DOI: 10.18287/2542-0445-2020-26-4-109-114

НАУЧНАЯ СТАТЬЯ

УДК 81'42

Дата поступления: 26.09.2020
рецензирования: 18.10.2020
принятия: 27.11.2020

Д.И. Имамгаязова
Башкирский государственный университет, г. Уфа, Российская Федерация
E-mail: diana.imamgaiazova@gmail.com. ORCID: http://orcid.org/0000-0002-5740-1951

Фреймирование киберпреступлений в медиатекстах на русском и английском языках

Аннотация: Освещая инциденты кибератак, СМИ информируют общественность о возможных угрозах и формируют конвенциональные представления об организаторах и мотивах киберпреступлений. Исследование фреймирования киберпреступлений в медиатекстах на русском и английском языках позволяет выявить, как с помощью языковых средств формируются стереотипные знания о новом феномене в разных лингвокультурных сообществах. В медиатекстах на русском и английском языках кибератаках презентуются через фреймы «война», «игра», «эпидемия» и «преступления». Фреймы предстают как динамические когнитивные образования, содержание и структура которых изменяется в зависимости от контекста.
Ключевые слова: фреймирование, фреймы киберпреступлений, анализ фреймов, когнитивная лингвистика, фрейм «война», фрейм «эпидемия».
Цитирование. Имамгаязова Д.И. Фреймирование киберпреступлений в медиатекстах на русском и английском языках // Вестник Самарского университета. История, педагогика, филология**.** 2020. Т. 26, № 4. С. 109–114. DOI: http://doi.org/10/12287/2542-0445-2020-26-4-109-114.
Информация о конфликте интересов: автор заявляет об отсутствии конфликта интересов.

© **Диана Ильдаровна Имамгаязова** – магистр филологии, магистр философии, экстерн филологического факультета, кафедра современного русского языкознания, Башкирский государственный университет, 450076, Российская Федерация, Республика Башкортостан, г. Уфа, ул. Заки Валиди, 32.

SCIENTIFIC ARTICLE

Submitted: 26.09.2020
Revised: 18.10.2020
Accepted: 27.11.2020

D.I. Imamgaiazova
Bashkir State University, Ufa, Russian Federation
E-mail: diana.imamgaiazova@gmail.com. ORCID: http://orcid.org/0000-0002-5740-1951

Framing of cybercrimes in Russian and English media texts

Abstract: Covering the incidents of cyber attacks, mass media inform the public about possible security threats and form the conventional knowledge of cyber criminals and their motives. The study of cybercrime framing in Russian and English media texts allows for reconstructing the sense-making process for a relatively new phenomenon in the different linguocultural communities. Russian and English-language media represent cyber attacks via frames of war, game, pandemic and crime. The frames appear as dynamic cognitive models that are able to adjust their content and structure to different contexts.
Key words: framing, cybercrime framing, frame building, cognitive linguistics.
Citation. Imamgaiazova D.I. Framing of cybercrimes in Russian and English media texts. *Vestnik Samarskogo universiteta. Istoriia, pedagogika, filologiia = Vestnik of Samara University. History, pedagogics, philology,* 2020, vol. 26, no. 4, pp. 109–114. DOI: http://doi.org/10.18287/2542-0445-2020-26-4-109-114. (In Russ.)
Information on the conflict of interests: author declares no conflict of interest.

© **Diana I. Imamgayazova** – Master of Philology, Master of Philosophy, external student of the Faculty of Philology, Department of Contemporary Russian Linguistics, Bashkir State University, 32, Zaki Validi Street, Ufa, 450076, Russian Federation, Republic of Bashkortostan.

Лингвокогнитивные исследования фреймов

В социогуманитарных науках фрейм понимается как «рамочная, каркасная модель обобщенного знания, имеющая универсальный, типовой характер» [Самарин 2012]. В лингвокогнитивных исследованиях фрейм предстает в качестве «структурированной единицы знания, в которой выделяются определенные компоненты и отношения между ними» [Болдырев 2004, с. 29]. Формирование значения во фреймовой семантике происходит за счет выделения, или «перспективизации», определенного фрагмента знания о типовой, часто повторяющейся ситуации [Болдырев 2004, с. 29].

В концепции Минского [Минский 1979] фрейм предстает как сеть с ячейками (слотами), которые заполняются концептуальным содержанием о ком-

понентах, аспектах и частях стереотипной ситуации. Через заполнение слотов происходит конкретизация обобщенного знания, заданного фреймом. В свою очередь, фрейм может выступать элементом структуры следующего уровня – фреймовой системы.

Многие современные исследования массовой коммуникации посвящены изучению трансляции и трансформации фреймов, заданных политическими акторами. При этом в фокусе внимания политологов находится прагматический аспект коммуникации: оценка эффективности фреймирования социальных проблем, идентичностей и взаимодействия [Entman 2010; Van Hulst, Yanow 2016], тогда как лингвисты обращают внимание на языковые средства фреймирования и функционирование фреймов в рамках определенного дискурса.

Основные стратегии фреймирования в политической коммуникации были выявлены в работе Сноу и Бенфорда [Snow, Benford 1992, p. 135]:

а) диагностическое фреймирование, которое указывает на истоки проблемы и закрепляет ответственность за нее за конкретным актором. В диагностическом фрейме присутствует субъект («кто или что является угрозой») и объект («кому или чему угрожают»). В некоторых случаях объект может быть генерализирован («глобальная угроза»);

б) прогностическое фреймирование, которое предлагает решения обсуждаемой проблемы. Во фрейме представлены конкретные тактики, предлагаемые для достижения поставленной цели;

в) мотивационное фреймирование, используемое для призыва к действию и сплочения вокруг «общей цели». Мотивационный фрейм апеллирует к общим ценностным установкам и убеждениям целевой аудитории.

При изучении конструирования фреймов в медиатекстах исследователи выделяют два взаимосвязанных компонента:

1) средства фреймирования – «явно воспринимаемые элементы в тексте или конкретные лингвистические структуры, такие как метафоры и гиперболы»;

2) средства аргументации, которые «включают (скрытно) передаваемую в тексте трактовку проблемы, ее причин, оценки и (или) рекомендуемых мер» [Burgers, Konijn, Steen 2016, p. 411].

В данной статье процесс конструирования фрейма киберпреступности изучается с позиций лингвопрагматики с целью установить, как фреймы в медиатекстах влияют на формирование концептуальных моделей и когнитивных схем, актуализируемых при столкновении с угрозами информационной безопасности.

Фреймирование киберпреступлений в СМИ

Зарубежные исследователи выявили, что освещение киберпреступлений в СМИ зачастую не совпадает с пониманием ситуации, установившимся в профессиональной среде.

Так, Чу и Смит [Choo, Smith 2008] разделяют организаторов киберпреступлений на три группы:

1) «традиционные» организованные преступные группы (далее – ОПГ), использующие информационные технологии как инструмент в преступной деятельности;

2) онлайн-ОПГ, формирующиеся и взаимодействующие только в киберпространстве с целью совершения экономических преступлений;

3) идеологически или политически мотивированные группы, которые используют киберпространство для достижения своих интересов (пропаганда, рекрутинг, привлечение финансирования и др.). Проведенный опрос экспертов по кибербезопасности подтверждает, что последний тип наименее распространен.

По данным государственных служб Великобритании, большинство киберпреступлений, совершаемых в стране, имеют экономические мотивы [Lavorgna, Sergi 2016]. При этом в медиафреймах атрибуция ответственности за киберпреступления зачастую связана с определенной нацией. «Чаще всего новости в прессе базируются на фрейме “Иностранный заговор”, где действия преступников расцениваются как скоординированная кибератака против Британии. По сообщениям в СМИ, организованная киберпреступность в основном базируется в России и Африке и представляет угрозу национальной безопасности, в то время как ОПГ, базирующиеся в других странах, регулярно совершают хищение личных данных и банковских реквизитов британских интернет-пользователей, практически не опасаясь преследования» [Lavorgna 2018, p. 361].

При освещении киберпреступлений в американских СМИ сформировалась устойчивая метафора cyber Pearl Harbor[1], повторяющаяся в медиатекстах в 1991–2016 гг. (см. рис.). По мнению ряда исследователей, фреймирование киберпреступлений в СМИ через метафору военной атаки времен Второй мировой войны сформировано правительством США вопреки тому, что публичные заявления политиков о мотивах преступников зачастую не имели фактических доказательств [Lawson, Middleton 2019].

Американские ученые Карас, Мур и Пэррот подробнее изучили метафорическое поле сферы кибербезопасности в дискурсе СМИ. Основными сферами-источниками для построения метафор служили военная терминология, сферы биологии, медицины и здравоохранения, рыночной экономики и др. В частности, рассматривались часто употребляемые в медиатекстах метафоры «крепость», «полиция и разбойники», «военные действия», «боевые искусства» и «космос» [Karas, Moore, Parrott 2008, p. 15–16]. Менее частотными, но достаточно устоявшимися стали метафоры «экосистема», «иммунитет», «здравоохранение и предупреждение заболеваний», «риск-менеджмент», «рыночная конкуренция» и «игра» [Karas, Moore, Parrott 2008, p. 18–19].

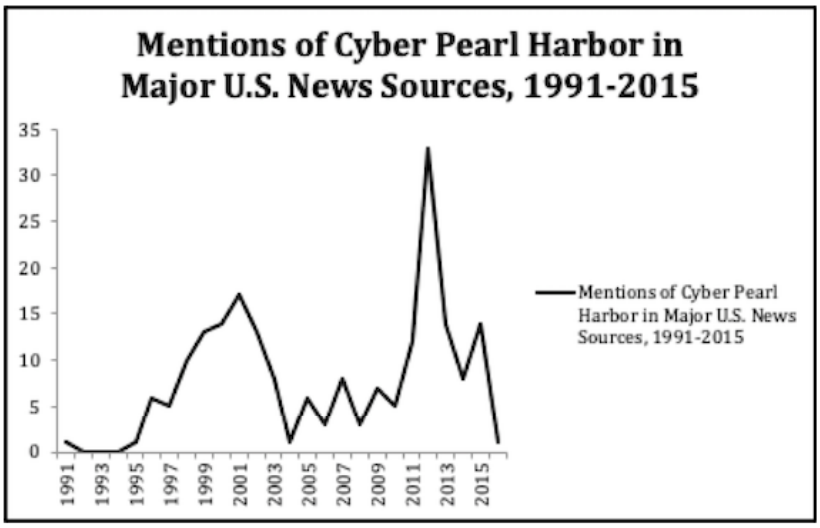

Рис. График частотности упоминания «кибер Перл Харбор» в СМИ США на основе данных Lexis Nexis Academic Universe
Fig. Graph of frequency of references to «cyber Pearl Harbor» in the US media based on data from Lexis Nexis Academic Universe

В российских исследованиях проблема фреймирования киберпреступности в СМИ разработана менее подробно. Фрейм «кибервойна» рассматривается в контексте изучения международных конфликтов [Степанова 2008, с. 29], тогда как конструирование и (ре)трансляция в СМИ фреймов в семантическом поле «киберпреступность» пока не рассматривались в академических работах.

Фреймы киберпреступлений в русскоязычных и англоязычных СМИ

Некоторые фреймы киберпреступлений встречаются в медиатекстах как на английском, так и на русском языках. Средствами фреймирования служат метафоры, метонимии, эпитеты и прецедентные высказывания, а также риторические приемы навешивания ярлыков и общей платформы – присоединения явления к уже популярной платформе или тенденции.

В качестве источника медиатекстов на английском языке использовался corpus NOW (News on the Web – «Новости в Сети»), объем корпуса – более 9 млрд слов из новостных порталов, газет и журналов, размещаемых в сети Интернет с 2010 г. по настоящее время. В данном исследовании поиск ограничен упоминаниями в 2019–2020 гг. Для сбора материалов СМИ на русском языке использовался семантический поиск в агрегаторе новостей Google News за аналогичный период времени.

А) **Фрейм «война».** Фрейм конструируется с помощью таких ярлыков, как «military hacker» («военные хакеры», «хакеры на военной службе») и «cyber espionage» («кибершпионаж», «кибербразведка»), а также средств языковой выразительности.

Russian military hackers *have been* ***boring into*** *the Ukrainian gas company*[2] («Русские военные хакеры пробурили путь в украинскую газовую компанию». Перевод – *Д. И.*).

Iran's ***formidable cyber arsenal*** *includes malware and DDoS attacks*[3] («Угрожающий кибераренал Ирана включает вредоносные программы и DDoS-атаки». Перевод – *Д. И.*).

Iran *had* ***targeted*** *aerospace companies, defense contractors, energy companies and telecommunications firms for* ***cyber-espionage operations*** *around the world*[4] («Иран нацелился на аэрокосмические компании, оборонных подрядчиков, энергетические и телекоммуникационные фирмы для организации сети кибершпионажа по всему миру». Перевод – *Д. И.*).

Another ***layer of your cybersecurity fortress*** *should be a VPN*[5] («Следующим уровнем крепости вашей кибербезопасности должна стать виртуальная частная сеть». Перевод – *Д. И.*).

В русскоязычных СМИ также присутствует фрейм «война». При этом чаще используются прецедентные высказывания и отсылки к известным военным конфликтам прошлых эпох.

«***Холодная кибервойна****: что нужно знать про* ***хакерские атаки США на Россию***»[6].

«***Кибершпионаж*** *в разведке ФРГ:* ***взлом во имя Родины***»[7].

«*Рейган –* ***отец*** *первой* ***кибервойны*** *против СССР*»[8].

Фрейм «война» является одним из субфреймов «конфликтных социальных отношений», который представляет пропозициональную когнитивную модель – стереотипную ситуацию противостояния между двумя или несколькими субъектами. Данный метафрейм также может профилироваться субфреймами «протест», «противостояние», «конкуренция». К облигаторным слотам фрейма «война» относятся субъект, предикат и объект, к терминальным – время, локация, способ / инструмент, спецификация (причины, следствия) и оценка.

При вербализации фрейма «война» в русском и английском языках возникают семантические раз-

личия. Англоязычные глаголы, реализующие предикат в данном фрейме (*to fight, to combat, to attack* и др.), обладают двухместной валентностью, что делает обязательной вербализацию субъекта и объекта (*Side A attacks Side B*). В русском языке возможно употребление безличных глаголов и отглагольных форм, в которых упоминание субъекта необязательно («Сторону А атаковали»). Появление подобных конструкций в медиатекстах ведет к тому, что аудитория «достраивает» структуру фрейма, исходя из контекста и стереотипных представлений о сторонах конфликта.

Б) **Фрейм «эпидемия».** Сфера эпидемиологии выступает одним из основных концептуальных источников для метафор киберпреступлений. Фрейм «Эпидемия» актуализируется в репортажах о нетаргетированных атаках, где отсутствует четкая атрибуция ответственности. Процесс деактивации угрозы описывается как «лечение» компьютера или другого устройства.

The NYPD's high-tech fingerprint database was temporarily brought down by a ***virus-infected computer****. <...> The Joint Terrorism Task Force were notified of the* ***contamination***[9] («База данных полиции Нью-Йорка с отпечатками пальцев была временно деактивирована из-за зараженного вирусом компьютера. Группа противодействия терроризму была проинформирована о заражении». Перевод – *Д. И.*).

Nuspire caught 2.7 million ***botnets****, a 19 % decrease from the previous quarter but still totaling* ***30,000 infections per day***[10] («Nuspire зафиксировал 2,7 млн "ботнетов" – это на 19 % меньше, чем в предыдущем квартале, но все еще приводит к 30 тыс. заражений в день». Перевод – *Д. И.*).

«*Одни* ***вирусы*** *внедряются и воруют персональные данные, другие превращают ПК в "****компьютер-зомби****", который незаметно для владельца рассылает спам или становится участником атаки на какой-нибудь сайт. <…> В прошлом веке* ***вирусы*** *чаще всего "****приносили*** *на дискете". Приходилось вызывать специалиста, чтобы тот* ***излечил вычислительную машину от "болезни"****»*[11].

«***Вирус распространяется*** *через файлы приложений, скачанные с сайтов, или в составе других программ. После установки* ***зараженного софта он отделяется*** *в самостоятельное приложение. И даже если его удалить –* ***"вылечить" смартфон*** *уже не получится*»[12].

Облигаторными слотами фрейма «эпидемия» являются субъект, предикат, объект и локация, терминальными: время, способ, причина и следствие. В текстах СМИ о «киберэпидемиях» часто актуализуются понятия о масштабе и скорости распространения вредоносных программ, характере ущерба и мерах предосторожности. При этом структура фрейма претерпевает трансформацию. Локация распространения является неотъемлемым компонентом когнитивной модели фрейма «эпидемия» в случае биологического заражения. Когда речь идет об «инфицировании» компьютерных устройств, то вредоносные программы в последние годы распространяются преимущественно через виртуальные сети, без физического контакта (через флэш-карты, диски и др.). При этом заполнение слота «локация» становится необязательным, что иллюстрирует динамический характер структуры фрейма.

В) **Фрейм «преступление».** Концептуализация киберпреступлений часто базируется на переносе понятий из сферы офлайн-преступлений. При конструировании фрейма могут использоваться метафоры физических объектов (взлом сейфа, банковской ячейки) и термины криминалистики (цифровой отпечаток, след).

Cyber gangsters *publish staff passwords following 'Sodinokibi' attack*[13] («Кибергангстеры опубликовали пароли сотрудников после атаки группировки "Содинокиби"». Перевод – *Д. И.*).

GozNym ***cyber-crime gang*** *which stole millions* ***busted***[14] («Разоблачена банда киберпреступников GozNym, похитившая миллионы. Перевод – *Д. И.*).

«***Киберполиция*** *разоблачила одессита, который обокрал банк на 1 млн грн*»[15].

«*Для защиты пользователей необходимы комплексные решения, которые будут выявлять* ***цифровой отпечаток устройства*** *и типичное поведение пользователей*»[16].

В рассмотренных русскоязычных текстах СМИ о киберпреступлениях представлено более широкое разнообразие лексических единиц, презентующих фрейм «преступление», нежели в англоязычных. В частности, вербализуются методы расследования («слежка», «перехват», «обезвреживание»), распространены авторские неологизмы при наименовании киберпреступников («хакер-наемник», «кибермафия», «хакер-одиночка» и др.).

Г) Фрейм **«конкурентная игра».** В англоязычных СМИ киберпреступления также часто описываются через фрейм «конкурентная игра», что нехарактерно для русскоязычных СМИ.

"*In order to understand* ***China's military approach in cyber defense****, look to the ancient board* ***game of Go****", says the head of the Defense Intelligence Agency*[17] («"Для понимания китайской военной доктрины по кибербезопасности нужно изучить древнюю игру го", – отметил глава Агентства военной разведки». Перевод – *Д. И.*).

The hack back bill *legitimizes* ***a messy game*** *of revenge for businesses*[18] («Закон об Обратном Взломе легитимирует грязную игру мести для бизнеса». Перевод – *Д. И.*).

Структура и содержание фреймов, с помощью которых в текстах СМИ презентуется новости о киберпреступлениях, трансформируются в зависимости от лингвокультурного контекста. Схожими для дискурса англоязычных и русскоязычных СМИ является использование фреймов «война», «преступление» и «эпидемия». При этом фрейм «игра» характерен только для медиатекстов на английском языке, а фрейм «преступление» пред-

ставлен более широким разнообразием лексики в русскоязычных медиатекстах – за счет заимствований и неологизмов (поиск русских аналогов для замещения англицизмов). Для обоих языков характерно активное использование метафор и метонимии.

Перспектива изучения фреймов киберпреступности

Дальнейшее изучение фреймов киберпреступлений и кибербезопасности в масс-медиа может способствовать развитию научной дискуссии в нескольких направлениях. Во-первых, будет сформировано более полное понимание сущности и ограничений концептов, заимствованных из других сфер, для обсуждения проблем кибербезопасности. Во-вторых, понимание частотности использования тех или иных фреймов в публичной сфере позволит понять, как именно концептуализация кибербезопасности влияет на исследование проблематики и разработку политических решений. В-третьих, наиболее востребованные медиафреймы становятся основой для формирования концептуальных моделей и когнитивных схем, актуализируемых при работе с информационными системами в целом. В-четвертых, медиафреймы служат эвристической цели – объяснению проблематики сферы кибербезопасности для неспециалистов за счет использования концептов из сфер, хорошо знакомых массовой аудитории. Таким образом, фреймирование проблем кибербезопасности может применяться в сфере образования.

Примечания

[1] Cyber Pearl Harbor – «Кибер Перл-Харбор». Отсылка к «Нападению на Перл-Харбор» – операции времен Второй мировой войны, во время которой произошло внезапное комбинированное нападение японской авиации и подводных лодок на американские военные базы, расположенные на Гавайских островах.

[2] Russians Hacked Ukrainian Gas Company at Center of Impeachment // New York Times. URL: https://www.nytimes.com/2020/01/13/us/politics/russian-hackers-burisma-ukraine.html (дата обращения: 21.03.2020).

[3] The US is worried about Iran retaliating with a cyberattack // VOX. URL: https://www.vox.com/recode/2020/1/7/21055715/iran-cyber-attack-threat-soleimani.

[4] Iran attack: How strong is Iran's military? // BBC. URL: https://www.bbc.com/news/world-middle-east-50982743 (дата обращения: 21.03.2020).

[5] Cybersecurity best practices for 2020 // TechTalks. URL: https://bdtechtalks.com/2020/01/31/cybersecurity-best-practices-2020.

[6] Холодная кибервойна: что нужно знать про хакерские атаки США на Россию // ТАСС. URL: https://tass.ru/mezhdunarodnaya-panorama/6562214 (дата обращения: 21.03.2020).

[7] Кибершпионаж в разведке ФРГ // Deutsche Welle. URL: https://www.dw.com/ru/кибершпионаж-в-разведке-фрг-взлом-во-имя-родины-17042019/av-48379255 (дата обращения: 21.03.2020).

[8] Рейган – отец первой кибервойны против СССР // Комсомольская правда. URL: https://www.kp.ru/daily/26209.3/3093616 (дата обращения: 21.03.2020).

[9] How the NYPD's fingerprint database got shut down by a computer virus // New York Post. URL: https://nypost.com/2019/11/24/how-the-nypds-fingerprint-database-got-shut-down-by-a-computer-virus (дата обращения: 21.03.2020).

[10] How to defend your organization against the latest malware, botnets and security exploits // TechRepublic. URL: https://www.techrepublic.com/article/how-to-defend-your-organization-against-the-latest-malware-botnets-and-security-exploits (дата обращения: 21.03.2020).

[11] Вирусы и антивирусы // Российская газета. URL: https://rg.ru/2011/02/03/antivirus.html (дата обращения: 21.03.2020).

[12] Неудаляемый вирус заразил более 45 тысяч Android-устройств // Москва24. URL: https://www.m24.ru/audios/Moskva-FM/31102019/142263 (дата обращения: 21.03.2020).

[13] Cyber gangsters publish staff passwords following 'Sodinokibi' attack on car parts group Gedia // Computer Weekly. URL: https://www.computerweekly.com/news/252477341/Cyber-gangsters-publish-staff-passwords-following-Sodinokibi-attack-on-car-parts-group-Gedia (дата обращения: 21.03.2020).

[14] GozNym cyber-crime gang which stole millions busted // BBC. URL: https://www.bbc.com/news/technology-48294788 (дата обращения: 21.03.2020).

[15] Киберполиция разоблачила одессита, который обокрал банк на 1 млн грн // Интерфакс. URL: https://interfax.com.ua/news/general/640109.html (дата обращения: 21.03.2020).

[16] Илья Сачков: «Сейчас кибербезопасность – это важный элемент пирамиды Маслоу» // Инвест-Форсайт. URL: https://www.if24.ru/group-ib-kiberbezopasnost (дата обращения: 21.03.2020).

[17] US Air Force chief: The biggest threat posed by China is in space // DefenseNews. URL: https://www.defensenews.com/smr/reagan-defense-forum/2019/12/07/air-force-chief-the-biggest-threat-posed-by-china-is-in-space (дата обращения: 21.03.2020).

[18] The hack back bill legitimizes a messy game of revenge for businesses // Yahoo Business. URL: https://finance.yahoo.com/news/hack-back-bill-legitimizes-messy-171008949.html (дата обращения: 21.03.2020).

Источники фактического материала

NOW Corpus: корпус текстов. URL: https://www.english-corpora.org/now (дата обращения: 21.03.2020).

Google News: агрегатор новостей. URL: https://news.google.com (дата обращения: 21.03.2020).

Библиографический список

Burgers, Konijn, Steen 2016 – *Burgers C., Konijn E.A., Steen G.J.* Figurative framing: Shaping public discourse through metaphor, hyperbole, and irony // *Communication Theory*. 2016. Vol. 26, No. 4. P. 410–430. DOI: http://doi.org/10.1111/comt.12096.

Choo, Smith 2008 – *Choo K.K.R., Smith R.G.* Criminal exploitation of online systems by organised crime groups // Asian Journal of Criminology. 2008. Vol. 3, No. 1. P. 37–59. DOI: http://doi.org/10.1007/s11417-007-9035-y.

Entman 2010 – *Entman R.M.* Media framing biases and political power: Explaining slant in news of Campaign 2008 // *Journalism*. 2010. Vol. 11, No. 4. P. 389–408. DOI: http://doi.org/10.1177/1464884910367587.

Karas, Moore, Parrott 2008 – *Karas T.H., Moore J.H., Parrott L.K.* Metaphors for cyber security / *SANDIA report,* vol. SAND 2008-5381, pp. 3–42. DOI: http://doi.org/10.2172/947345%20.

Lavorgna 2018 – *Lavorgna A.* Cyber-organised crime. A case of moral panic? // *Trends in Organized Crime*. 2018. Vol. 22, No. 4. P. 357–374. DOI: http://doi.org/10.1007/s12117-018-9342-y.

Lavorgna, Sergi 2016 – *Lavorgna A., Sergi A.* Serious, therefore organised? A critique of the emerging «cyber-organised crime» rhetoric in the United Kingdom // *International Journal of Cyber Criminology.* 2016. Vol. 10, No. 2. P. 170–187. DOI: http://doi.org/10.5281/zenodo.163400.

Lawson, Middleton 2019 – *Lawson S., Middleton M.K.* Cyber Pearl Harbor: Analogy, fear, and the framing of cyber security threats in the United States, 1991–2016 // *First Monday*. 2019. Vol. 24, No. 3. DOI: http://doi.org/10.5210/fm.v24i3.9623.

Snow, Benford 1992 – *Snow D.A., Benford R.D.* Master frames and cycles of protest // *Frontiers in social movement theory*. London: Yale University Press, 1992. P. 133–155. DOI: http://doi.org/10.2307/2580310.

Van Hulst, Yanow 2016 – *Van Hulst M., Yanow D.* From policy «frames» to «framing»: theorizing a more dynamic, political approach // *The American review of public administration.* 2016. Vol. 46, No. 1. P. 92–112. DOI: http://doi.org/10.1177/0275074014533142.

Болдырев 2004 – *Болдырев Н.Н.* Концептуальное пространство когнитивной лингвистики // Вопросы когнитивной лингвистики. 2004. № 1. С. 18–36. URL: https://cyberleninka.ru/article/n/kontseptualnoe-prostranstvo-kognitivnoy-lingvistiki; https://www.elibrary.ru/item.asp?id=17358043.

Минский 1979 – *Минский М.* Фреймы для представления знаний. Москва: Энергия, 1979. 152 с. URL: https://litresp.ru/chitat/ru/%D0%9C/minskij-marvin/frejmi-dlya-predstavleniya-znanij.

Самарин 2012 – *Самарин А.В.* Кросс-мобильность теории фрейма в системе научных знаний // Фундаментальные исследования. 2012. № 3 (6). С. 604–608. URL: https://www.fundamental-research.ru/ru/article/view?id=30083; https://www.elibrary.ru/item.asp?id=17865089.

Степанова 2008 – *Степанова Е.А.* Государство и человек в современных вооруженных конфликтах // Международные процессы. 2008. Т. 6, № 1 (16). С. 29–40. URL: https://elibrary.ru/item.asp?id=16993640; http://www.intertrends.ru/system/Doc/ArticlePdf/84/Stepanova-16.pdf

References

Burgers, Konijn, Steen 2016 – *Burgers C., Konijn E.A. and Steen G.J.* (2016) Figurative framing: Shaping public discourse through metaphor, hyperbole, and irony. *Communication Theory*, vol. 26, no. 4, pp. 410–430. DOI: http://doi.org/10.1111/comt.12096.

Choo, Smith 2008 – *Choo K.K.R. and Smith R.G.* (2008) Criminal exploitation of online systems by organised crime groups. *Asian Journal of Criminology*, vol. 3, no. 1, pp. 37–59. DOI: http://doi.org/10.1007/s11417-007-9035-y.

Entman 2010 – *Entman R.M.* (2010) Media framing biases and political power: Explaining slant in news of Campaign 2008. *Journalism*, vol. 11, no. 4, pp. 389–408. DOI: http://doi.org/10.1177/1464884910367587.

Karas, Moore, Parrott 2008 – *Karas T.H., Moore J.H. and Parrott L.K.* (2008) Metaphors for cyber security. In: *SANDIA report,* vol. SAND 2008–5381, pp. 3–42. DOI: http://doi.org/10.2172/947345.

Lavorgna 2018 – *Lavorgna A.* (2018) Cyber-organised crime. A case of moral panic? *Trends in Organized Crime,* vol. 22, no. 4, pp. 357–374. DOI: http://doi.org/10.1007/s12117-018-9342-y.

Lavorgna, Sergi 2016 – *Lavorgna A., Sergi A.* (2016) Serious, therefore organised? A critique of the emerging «cyber-organised crime» rhetoric in the United Kingdom. *International Journal of Cyber Criminology*, vol. 10, no. 2, pp. 170–187. DOI: http://doi.org/10.5281/zenodo.163400.

Lawson, Middleton 2019 – *Lawson S., Middleton M.K.* (2019) Cyber Pearl Harbor: Analogy, fear, and the framing of cyber security threats in the United States, 1991–2016. *First Monday*, vol. 23, no. 3. DOI: http://doi.org/10.5210/fm.v24i3.9623.

Snow, Benford 1992 – *Snow D.A., Benford R.D.* (1992) Master frames and cycles of protest. In: *Frontiers in social movement theory*. London: Yale University Press, pp. 133–155. DOI: http://doi.org/10.2307/2580310.

Van Hulst, Yanow 2016 – *Van Hulst M., Yanow D.* (2016) From policy «frames» to «framing»: theorizing a more dynamic, political approach. *The American review of public administration*, vol. 46, no. 1, pp. 92–112. DOI: http://doi.org/10.1177/0275074014533142.

Boldyrev 2004 – *Boldyrev N.N.* (2004) The conceptual space of cognitive linguistics. *Issues of Cognitive Linguistics,* no. 1, pp. 18–36. Available at: https://cyberleninka.ru/article/n/kontseptualnoe-prostranstvo-kognitivnoy-lingvistiki; https://www.elibrary.ru/item.asp?id=17358043. (In Russ.)

Minsky 1979 – *Minsky M.* (1979) Framework for representing *knowledge.* Moscow: Energiia, 152 p. Available at: https://litresp.ru/chitat/ru/%D0%9C/minskij-marvin/frejmi-dlya-predstavleniya-znanij. (In Russ.)

Samarin 2012 – *Samarin A.V.* (2012) Cross-frame theory of mobility in scientific knowledge. *Fundamental Research*, no. 3 (6), pp. 604–608. Available at: https://fundamental-research.ru/ru/article/view?id=30083; https://www.elibrary.ru/item.asp?id=17865089. (In Russ.)

Stepanova 2008 – *Stepanova E.A.* (2008) State and human in contemporary armed conflicts. *International trends*, vol. 6, no. 1 (16), pp. 29–40. Available at: https://elibrary.ru/item.asp?id=16993640; http://www.intertrends.ru/system/Doc/ArticlePdf/84/Stepanova-16.pdf. (In Russ.)