УДК 003.26.09

ИСТОРИЯ КРИПТОГРАФИИ И НОВЫЙ ЭТИЧЕСКИЙ СТАТУС ИНФОРМАЦИИ

Фикс Александр Сергеевич,
*магистрант, Институт романо-германских языков,
информационных и гуманитарных технологий,
ФГБОУ ВПО «Пятигорский государственный
лингвистический университет», Пятигорск, Россия⁴*

1alsefi@gmail.com

Аннотация. История криптографии насчитывает несколько тысяч лет и неразрывно связана с историей человечества. Век за веком шифрование информации становилось актуальным в различных сферах человеческого бытия: от сферы сакрального до сферы бытового. Развитие криптографии и области ее применения обусловлены развитием коммуникационных средств. Широкая доступность телекоммуникационных средств изменила ценность информации, делая ее сверхценной, одновременно повышая значимость криптографических решений. В данной статье автор рассматривает историю развития криптографии и повлиявшие на этот процесс факторы. Особое внимание уделяется анализу причин изменения ценности информации, а также описанию проблемных областей информационного общества в свете последних событий. Главным фактором, сказавшимся, по мнению автора, на понимании роли криптографии, стали события 2013 года.

Ключевые слова: Интернет; информационное общество; криптография; история криптографии; этика; информационная этика.

THE HISTORY OF CRYPTOGRAPHY AND NEW ETHIC STATUS OF INFORMATION

Fix Alexander S.,
*undergraduate student of Institute of Roman and Germanic
Languages, Information and Humanitarian Technologies,
Pyatigorsk State Linguistic University, Pyatigorsk, Russia,*

1alsefi@gmail.com

⁴ Научный руководитель: Барышников П.Н., канд. филос. наук, доцент, ФГБОУ ВПО «Пятигорский государственный лингвистический университет», pnbaryshnikov@pglu.ru.

Abstract. Over a period of several thousand years the history of cryptography evolved synchronous to the evolution of mankind. Century after century, encryption of the information became relevant in various spheres of human existence: from the sphere of the sacred to the domestic sphere. The progress of the cryptography and its application due to the development of communication tools. The wide availability of telecommunication facilities has changed the value of the information, making it overvalued, at the same time, increasing the importance of cryptographic solutions. In this article, the author examines the history of cryptography, as well as the factors, which influenced on its progress. Special attention is paid to the analysis of the causes of changes of the informational value, as well as description of the problem areas of the information society in view of recent events. On the author's opinion, the main factor that influenced on the understanding of the role of cryptography, were the events of 2013.

Keywords: Internet, information-oriented society, cryptography, history of cryptography, ethics, information ethics

Изменение парадигмы применения криптограммы вызвано многими факторами, однако главенствующую роль сыграло изменение онтологического статуса информации [1]. Данная статья условно состоит из двух частей: исторической и актуальной. Мы постараемся в диахронии проследить эволюцию применения различных криптографических решений, а также попытаемся объяснить обусловленность таких изменений и рассмотрим причины, по которым криптография приобрела особое значение. «История криптографии вызывает интерес именно сейчас, в век информационного общества, когда информация становится сверхценной», – утверждают специалисты [2: 10]. Актуальные события требуют особого философского осмысления.

Вероятно, доподлинно мы никогда не узнаем, когда впервые человека посетила мысль о необходимости сокрытия информации, однако здесь впору вспомнить слова каплуна – героя одного произведения Вольтера: «...слова даны людям, чтобы скрывать подлинные мысли» [3: 455]. Однозначно можно утверждать лишь то, что потребность в криптографии появилась примерно в одно время с возникновением письма.

Самым древним свидетельством применения шифрования служит древнеегипетский папирус, в котором перечисляются мо-

нументы, созданные при фараоне Аменемхете II. Вероятно, автор манускрипта старался не скрыть смысл текста или затруднить его восприятие, а сделать текст экспрессивнее, воспользовавшись «одним из существенных элементов шифрования – умышленным преобразованием письменных символов» [4: 12].

Известный пример шифрования – атбаш, который является простым шифром подстановки для иврита, основанным на сдвиге алфавита на всю свою длину. Известен пример криптограммы из Библии, где под именем Сесах скрывалось имя царя Вавилона (Иер. 25:26).

Другим примером шифрования является скитала – шифр Древней Спарты, состоящий из цилиндра и полоски пергамента, которая обвивает цилиндр по спирали. На пергамент наносилось сообщение по длине цилиндра; если строка была заполнена, то сообщение продолжали писать на следующей строке до тех пор, пока не заканчивался текст сообщения или доступный объем цилиндра, после чего цилиндр вынимался, а полоска пергамента передавалась адресату. Адресат для прочтения должен был использовать цилиндр того же диаметра.

Диск Энея – устройство, созданное Энеем Тактиком в IV веке до н.э., – представляет собой диск, в котором проделаны отверстия по количеству букв алфавита, а в центре прикрепляется катушка с нитью. Для кодирования сообщения нить продевается поочередно в каждое отверстие, соответствующее букве. Эней Тактик описал еще один способ передачи тайны – книжный шифр, однако он относится к стеганографии.

Мартин Хайдеггер писал: «тайна только тогда тайна, когда не выходит наружу даже то, что тайна есть» [5]. Данная цитата очень точно и емко отображает суть стеганографии – науки о скрытой передаче информации при сохранении в тайне самого акта передачи. Вышеупомянутый Эней Тактик приложил руку к созданию книжного шифра Энея, суть которого заключается в передаче информации с помощью специальных малозаметных пометок в тексте книги, проставленных рядом с буквами. Кроме того, под книжным шифром понимается такой шифр, в котором используется любой фрагмент текста из книги, а сам шифр состоит из точного указания номера строки и номера буквы в строке. Одна и та же буква могла получать несколько обозначений, что увеличивало надежность шифра.

Широко известен также квадрат Полибия, или шахматная доска Полибия. Данная система представляет собой замену каждой буквы нижестоящей буквой в квадрате, или парой координатных чисел. Из древности до наших дней сохранились данные о шифре Цезаря. Как и атбаш, шифр сдвига тоже является шифром подстановки, в котором каждый символ заменяется другим символом того же алфавита, находящимся на некотором расстоянии от заменяемого символа. Как следует из названия, шифр использовался Цезарем для переписки с генералами. Успешность его применения объясняется неграмотностью противника [2: 28].

Огромное влияние на развитие криптологии имела арабская цивилизация. Именно арабы первые открыли и описали метод криптоанализа. Стремительно развивающееся исламское государство испытывало потребность в хорошо налаженной системе государственного управления. Аппарат чиновников полагался на отлаженную систему обмена сообщениями, безопасность которой обеспечивалась шифрованием. Чиновники пользовались шифроалфавитом наподобие тех, что были описаны выше. Однако вклад арабов состоит не только в широком использовании шифроалфавитов, но и в создании криптоанализа (дешифрование сообщения без знания ключа). Столь высокие достижения в криптологии можно объяснить высоким уровнем развития в области математики и лингвистики. На наш взгляд, решающим фактором развития криптологии в арабском мире стала религия [2: 20]. Исламские теологи активно исследовали Хадисы на предмет частотности используемых в них слов. Главным открытием стало то, что некоторые буквы в арабском языке встречаются чаще остальных. Это открытие привело к прорыву в криптографии. Позднее арабский ученый Аль-Кинди впервые описал криптосистему на основе частотного анализа в труде «Рукопись по дешифрованию криптографических сообщений».

На Западе криптография не имела широкого распространения вплоть до наступления эпохи Возрождения. Шифры, которые применялись в то время, отличались предельной простотой – фразы писались в обратном порядке или по вертикали, гласные заменяли точками, использовали иностранные алфавиты, каждая буква открытого текста заменялась следующей. Кроме того считалось, что криптография и стеганография тесно связаны с черной магией и каббалой.

С появлением в Европе, в XVI веке, первых дипломатов возникла необходимость шифровать сообщения. Шифры стали применяться не только представителями власти или церкви, но и учеными для защиты приоритета научных открытий. «Стеганография развивалась как метод шифровки, пригодный для политики и военного дела. Не зря она зарождается вместе с началом конфликтов между национальными государствами, а ее расцвет приходится на период крупных абсолютистских монархий» [6: 134]. Начиная примерно с 1400 г. и до 1850 г. в шифровальной практике доминировали системы, которые являлись наполовину кодом и наполовину шифром [4: 9].

В XIV веке увидела свет книга Чикко Симонети с описанием принципа лозунгового шифра. В XV веке вышла работа Габриэля де Лавинда «Трактат о шифрах», в которой характеризуется шифр пропорциональной замены, обеспечивающий замену букв несколькими символами, пропорционально частотности букв в исходном тексте [7: 18]. В Милане получает распространение миланский ключ.

В 1466 г. появляется «Трактат о шифрах» Леона Альберти. В нем рассматривается полуалфавитный шифр собственного изобретения, реализованный в виде шифровального диска, где для шифровки использовалось два отдельных алфавита. Альберти впервые основывал свои изыскания на принципе комбинаторики [8: 98].

В 1518 году в Германии произошел прорыв в развитии криптографии – опубликована книга «Полиграфия» под авторством аббата Иоганнеса Тритемия, включающая несколько способов шифрования, один из которых становится основой для развития идеи полуалфавитной замены.

Мысли Тритемия развил Джовани Белазо. Он выпустил в 1533 году книгу «Шифр сеньора Белазо», в которой для шифрования предлагался к использованию пароль – слово или группа слов, записываемых над открытым текстом, а каждый символ пароля означал номер заменяемой буквы. Данный способ впоследствии получил название «шифр Виженера» по имени своего создателя [9: 25]. Блейс де Вижинер был послан, в XVI веке написал книгу «Трактат о шифрах», в которой предложил использовать для шифрования 26 алфавитов, а порядок использования шифра определялся знанием пароля. Схожий принцип был в дальнейшем применен Томасом Джефферсоном.

Первым профессиональным криптоаналитиком был Антуан Россиньоля, служивший при Людовике XIV. На основании трудов Россиньоля можно предположить, что именно он является первым, кто сформулировал концепцию «временной стойкости шифров». Россиньоля изобрел шифр, который назвал «великим» и стойкость которого была несомненна, вплоть до конца XIX века, пока Этьен Базери не взломал его [8: 107].

Важнейшим нововведением в криптографии стало внедрение роторных шифровальных систем, которые сильно упростили использование полуалфавитных шифров. Пионером был Томас Джефферсон, создавший в 1790 г. дисковый шифр. Его устройство позволило автоматизировать процесс шифрования [10].

Изобретение телеграфного аппарата повлияло на криптографию, многие прежние шифровальные решения оказались непригодны в силу их несовместимости с принципами телеграфа. В 1854 г. в обход британских войск входит шифр Плейфера, основанный на принципе шифрования биграмм – пар символов вместо одиночных символов. Шифр Плейфера останется актуальным вплоть до начала Второй мировой войны [11].

Первая мировая война способствовала дальнейшему внедрению шифрования. Так, потребности военной и оборонной сфер стали главными импульсами дальнейшего развития криптографических и криптоаналитических средств.

С 20-х годов XX века стала активно использоваться «Энигма» – шифровальная машина роторного типа, разработанная Эдвардом Хеберном и впоследствии усовершенствованная Артуром Кирхом. Наибольшее распространение получила в Германии во время Второй мировой войны. Алан Тьюринг внес большой вклад в дешифровку перехваченных сообщений и в создание электронно-механической машины Bombe [12: 141].

Работа Клода Шеннона «Теория связи в секретных системах», выпущенная в 1949 г., является еще одной переходной точкой, когда утвердились новые теоретические принципы криптографической защиты информации. Криптография провозглашается математической наукой. К концу 1960-х появляются первые – более совершенные – блочные шифры, которые сменяли роторные системы.

С 1970-х бурное развитие получает компьютерная криптография, что объясняется серьезным увеличением вычислительных

мощностей, которые позволяли уже к тому моменту создавать полноценные криптосистемы. Компьютерные криптосистемы в разы превосходили свои механические аналоги. Кроме того, с 1970-х криптография становится полноценной гражданской отраслью [7: 23]. В 1978 г. возникает стандарт шифрования – DES, появление которого способствовало развитию новых криптоаналитических алгоритмов [13: 12].

В 1976 году выходит работа Уитфилда Диффи и Мартина Хеллмана «Новые направления в криптографии», в которой был описан способ шифрования с открытым ключом. Первой криптосистемой с открытым ключом считается алгоритм RSA, название которого является акронимом имен создателей – Rivest, Shamir, Adleman [14: 5].

С этих пор интерес к криптографии проявляют независимые исследователи, оборонная промышленность и представители бизнеса. Одновременно увеличивается активность властей. Так, в США АНБ (Агентство национальной безопасности) пыталось всячески засекретить любые разработки и достижения в этой области не только государственных организаций, но и независимых исследователей. Широкий резонанс получил законопроект, требовавший от разработчиков шифровальных устройств включать в свои продукты так называемый *backdoor* – черный ход, – который позволял бы спецслужбам получать доступ к передаваемой информации. В дальнейшем, в 1993 году, АНБ предпринимало попытку продвижения проекта *Clipper Chip*, который давал бы возможность третьей стороне получать доступ к закрытому ключу [12: 10].

В 80-90-е гг. прошлого века появляются новые виды шифрования: вероятностное шифрование, квантовая криптография и т.д. Развитие квантовой физики проявляет потенциальные горизонты развития криптографии. Расширяются области применения криптографии.

Краткая ретроспектива позволяет заключить, что на протяжении всей истории в криптографии существовала определенная коммуникативная парадигма. Шифры использовались генералами для связи между частями войск или дипломатами для обмена депешами, важную роль шифры сыграли также в сакральной сфере. Безусловно, здесь можно возразить, что шифры могли использоваться обывателями в прежние эпохи, однако достоверных

фактов, свидетельствующих об этом, нет. На наш взгляд, смена парадигмы применения криптографии произошла в XXI веке, хотя предпосылки этого закладывались с момента изобретения телеграфа, а затем и проводного телефона. Правда, демократичными средствами коммуникации стали мобильный телефон и смартфон. Стремительный технический прогресс позволил свести к минимуму затраты на производство подобных устройств, а беспроводные сети Интернета уже постепенно опутывают даже отдаленные участки мира. Рассмотрим цифры по России: «доля пользователей Интернета в современной России в 2 раза превышает число тех, кто не применяет интернет-коммуникацию. При этом наблюдается интенсивное расширение аудитории глобальной Сети, так как почти половина активных пользователей включилась в интернет-коммуникацию за последние 2-4 года» [15].

С момента изобретения Интернета и его дальнейшего повсеместного распространения, а также превращения его в главное средство обмена информацией между людьми криптография стала актуальной для всех слоев населения. На наш взгляд, главным катализатором распространения данного тезиса стали, вероятно, разоблачения Эдварда Сноудена. Однако мы не хотим сказать, что он стал первым говорить о необходимости повышения криптографической грамотности. Актуальность криптографии в наше время объясняется тем, что доступ к Интернету и другим сетям обмена информацией есть у подавляющего большинства людей в развитых странах (при таких тенденциях доступ к сетям в скором времени будет и у всего человечества), однако далеко не вся информация, которой обмениваются люди, является защищенной. Напомним, за последнее время широкое распространение получили покупки онлайн, социальные сети, услуги государственных порталов, на которых сосредоточена важнейшая личная информация граждан. Кроме того, что информация сделалась более разнообразной и более конфиденциальной, увеличилось и общее количество информации.

Предтечей Сноудена было движение криптоанархистов [16] – приверженцев философской концепции, суть которой заключается в использовании сильных криптографических решений на основе публичных ключей для защиты от массовых несанкционированных сборов информации, а также в сохранении полной анонимности в Сети. Схожи взгляды и у шифропанков, к которым

причисляются Брем Коэн (создатель протокола bit-torrent), Айвен Голдберг (автор термина «интернет-зависимость»), Джулиан Ассанж (основатель wikileaks) и многие другие.

В середине 2013 года системный аналитик и сотрудник АНБ Эдвард Сноуден передал прессе ряд документов, из которых было ясно, что АНБ осуществляет перехват электронных сообщений, телефонных звонков (в том числе глав государств), отслеживание передвижения владельцев мобильных телефонов, потоков SMS, наблюдение за сотрудниками иностранных дипломатических миссий, отслеживание, а также перехват и глубокий анализ информации, передаваемой по магистральным каналам. Кроме того стало известно, что АНБ осуществляло сотрудничество с крупнейшими телекоммуникационными компаниями и крупнейшими интернет-провайдерами США, а также имеет возможности для осуществления несанкционированного доступа к личной информации владельцев смартфонов на популярных платформах.

США принимают все необходимые меры, чтобы обезопасить свои каналы связи, но в то же время они осуществляют широко-масштабный перехват и дешифрование сообщений других стран [4]. «Суммарная вычислительная мощность, доступная АНБ, возможно, самая большая в мире. И при этом про само АНБ известно крайне мало, даже существует полушутливая расшифровка аббревиатуры NSA: No Such Agency (Нет Такого Агентства)» [13: 20].

На основе представленных Сноуденом документов можно попытаться сделать несколько осторожных предположений, находящихся на грани конспирологии и мании преследования:

- во-первых, власти США в лице АНБ обладают достаточными мощностями для ведения электронной разведки и слежки за любым человеком независимо от его гражданства и статуса в любой точке мира;

- во-вторых, слежка может проводиться вопреки любому законодательству. Напомним, неприкосновенность переписки и презумпция невиновности были провозглашены и закреплены не раз за мировую практику: Декларация прав человека и гражданина Франции, Билль о правах человека Великобритании и США. Кроме того данные принципы закреплены не только в Декларации прав человека от 10 декабря 1948 года, но и в Международном пакте о гражданских и политических правах 1966 г.

Главный тезис сторонников внедрения и распространения электронной слежки и сбора информации заключается в том, что заблаговременное получение данных позволит предотвратить террористический акт или иное преступление [17]. Этот же аргумент используется и в отношении сторонников распространения персональных средств шифрования. Однако статистика говорит об обратном: за 2013 год из 3500 прослушанных и перехваченных разговоров только в 41 случае злоумышленники использовали средства шифрования, и в 9 случаях, когда полиция не смогла получить доступ к информации [18].

Спустя полтора года после события 2013 года можно заключить, что поступок Сноудена в той или иной мере повлиял на мир. Так, например, через год после публикаций некоторые общественные организации выступили за проведение акции против интернет-слежки (5 июня 2014 г.), а в России была учреждена премия имени Эдварда Сноудена в области интернет-медиа.

Итак, история криптографии насчитывает несколько тысяч лет. Первое околкриптографическое решение едва ли было направлено на сокрытие информации. Первые надежные способы передачи информации появлялись благодаря военным конфликтам. Становление разветвленного государственного аппарата в арабском мире способствовало распространению криптографии среди чиновников, а также появлению первых научных трудов по криптоанализу. Географические открытия, развитие торговых отношений в Европе ввело криптографию в гражданскую сферу, параллельно развивается стеганография. Религия оказывает существенное влияние на развитие криптографии. Распространение получают полуалфавитные шифры. Развивающаяся дипломатия испытывает потребность в новых, более стойких криптографических решениях. Постепенно шифры начинают механизироваться. Появление телеграфа требует новых шифров, которые бы соответствовали принципам работы телеграфов. Мировые войны XX века утверждают в очередной раз необходимость шифрования. Развитие электронных, а затем и компьютерных технологий революционно изменяет принципы построения криптосистем. Кроме того, появление телефона, мобильной связи и Интернета вводит криптографию в гражданское поле. Бурный технический прогресс конца XX века способствует широкой информатизации общества. Информация стала сверхцен-

ной, что обуславливает дальнейшие поиски более совершенных криптографических решений и повышение безопасности рядовых пользователей сетей.

Литература:

1. *Отраднова О.А.* Проблема онтологического статуса информации // Философские проблемы информационных технологий и киберпространства. 2012. № 1. – С. 128-132. (*Otradnova O.A.* Problem of ontological status of information // *Filosofskie problemy informacionnyx technologij i kiberprostranstva.* 2012. № 1. – P. 128-132.)
2. *Сингх С.* Книга кодов: тайная история кодов и их взлома // Пер. с англ. А. Галыгина. М.: АСТ: Астрель, 2007. – 447 с. (*Singh S.* The Code Book – a history of cryptography // Per. s angl. A. Galygina. M.: AST: Astrel', 2007. – 447 s.)
3. *Вольтер.* Поэмы. Философские повести. Pamфлеты // Предисл., сост., примеч. В.И. Пашенко. К.: Политиздат Украины, 1989. – 483 с. (*Voltaire.* Poems. Philosophical stories. Pamphlet // Predisl., sost., primch. V.I. Pashhenko. K.: Politizdat Ukrainy, 1989. – 483 s.)
4. *Кан Д.* Взломщики кодов // Пер. А. Ключевский. М.: Центрполиграф, 2000. – 480 с. (*Kahn D.* The Codebreakers // Per. A. Klyuchevskij. M.: Centrpoligraf, 2000. – 480 s.)
5. *Хайдеггер М.* Из диалога о языке между японцем и спрашивающим. URL: www.heidegger.ru/download_file.php?type=2&id=71. (*Heidegger M.* From dialogues about the language between a Japanese and an enquirer. URL: www.heidegger.ru/download_file.php?type=2&id=71.)
6. *Эко У.* Поиски совершенного языка в европейской культуре // Пер. с итал. А. Миролубовой (Серия «Становление Европы»). М.: Александрия, 2007. – 430 с. (*Eko U.* The Search for the Perfect Language // Per. s ital. A. Mirolyubovoj (Seriya «Stanovlenie Evropy»). M.: Aleksandriya, 2007. – 430 s.)
7. *Носов В.А.* Краткий исторический очерк развития криптографии // Московский университет и развитие криптографии в России. Материалы конференции МГУ 17-18 октября 2002 г. М.: МЦНМО, 2003. – С. 17-25. (*Nosov V.A.* Brief historical essay *Kratkij istoricheskij ocherk razvitiya kriptografii* // *Moskovskij universitet i razvitie kriptografii v Rossii. Materialy konferencii MGU 17-18 oktyabrya 2002 g.* M.: MCNMO, 2003. – S. 17-25.)
8. *Адаменко М.В.* Основы классической криптологии: секреты шифров и кодов. М.: ДМК Пресс, 2012. – 256 с. (*Adamenko M.V.* The bases of classical cryptology: secrets of cypher and codes. M.: DMK Press, 2012. – 256 s.)
9. *Dooley, John F.* A Brief History of Cryptology and Cryptographic Algorithms. New York: Springer, 2013. – 99 p.
10. *Аверченков В.И.* Системы защиты информации в ведущих зарубежных странах: учебное пособие для вузов [Электронный ресурс] / В.И. Аверченков, М.Ю. Рытов, Г.В. Кондрашин, М.В. Рудановский. –

- 3-е изд., стереотип. М.: ФЛИНТА, 2011. – 244 с. (*Averchenkov V.I. Systems of information security in foreign countries: tutorial for institutes of higher education [E'lektronnyj resurs] / V.I. Averchenkov, M.Yu. Rytov, G.V. Kondrashin, M.V. Rudanovskij. – 3-e izd., stereotip. M.: FLINTA, 2011. – 244 s.)*
11. *Бабаш А.В., Шанкин Г.П.* Средневековая криптография. URL: http://cccp.narod.ru/work/book/kgb/babash_02.html. (*Babash A.V., Shankin G.P. The cryptography of medieval. URL: http://cccp.narod.ru/work/book/kgb/babash_02.html.*)
 12. *Жельников В.* Криптография от папируса до компьютера. М.: АБФ, 1996. – 336 с. (*Zhel'nikov V. Cryptography from papyrus to computer. M.: ABF, 1996. – 336 s.*)
 13. *Скляр Д.В.* Искусство защиты и взлома информации. СПб.: БХВ-Петербург, 2004. – 288 с. (*Sklyarov D.V. The art of information security and break-in. SPb.: BVXV-Peterburg, 2004. – 288 s.*)
 14. *Баричев С.Г., Серов Р.Е.* Основы современной криптографии. М.: Горячая линия – Телеком, 2011. – 175 с. (*Barichev S.G., Serov R.E. The bases of modern cryptography. M.: Goryachaya liniya – Telekom, 2011. – 175 s.*)
 15. *Бродовская Е.В., Шумилова О.Е.* Российские пользователи и непользователи: соотношение и основные особенности // Мониторинг. 2013. № 3 (115). – С. 5-18. (*Brodovskaya E.V., Shumilova O.E. Russian users and non-users: correlation and main features // Monitoring. 2013. № 3 (115). – S. 5-18.*)
 16. *Ладлоу П.* Криптоанархия, кибергосударства и пиратские утопии. М.: Ультра. Культура, 2005. – 600 с. (*Ludlow P. Crypto Anarchy, Cyberstates, and Pirate Utopias. M.: Ul'tra. Kul'tura, 2005. – 600 s.*)
 17. *Chomsky N.* Edward Snowden, the World's Most Wanted Criminal / Truth-out. URL: <http://www.truth-out.org/opinion/item/24071-noam-chomsky-edward-snowden-the-worlds-most-wanted-criminal>.
 18. Wiretap Report 2013 / United states courts URL: <http://www.uscourts.gov/Statistics/WiretapReports/wiretap-report-2013.aspx#sa9>.