Т. А. Сысоева

ТЕМАТИЧЕСКАЯ СТРУКТУРА СТАТЕЙ О КИБЕРБЕЗОПАСНОСТИ (на материале белорусских и американских изданий)

Глобальная авторская интенция определяет замысел медийного сообщения, диктует его общее содержание и конкретную форму. Таким образом

обеспечивается целостность текста, или его смысловая связность. Благодаря целостности сообщение предстает как законченное произведение, характеризующееся единством темы, а отраженная в нем ситуация представлена во взаимосвязи всех ее компонентов.

Одна из составляющих целостности – **тематическое единство**, которое объединяет все фрагменты сообщения и воплощается в ключевых словах. Однако в современной медиасфере единство темы может поддерживаться в том числе разными текстами. Это происходит в тех случаях, когда в разных публикациях (теле- или радиопередачах) освещаются одни и те же события, обсуждаются одни и те же проблемы. Единое тематическое начало обеспечивает стабильность медиадискурса, определяет его доминанты и в то же время позволяет дифференцировать разные медиажанры или разные издания/редакции.

Рассмотрим ключевые слова, актуализирующие категорию тематического единства в аналитических статьях о кибербезопасности и защите персональных данных в Интернете, которые были опубликованы на сайтах белорусских изданий «СБ. Беларусь сегодня», «Народная газета» и американских изданий «The Washington Post», «The Seattle Times» в 2021 г. Определим основные понятия, объединяющие статьи данной тематики, и сопоставим их в лингвокультурном аспекте.

Для исследуемых статей были выделены следующие группы маркеров.

Прежде всего, это ***слова*** и ***словосочетания***, ***обозначающие*** саму ***сферу деятельности***, область применения обсуждаемых мер защиты: *киберпространство*, *виртуальное пространство*, *всемирная паутина*; *Internet*, *network*. На задачи, которые необходимо решить в данной сфере, указывают следующие единицы: *кибербезопасность*, *информационная безопасность*, *защита информации/персональных данных*, *борьба с киберпреступностью*, *пресечение вредоносных кибердействий*, *противодействие киберугрозам*; *cybersecurity*, *cyber defense*, *avert cyber-attack*, *response to the attack*. Как видно из примеров, речь идет о мерах (что нужно обеспечить) и о контрмерах (что нужно пресекать).

Перечисленные выше индикаторы соотносятся с глобальной темой – *кибербезопасность и ее обеспечение*. В свою очередь, конкретизировать информацию позволяют маркеры частных подтем. К таким подтемам в исследуемом материале относятся агенты, т.е. участники процесса онлайн-коммуникации, нуждающиеся в киберзащите или пострадавшие от киберпреступлений: *интернет-пользователь*, *интернет-игрок*; *victim of the hack*.

Следующая группа индикаторов – ***действия, совершаемые агентами при осуществлении деятельности в Интернете***: *сделать рассылку*, *кликать по ссылке*, *поставить лайк*, *комменировать*, *(пере)постить*, *вводить логин/пароль/запрос*, *загрузить в бот*, *посещать сайт*, *оставить след в Интернете*, *подключиться к веб-ресурсам*, *осуществить кибердействие*; *post*, *tweet*. Обращает на себя внимание тот факт, что в русскоязычном материале подобных индикаторов значительно больше.

Отдельно выделим ***организации (учреждения, институты), имеющие отношение к решению вопросов кибербезопасности***: *компания «Digital Shadows»*, *корпорация «Microsoft»*, *Управление по раскрытию преступлений в сфере высоких технологий МВД*; *software giant*, *e-mail security firm/company*, *cybersecurity firm/company*, *cyber-research firm*. В данном случае стоит подчеркнуть, что в американских изданиях упоминается гораздо больше организаций, объединений и т.д., занимающихся вопросами кибербезопасности. Это могут быть как государственные, так и частные компании, которые специализируются в разработке соответствующего программного обеспечения, проведении исследований, выявлении кибепреступлений. Совершенно ожидаемо, что перечень представителей организаций, отвечающих за кибербезопасность или осуществляющих борьбу с киберпреступлениями, гораздо богаче в англоязычных текстах: *оперуполномоченный группы по противодействию киберпреступности*, *эксперт по кибербезопасности*; *executive vice president of cybersecurity strategy*, *chief cyberstrategist*, *cybersecurity analyst/expert*, *senior security researcher*, *ransomware expert*, *cyber/cybersecurity sleuth*. Иногда речь идет о более абстрактной категории – сообществе киберспециалистов (*cybersecurity circles*, *cybersecurity community*). Заслуживает внимание упоминание продуктов (платформ, приложений, программ и т.п.), созданных действующими организациями. Приведем примеры из этой группы индикаторов: *приложение для смартфона*, *программный модуль*, *почтовый сервис*, *мессенджер*, *поисковая система/поисковик*, *онлайн-платформа*, *маркетплейс*, *интернет-банкинг*; *exchange e-mail service/ software*, *search bot*.

Подтему *киберпреступники* маркируют следующие слова и словосочетания: *киберзлодей*, *кибермошенник*, *хакер*, *злоумышленник в сети*; *cybercriminal*, *hacker*, *attacker*, *perpetrator*, *intruder*. Примечательно, что американских статьях дается более детальный «портрет» нарушителя (*Russian-speaking and North Korean cybercriminals*, *state-backed hackers*), а также подчеркивается групповой характер действий (*cyber-espionage gang*, *hacking group*). Авторы русскоязычных статей чаще говорят о сфере незаконной деятельности киберпреступников, «месте» совершения преступлений, обозначая их следующим образом: *хакерский форум*, *подпольный маркетплейс*, *paste-сайт*, *файлообменник*, *даркнет*.

Виды киберпреступлений, ***примеры нарушения кибербезопасности*** отмечены соответствующими индикаторами: *ИТ-преступление*, *киберпреступление*, *высокотехнологичная преступность*, *интернет-мошенничество*, *утечка данных/персональных сведений*, *взлом аккаунта/странички/программного обеспечения*, *кража интеллектуальной собственности/логина/ пароля*, *вымогательство сведений*, *атака со стороны хакеров*, *кибератака*, *кибершпионаж*, *рассылка вредоносного программного обеспечения*, *социальная инженерия*, *вишинг*; *cybersecurity/cyber-data breach*, *cyberattack*, *hacking/ espionage/cyberspying/ransomware attack*, *cyber espionage operation*, *leaked documents*, *data loss*. При этом в американских изданиях подчеркивается глобальный характер подобных преступлений: *global cybersecurity crisis, global ransomware scourge*.

Выполняемые киберпреступниками действия таковы: *совершить кибератаку*, *взломать аккаунт/компанию*, *«зашить» вредоносную программу*, *собирать логины/пароли*, *украсть/слить пароль*, *заразить компьютер*, *запустить вирус*; *steal e-mails/data/secrets*, *infiltrate e-mail systems*, *break into a network/target*, *breach/target an organization*, *hit a company/a target*, *compromise a company*, *expose a server to intrusion*. Используемые хакерами инструменты маркируются в двух языках (*спецпрограмма по подбору паролей*, *таргетированное письмо*; *ransomware*, *malware*), тогда как акцент на конкретных мерах защиты делается в американских изданиях: *secure the system*, *upgrade security features*, *monitor the incoming network traffic*, *detect/block an intrusion attempt*, *detected/block ransomware*, *stymie an attack*, *detect a hack*, *identify/fix weaknesses in software*, *send out a fix*, *release patches/fixes*, *patch the system/the vulnerability*, *get vulnerable servers fixed*.

Таким образом, тематическая структура исследуемых статей выстраивается иерархически и может быть представлена в виде глобальной темы и подтем, которые в тексте обозначаются соответствующими языковыми индикаторами. Общей для статей из американской и белоруской периодики является актуальная проблема *кибербезопасность и ее обеспечение*, описание которой осуществляется через частные категории: *участники онлайн-коммуникации и их действия в Сети – киберпреступники и совершаемые ими ИТ-преступления – организации, предлагающие способы киберзащиты*. Лингвокультурная специфика реализации данной структуры состоит в следующем. В белорусской прессе подчеркивается неосторожное поведение пользователей Интернета, упоминаются сети и платформы, являющиеся особым «местом» совершения киберпреступлений. В свою очередь, в американской периодике на первый план выходит описание организаций и сообществ, отвечающих за кибербезопасность, а также более детально рассматриваются конкретные меры киберзащиты.