление информационной безопасностью, управление рисками [Текст]: монография / Б.А. Швырев, Д.А. Тимонов. – М., 2018. – 170 с.
13. Основные понятия национальной кибербезопасности государств, входящих в Северо-Атлантический альянс [Текст]: монография / Б.А. Швырев. – М., 2018. – 114 с.
14. Политические и стратегические цели национальной кибербезопасности [Текст]: монография / Б.А. Швырев. – М., 2018. – 131 с.

## References

1. Sadovskaya T.G., Horev A.A. Sredstva i metody obespecheniya bezopasno-sti biznesa. Tekhnicheskie kanaly utechki informacii: ucheb. Posobie [Means and methods to ensure business safety. Technical channels of information leakage: studies. allowance]. – М.: Izd. MGTU im. N.EH.Baumana, 2009. – 80 p.
2. Horev A.A. Zashchita informacii ot utechki po tekhnicheskim kanalam. CHast' 1. Tekhnicheskie kanaly utechki informacii: ucheb. posobie [Protection of information from leakage through technical channels. Part

1. Technical channels of information leakage: studies. allowance]. – M.: Gostekh-komissiya RF [Gostekh-Commission of the Russian Federation], 1998. – 320 p.

3. Tekhnicheskie sredstva i metody zashchity informacii: Uchebnik dlya vuzov [Technical means and methods of information protection: A textbook for universities] / Zajcev A.P., Shelupanov A.A., Meshcheryakov R.V. i dr.; pod red. A.P. Zajceva i A.A. Shelupanova. – M.: ООО «Izdatel'stvo Mashinostroenie» [«Publishing Mashinostroenie»], 2009/ – 508 p.

4. Horev A.A. Sposoby i sredstva zashchity informacii: ucheb. posobie [Methods and means of information protection: studies. allowance]. – M.: MO RF, 1998. – 316 p.

5. Horev A.A. Tekhnicheskaya zashchita informacii: ucheb, posobie dlya studentov vuzov. V 3-h t. T. 1. Tekhnicheskie kanaly utechki informacii [Technical protection of information: studies, a manual for students of universities. In 3 tons. T. 1. Technical channels of information leakage] - M.: NIC «Analitika», 2008. – 436 p.

6. "Comprehensive Summary of Modulation Techniques for LiFi. LiFi Re-search". [www.lifi.eng.ed.ac.uk](http://www.lifi.eng.ed.ac.uk). Retrieved 2018-01-16.

7. Harald Haas. "Harald Haas: Wireless data from every light bulb". [ted.com](http://ted.com). Archived from the original on 8 June 2017.

8. "Archived copy". Archived from the original on 2 February 2016. Retrieved 2 February 2016.

9. E.F. Schubert, T. Gessmann, J.K. Kim, Light Emitting Diodes, Wiley Online Library, 2005.

10. A. Zukauskas, M.S. Shur, R. Gaska, Introduction to Solid-state Lighting, J. Wiley, United States, 2002.

11. Ukaz Prezidenta RF [[Presidential Decree] ot 05.12.2016 g. №646 «Ob utverzhdenii Doktriny informacionnoj bezopasnosti Rossijskoj Federacii» [«On approval of the Information Security Doctrine of the Russian Federation»] // SZ RF. 2016. №50. St. 7074

12. Upravlenie informacionnoj bezopasnost'yu, upravlenie riskami [Information security management, risk management]: monografiya [monograph] / Shvyrev B.A., Timonov D.A. – M., 2018. – 170 p.

13. Osnovnye ponyatiya nacional'noj kiberbezopasnosti gosudarstv, vho-dyashchih v Severo-Atlanticheskij al'yans [Basic concepts of national cyber security of the states included in the North Atlantic Alliance]: monografiya [monograph] / B.A. Shvyrev. – M., 2018. – 114 p.

14. Politicheskie i strategicheskie celi nacional'noj kiberbezopasnosti [Political and strategic goals of national cybersecurity]: monografiya [monograph] / B.A. Shvyrev. – M., 2018. – 131 p.

---

**ШВЫРЕВ Борис Анатольевич**, кандидат физико-математических наук, ведущий научный сотрудник Федерального казенного учреждения «Научно-исследовательский институт Федеральной службы исполнения наказаний». 125130, Российская Федерация, г. Москва, ул. Нарвская, д. 15а, стр. 1. E-mail: bor2275@yandex.ru

**ТИМОНОВ Дмитрий Александрович**, начальник лаборатории Научно-исследовательского центра Краснодарского высшего военного училища имени генерала армии С.М. Штеменко. 350063, Российская Федерация, г. Краснодар, ул. Красина, дом 4. E-mail: dmitrii-timonov@bk.ru

**SHVYREV Boris**, Russian Federation, Moscow, Research Institute of the Federal Penitentiary Service of Russia, Leading Researcher, Candidate of Physical and Mathematical Sciences. Bld. 15a, p. 1, Narvskaya Str., Moscow, 125130. E-mail: bor2275@yandex.ru

**TIMONOV Dmitry**, Russian Federation, Krasnodar, the head of laboratory of The research center of Krasnodar higher military school of the General of army S. M. Shtemenko. Bld. 4, Krasina Str., Krasnodar, 350063. E-mail: dmitrii-timonov@bk.ru