**References**

1. Eliseev S.N., Pesotsky P.V. Model radiokanala dlja peredachi soobszheniy visokoskorostnih transportnih sredstv [Model of radiochannel for transmission messages of high-speed vehickles] *Shkola universitetskoy nauki: Paradigma razvitija,* June 2015, vol. 16, no. 2, pp. 142-148.
2. Alimohammad A., Fard S.F., Cockburn B.F. Accurate Simulation of Nonisotropic Fading Channels with Arbitrary Temporal Correlation. *IET Communications*, vol. 6, no. 5, 2012, pp. 557-564. doi: 10.1049/iet-com.2011.0082.
3. Gerasimov A.B. et al. *Polunaturnoe modelirovanie radiotehnicheskih system* [Seminatural simulation of radio systems]. Jaroslavl, JarGU Publ., 2014. 128 p.
4. Abdi A., Barger J.F., Kaveh M. A parametric model for the distribution of the angle of arrival and associated correlation function and power spectrum at the mobile station. *IEEE Trans. on Vehicular Technology,* 2002, vol. 51, no. 3, pp. 425-434. doi: 10.1109/TVT.2002.1002493.
5. Bellanger M.G. *Traitement numerique du signal. 8-e edition*. DUNOD, 2006. 447 p. (In French).
6. Selesnick I.W., Lang M., Burrus C.S. Magnitude squared design of recursive filters with the Chebyshev norm using a constrained rational Remez algorithm. *Proceeding of the sixth IEEE DSP Workshop,* p. 23-26, Yosemit, CA, October 1994. doi: 10.1109/DSP.1994.379882.
7. Baraboshin A. Ju., Luchin D.V., Maslov E.N. Tehnologija razrabotki sredstv peredachi dannih po radiokanalam razlichnih diapazonov. [Technjlogy of data transmission means development for radio channels of difftrent rangts]. *Electrosvjaz*, 2015, no. 8, pp. 16-24.
8. Rappaport T.S. *Wireless Communications-Principles and Practice*. Prentice Hall PTR, 2002. 641 p.
9. Clarke R.H. A statistical theory of mobile-radio reception. BSTJ, 1968, vol. 47, pp. 957-1000.

*Received 18.11.2015*

# ЭЛЕКТРОМАГНИТНАЯ СОВМЕСТИМОСТЬ И БЕЗОПАСНОСТЬ ОБОРУДОВАНИЯ

УДК 519-7; 004.56

## ИСПОЛЬЗОВАНИЕ МУЗЫКАЛЬНЫХ ТЕКСТОВ И ТРАНСЛЯЦИИ МУЗЫКАЛЬНЫХ ПРОИЗВЕДЕНИЙ ДЛЯ ПЕРЕДАЧИ ШИФРОВАННЫХ СОБЩЕНИЙ

*Гросс А.А.*
*Заочный университет в г. Хаген, Германия*
*E mail: anastasia.gross@mail.ru*

В статье приведены примеры применения приемов криптографии и стеганографии на музыкальных текстах, описаны некоторые ограничения этих методов. Описаны методы сокрытия информации, известные из зарубежной литературы, и предложен метод, который позволяет предварительно определить наличие в музыкальном произведении некоторых видов шифров. Представлены инструкция для дешифровки и шаги, которые необходимо предпринять для того, чтобы не только взламывать, но и создавать шифры на основе известных методов.

***Ключевые слова:*** криптография, стеганография, музыка.

### Введение

Криптология объединяет криптографию и криптоанализ, то есть способы преобразования информации, для того чтобы сделать ее недоступной для нежелательных лиц и процесс ее взлома при помощи специальных методов [1]. Часто определение научной дисциплины разнится в обиходе специалистов и в обыденном сознании. Так, в обыденном сознании слово «расшифровка» тождественно пониманию чего-то загадочного, например расшифровка древних иероглифов. Но расшифровка не тождественна угадыванию. Это процесс обратного преобразования информации при использовании определенного алгоритма или их комбинаций.

Преобразование информации, представленной в виде букв и цифр, хорошо известно на протяжении исторического периода. Использование музыкальных текстов и исполнения музыкальных произведений для этой цели менее распространено. Между тем математика в историческом плане теснее связана с музыкой, чем кажется на

первый взгляд. Во-первых, долгое время математика и музыка считались в Европе двумя из семи свободных искусств. В Средние века, а подробное описание практических примеров мы с них и начнем, в университетах было четыре факультета, три высших и один дополнительный – факультет искусств. На нем можно было обучаться отдельно, но обязательно было окончить его, чтобы поступить на любой высший: юридический, медицинский или теологический, который был самым престижным.

Факультет искусств содержал в начальной ступени обучения «тривиум», от слова «три»: грамматику, диалектику (в то время так называлась логика) и риторику. Отсюда и происходит слово «тривиальный» – синоним общеизвестного. Затем шел «квадривиум» который включал: арифметику, геометрию, астрономию и музыку. Предметы тривиума и квадривиума и составляли семь свободных искусств.

В наше время музыкальное и математическое образование в России разошлись, хотя в Европе они до сих пор достаточно связаны. И это объясняет существенно большее количество источников, которые описывают использование музыкальных текстов или исполнение музыки вживую для передачи и сохранения скрытой информации, чем в России. В то же время это открывает новые возможности перед отечественными учеными.

## Возможности криптологии и стеганографии в музыке

Для того чтобы обсуждать связь музыки и криптологии, нужно отметить, что криптография стала возможной с возникновением письменности. Письменность музыки в том виде, в каком мы привыкли ею пользоваться, возникла не сразу – ярким примером связи музыки и теологии в средневековом сознании является предложенное Гвидо Аретинским название нот. Религиозное, символическое в искусстве того времени и заложило основу, на наш взгляд, для развития возможности использования криптографических методов в музыке. Пока не было полноценного музыкального языка, то есть письменного обозначения нот, не было и возможности их заменять и переставлять. Хотя возможность для сокрытия информации в живом исполнении оставалась.

Для более простого разучивания песнопений, например, средневековый монах Гвидо Аретинский, живший в IX-X веках нашей эры, вводил первые слоги молитвы к Иоанну Крестителю на латинском языке для обозначения высоты. Вот текст этой молитвы: «Ut (queant laxis), Re (-sonare firbis), Mi (-ra gestorum, Fa (-multi tuorum), Sol (-ve polluti), La (-bii reatum), a Si (Sankte Ioannes) – это инициалы Святого Иоанна. Первый слог «Ut» в силу своего глухого звучания не прижился и был заменен на более звонкое «Do». Хотя данная замена произведена не во всех странах [2].

Обратимся к статистике, чтобы понять, кто мог быть заинтересован в развитии музыкальной криптографии и кто мог ею тогда пользоваться. Среди обычных граждан музыкально образованных людей было крайне мало. О том, кто, кроме представителей духовенства, мог пользоваться подобными практиками, свидетельствуют данные о количестве светских музыкально образованных людей. Например, в средневековом Париже, согласно документам о сборе налогов, проживало от 20 до 60 тыс. человек. Из них музыкантами (возможно, также мастерами по изготовлению музыкальных инструментов) в разные годы были: в 1292 г. – 19 из 15000, в 1296 г. – 12 или 13 из 6000, в 1297 г. – 22 или 23 из 10000, а в 1313 г. – 11 из 6000 [3]. Поскольку каждое явление возникает благодаря объективным возможностям, то есть средствам и технологиям, но и, что не менее важно, по социальному запросу – нужно учитывать, важно ли это явление для общества в целом или для каких-то групп людей. О том, какие в те времена существовали средства и условия, рассказывает история, но она создается субъективно, в зависимости от выбора ученых – современников описываемых явлений, которые решают, что важно, с их точки зрения, а что неважно.

Три ключевые фигуры в Европе, которые относятся к рассматриваемой теме: Иоганн Тритемий, Афанасий Кирхер и Гаспар Шотт. Каждый из них жил или работал одно время в Баварии, точнее, в Нижней Франконии. В Бамберге наряду с Ватиканом и Авиньоном одно время находился Папский двор. Аббат Тритемий живший с 1 февраля 1462 г. по 15 декабря 1516 г., издал первую книгу по криптографии, замаскировав ее под оккультный труд, и поэтому она долгое время была запрещена. Гаспар Шотт написал книгу о стеганографии, Афанасий Кирхер преподавал философию и восточные языки в Вюрцбурге, столице Нижней Франконии, он описал теорию аффектов в музыке. Эта теория была уже неким подобием кодирования, где имело место соответствие одного символа другому. При этом речь шла не

просто о передаче впечатления, а об алгоритмах целенаправленной фиксации аффектов, поддающейся повторяемости, что, по большому счету, уже предполагает естественно-научный подход и «подключение» математики.

Шифр отличается от кода тем, что код – это система соответствия одних символов другим (яркий пример – азбука Морзе), и таблица соответствия известна. Если таблица соответствия неизвестна, то это шифр простой замены, а таблица – ключ. Два основных метода криптографии – это перестановка и замена, и то, что именно на что заменено и по какому принципу переставлено, – определяют ключи.

Насколько можно перенести алгоритмы, известные из истории для букв и цифр, на музыкальные тексты и исполнение? Если средства криптографии универсальны? А система нотной записи тоже знаковая система. Здесь существуют две проблемы. С точки зрения надежности коммуникации и с точки зрения классической науки:

- обеспечить незаметность для постороннего глаза;
- соблюсти при шифровании законы музыкальной гармонии.

Если нужно передать сообщение незаметно для чужих глаз, можно заменить буквы на ноты по любому произвольно выбранному признаку. Это впервые было сделано Гаспаром Шоттом в 1665 г. в книге «Школа стеганографии» [4]. Шотт располагает 11 тонов по возрастающей соответственно первым одиннадцати буквам латинского алфавита; следующие 11 по нисходящей, но другой длительности и последние две буквы снова вверх, не совпадающими по длительности с первыми двумя [4]. В другом варианте он делит алфавит пополам, но придерживается того же принципа [4].

Отметим, что в ряде случаев музыкальный текст при этом не будет соответствовать законам музыкальной гармонии. Второй момент – это необходимость не только применить средства криптографии, но и написать полноценное музыкальное произведение, то есть соблюсти законы гармонии. Здесь опять проявляет себя связь музыки и математики: в VI веке Кассиодор дал такое определение музыке: «Музыка – это наука, рассматривающая числа относительно явлений, наблюдаемых в музыке».

С похожей проблемой столкнулись ученые, когда возникла идея писать машинную музыку. В XX веке в Нью-Йорке было перехвачено сообщение, содержащее информацию нелегального тотализатора: ноты заменяли там буквы в произвольном порядке, и человеку, знакомому с музыкальной грамотой, сразу было понятно, что здесь «что-то не так» [5].

Напомним, что английская криптографическая служба во время Второй мировой войны принимала на службу только людей, знакомых с нотной грамотой, способных читать партитуры [6]. Им была известна также высокая корреляция между умением разгадывать загадки и музыкальными способностями специалистов.

Обратимся к еще одному методу тайной передачи сообщений – стеганографии, которая, как известно, позволяет скрыть сам факт передачи сообщения. Естественно, стеганография часто применяется совместно с криптографией, то есть сначала сообщение зашифровывается, а потом «прячется». Существуют приемы стеганографии, которые можно применить к нотной записи, если она уже соответствующим образом написана, то есть несет дополнительную информацию. Например, можно спрятать мелодию, которая уже была создана при помощи определенного алгоритма, скрывающего информацию, на рисунке. На изображении можно разместить пейзаж, а на переднем плане – плетень с лианой, цветы которой изображают ноты. При этом поперечные перекладины изгороди могут даже представлять собой такты.

Такой пример для передачи текстового сообщения при помощи азбуки Морзе описан у Шмеха. На открытке стебли и цветы тростника представляют точки и тире. Музыкальная стеганография существует в записи, а также в реальном времени, что сокращает временные возможности для перехвата и передачи информации третьим лицам [7].

Методы стеганографии изначально разработаны и используются для работы с изображениями. Однако исследователи данной области начали изучать использование данных методик для работы со звуком. Как следствие, были найдены некоторые алгоритмы для аудиостеганографии. Некоторые примеры из них описаны в [8].

Учитывая большую долю использования многозначных символов культуры Европы Средних веков и эпохи Возрождения, а также небольшие по объему исследования математическими методами музыкальных текстов, возникает идея провести исследование с помощью соответствующего программного обеспечения.

Музыкальные произведения исследовались статистическими методами в середине XX века для того, чтобы научиться создавать машинную музыку, – при этом было задано, что разброс по высоте между двумя близлежащими нотами не должен превышать шесть пунктов [9].

Учитывая тот факт, что многие монашеские ордена вынуждены были соблюдать конфиденциальную переписку, а музыкальное образование было доступно немногим светским лицам, вероятна возможность, что они прятали информацию в ноты для богослужений одним из вышеописанных способов. Так как самым простым предварительным способом узнать, содержит ли произведение какой-либо шифр на основе лингвистических единиц, является частотный анализ, то имеет смысл проанализировать доступный нам сегодня нотный материал сначала таким способом, а потом по всем известным из литературы ключам.

Суть частотного анализа заключается в том, что встречаемость отдельных букв в каждом языке разная, и в случае применения шифра простой замены это должно быть обнаружено программными средствами. На первом этапе планируется произвести распознавание музыкального текста из файлов формата TIFF или JPEG с помощью программы Sharp Eye 2, а затем при помощи программы, разработанной С.Г. Дробышевым, обработать таким образом сравнительно большой объем произведений, написанных духовными лицами того времени. Предварительный результат будет представлять гистограмма, где по оси абсцисс показаны порядковые номера нот, их длительности, буквенные обозначения и к какой октаве они относятся, а по оси ординат – встречаемость их в процентах в пределах анализируемого произведения.

Поскольку способы написания нот различались в разные исторические периоды, некоторые рукописи следует вводить в программу от руки или создавать программное обеспечение, которое сможет распознавать нотные шрифты, отличные от современных. Если не удастся найти шифры в музыкальных произведениях, то всегда остается возможность применения тех же алгоритмов для зашифровки сообщений – то есть найти принцип замены букв нотами, который не будет нарушать законы музыкальной гармонии. Интересно применить к музыке известные из истории алгоритмы шифрования программными методами. Таким образом, можно будет создавать песни, где музыка, во-первых, не будет вызывать подозрений, а во-вторых практически невозможно будет проанализировать при перехвате такой объем, который передается в сети Internet и через другие средства массовой информации.

## Литература


1. Connette S. Geheimschriften in der Elementarstufe unter besonderer Beruecksichtigung des genetischen Prinzips. Wissenschaftliche Hausarbeit. Paedagogische Hochschule Karlsruhe, 2009. – 204 p.
2. Pahlen K. Die grosse Geschichte der Musik in Zusammenarbeit mit Rosemarie Koenig. Paul List Verlag GmbH& Co KG. Muenchen. 1996. – 704 p.
3. Europaeische Musikgeschichte. Band 1. Hrsg. Sabine. Ehrmann-Herfort, Ludwig Fischer, Giselher Schubert. Baerenreiter-Verlag, 2002. – 688 p.
4. Gaspar Schott. Schola steganographica, 1665. The information hiding homepage // http://www.petitcolas.net/steganography/steganographica/ (accessed 7.09.2015)
5. Schmeh K. Versteckte Botschaften. Die faszinierende Geschichte der Steganografie. Heise Zeitschriften Verlag GmbH & Co KG, Hannover., 2009. – 246 p.
6. Interlude. Maureen Buja. Spies and Music // http://www.interlude.hk/front/spies-and-music/ (accessed 18.01.2016)
7. Hutchinson, Latia. Live Musical Steganography. (2014). Senior Theses. Paper 20. – 16 p.
8. Mohammed Salem Atoum, Subariah Ibrahim, Ghazali Sulong and Ali M-Ahmad. MP3 Steganography: Review IJCSI International Journal of Computer Science Issues, November 2012Vol. 9, Issue 6, No 3, 9. – P. 236-244.
9. Пекелис В.Д. Маленькая энциклопедия о большой кибернетике. М.: Детская литература, 1973. – 415 с.


*Получено 15.01.2015*

**Гросс Анастасия Александровна**, студентка магистратуры Заочного университета в г. Хаген, Германия. Тел. +7 968 730 9884. E -mail: anastasia.gross@mail.ru

## APPLICATION OF MUSICAL TEXTS AND MUSIC BROADCASTING FOR TRANSMISSION OF ENCRYPTED MESSAGE

*Gross A.A.*
*University of Hagen, 58084 Hagen, Germany*
*E- mail: anastasia.gross@mail.ru*

Safe transfer of confidential information was required through the all history of humanity. Here encryption and steganography are basic methods. Examples of data transmission by using of images containing hidden signs as well as letters or numbers are well known and described in various publications. Another method is data transmission and storage by using steganography, cryptography and their combinations over music texts. Some examples of music text steganography and cryptography application describe limitations of the method. We considered some methods for information encryption known from foreign historical literature and proposed method that provide to predetermine a presence of music in some types of scripts. This work presents manuals for decoding and hacking as well as design scripts with a help of known methods.

***Keywords:*** cryptography, steganography, music.

**DOI:** 10.18469/ikt.2016.14.1.14

**Gross Anastasia Aleksandrovna**, University of Hagen, 58084 Hagen, Germany; Master Student. Tel. +79687309884. E-mail: anastasia.gross@mail.ru

**References**

1. Sebastian Connette. *Geheimschriften in der Elementarstufe unter besonderer Beruecksichtigung des genetischen Prinzips*. Wissenschaftliche Hausarbeit. Paedagogische Hochschule Karlsruhe. 2009. 204 p. (In German).
2. Pahlen K. *Die grosse Geschichte der Musik in Zusammenarbeit mit Rosemarie Koenig*. Paul List Verlag GmbH& Co KG. Muenchen. 1996. 704 p. (In German).
3. Sabine Ehrmann-Herfort, Ludwig Fischer, Giselher Schubert. *Europaeische Musikgeschichte. Band 1. Hrsg*. Baerenreiter-Verlag, 2002. 688 p. (In German).
4. Gaspar Schott. *Schola steganographica*, 1665. The information hiding homepage. Available at: http://www.petitcolas.net/steganography/steganographica/ (accessed 7.09.2015).
5. Schmeh K. Versteckte Botschaften. *Die faszinierende Geschichte der Steganografie*. Heise Zeitschriften Verlag GmbH & Co KG, Hannover, 2009. 246 p.
6. Maureen Buja. *Interlude. Spies and Music*. Available at: http://www.interlude.hk/front/spies-and-music/ (accessed 18.01.2016).
7. Hutchinson, Latia. *Live Musical Steganography. Senior Theses. Paper 20*, 2014. 16 p.
8. Mohammed Salem Atoum, Subariah Ibrahim, Ghazali Sulong and Ali M-Ahmad. MP3 Steganography. *Review IJCSI International Journal of Computer Science Issues*, 2012, vol. 9, Issue 6, no. 3, 9. pp. 236-244.
9. Pekelis V.D. *Malen'kaya entsiklopediya o bol'shoy kibernetike* [Little Encyclopedia of big cybernetics]. Moscow, Detskaya literature Publ., 1973. 415 p.

*Received 15.01.2015*

# УПРАВЛЕНИЕ И ПОДГОТОВКА КАДРОВ ДЛЯ ОТРАСЛИ ИНФОКОММУНИКАЦИЙ

УДК 378.111

## ИННОВАЦИОННОЕ РАЗВИТИЕ ВУЗА. ИНТЕРСУБЪЕКТИВНОЕ УПРАВЛЕНИЕ

*Моисеева Т.В.*
*Институт проблем управления сложными системами РАН, Самара, РФ*
*E-mail: mtv-2002@yandex.ru*

Инновационное развитие вуза – предмет внимательного изучения сегодня. В связи с тем, что нет четкого понимания, что это такое и какие формы управления возможны (кроме традиционных иерархических), управление инновационным развитием вузов буксует. XXI век – время вхождения в постнеклассическую научную рациональность, заставляющую ориентироваться на субъектный, а не объектный подход к управлению. Принципы «идеальной» бюрокра-