ОРИГИНАЛЬНАЯ СТАТЬЯ

CC BY 4.0

DOI: 10.26794/1999-849X-2020-13-6-68-76
УДК 327.8:339.9(045)
JEL F02, F52, H56, M15

Обеспечение глобальной информационной безопасности в условиях применения «мягкой силы»

А.Г. Глебова
Финансовый университет, Москва, Россия
http://orcid.org/0000-0002-9449-6013

АННОТАЦИЯ

Актуальность темы рассмотрения настоящей статьи подтверждается все возрастающим интересом ученых и практиков — участников международных экономических отношений к вопросам обеспечения информационной безопасности в условиях применения «мягкой силы». *Предмет исследования* — глобальная и национальная информационная безопасность государства. *Цель работы* — выявление роли «мягкой силы» в обеспечении информационной безопасности государства на национальном уровне. Результаты исследования позволяют *сделать выводы* о том, что влияние «мягкой силы» на глобальную информационную безопасность безусловно и велико; информационная безопасность государства на национальном уровне обеспечивается формальными методами, включающими формирование соответствующей законодательной базы, регламентирующей не только правила пользования информацией ограниченного доступа, ее обработки и передачи, не только определяющей ответственность за нарушение установленных норм, но и условия получения и/или использования информационного контента населением с целью его защиты от воздействия недружественной «мягкой силы». Обеспечение информационной безопасности неформальными методами подразумевает принятие мер государственного воздействия на пользователей информации в стране и за рубежом, как правило, организационной и морально-этической направленности, обеспечивающих распространение взглядов, фактов, аргументов в форме новостей, образовательного и псевдо-образовательного контента с целью формирования общественного мнения.

Ключевые слова: международная безопасность; национальная безопасность; информационная безопасность; «мягкая сила»; методы обеспечения безопасности

Для цитирования: **Глебова А.Г. Обеспечение глобальной информационной безопасности в условиях применения «мягкой силы». *Экономика. Налоги. Право.* 2020;13(6):68-76. DOI: 10.26794/1999-849X-2020-13-6-68-76**

ORIGINAL PAPER

Ensuring Global Information Security in the Context of "Soft Power" Implementation

A.G. Glebova
Financial University, Moscow, Russia
http://orcid.org/0000-0002-9449-6013

ABSTRACT

The relevance of the topic of this article is confirmed by the growing interest of scientists and practitioners involved in international economic relations in ensuring information security in the context of the use of "soft power". *The subject of the research* is global and national information security of the state. *The purpose of the work* is to identify the role of "soft power" in ensuring information security of the state at the national level. The results of the study allow us *to conclude* that the impact of "soft power" on global information security is certainly great; information security of the state at the national level is provided by formal methods, including the formation of an appropriate legislative framework that regulates not only the rules for using restricted access information, its processing and transmission, not only determining responsibility for violating established norms, but also the conditions for receiving and/or using information content by the population in order to protect it from the impact of unfriendly "soft power". Providing information security by

© Глебова А.Г., 2020

informal methods implies taking measures of state influence on information users in the country and abroad, usually of an organizational and moral-ethical orientation, ensuring the dissemination of views, facts, and arguments in the form of news, educational and pseudo-educational content in order to form public opinion.

Keywords: international security; national security; information security; "soft power"; security methods

For citation: **Glebova A.G. Ensuring global information security in the context of "soft power" implementation. *Ekonomika. Nalogi. Pravo = Economics, taxes & law.* 2020;13(6):68-76. (In Russ.). DOI: 10.26794/1999-849X-2020-13-6-68-76**

СОВРЕМЕННАЯ КОНЦЕПЦИЯ «МЯГКОЙ СИЛЫ»

Актуальность вопросов обеспечения глобальной информационной безопасности обусловлена в первую очередь взрывным ростом информационных и коммуникационных технологий и массовым использованием информационного контента населением. Особенно острой становится проблема обеспечения информационной безопасности в столь быстроменяющихся условиях. Любое государство сталкивается с двояким проявлением этой проблемы: с одной стороны, оно должно защищать информацию ограниченного пользования на всех уровнях (в масштабах страны в целом и на уровнях региона, отдельного предприятия, отдельного человека) от внешних угроз, а с другой стороны, уберегать население страны от нежелательного информационного контента. При этом государство само может использовать стратегию «мягкой силы» для достижения своих стратегических целей как на территории своей страны, так и в международных отношениях.

Создателем понятия «мягкая сила» (*soft power*) является Дж. Най-младший, американский политолог и государственный деятель, впервые опубликовавший свои идеи в 1990 г. в *Foreign Policy*. Позднее, в 2002 г., в работе «*The Paradox of American Power: Why the World's Only Superpower Can't Goit Alone*» [1] им была сформулирована концепция, определяющая разницу между понятиями «мягкая сила» и «жесткая сила» (*hard power*), обозначены их особенности. При этом «жесткой силой» Дж. Най назвал материальные элементы государственной власти, а «мягкой силой» — ее духовные элементы [2, с. 67–68]. Позже он использовал понятие «умная сила» (*smart power*) [3], обозначая этим термином способность политической власти сочетать «мягкую» и «жесткую» силу для формирования наиболее эффективной стратегии. Авторы Честер А. Крокер, Фен Ослер Хэмпсон и Памела Р. Аалл в работе [4] также отмечают, что «умная сила» подразумевает «стратегическое применение дипломатии, убеждения, развитие компетенций, проецирование власти и влияния экономически эффективными способами, имеющими политическую и социальную легитимность».

Отличительной чертой «мягкой силы» российские ученые В.С. Ким и Я.А. Бохан считают отсутствие принуждения, рассматривая при этом культуру, экономическую модель развития и внешнюю политику государства как ценности «мягкой силы», образующие нормы, способные определять поведение и мотивировать к действию людей [5, с. 17]. К ключевым характеристикам «мягкой силы» можно отнести ее нематериальность, информативность и подвижность [6, с. 187].

Исследователи И.В. Радиков и Я.В. Лексютина полагают, что на мировой арене «мягкая сила» реализуется путем насаждения определенных стандартов, правил поведения, которыми должны руководствоваться государства в проведении внутренней и внешней политики [7]. В то же время, по мнению Е. Русакова, «мягкая сила» — это не примитивный пиар, не пропаганда, невелеречивые заявления о «мире», «добрососедстве», «партнерстве» и т.д. Она обладает «неосязаемой» привлекательностью, порождающей ответную позитивную реакцию [8].

В международных экономических отношениях «мягкая сила» также играет заметную роль: например, в [9] показано, что экспорт страны увеличивается, когда ее лидерство одобряется другими странами.

В быстроменяющихся условиях виртуализации современного экономического и политического пространства при множестве форм потребления контента и его упаковки в инструментальное поле «мягкой силы» все большую роль играют интернет-коммуникации [10], которые становятся важнейшими элементами «мягкой силы»: именно с помощью виртуальных инструментов осуществляется формирование общественного мнения, конструируется система ценностей, предпочтений, потребностей и настроений людей в виртуальном пространстве. При этом А.В. Агеева и Г.В. Красноцветов [11] отмечают, что технологии интернет-коммуникации придают «мягкой силе» в ряде случаев инвер-

сионный характер. Это может происходить при организации массовых акций через социальные платформы и мессенджеры, когда вариативность организованной активности может изменяться от акций, направленных на социальное созидание, формирование благоприятного имиджа, укрепление доверия и добрососедства (например, международный молодежный экофестиваль в Москве), до откровенно деструктивных, организованных извне действий, в том числе включающих противостояние правоохранительным органам (например, беспорядки в США после гибели Джорджа Флойда, протесты после президентских выборов в Белоруссии).

В своем исследовании Н. Цветкова [12] отмечает, что российские подходы к интернет-дипломатии изменили принципы и методы современной публичной дипломатии во всех странах.

Таким образом, стратегия информационной безопасности любого государства, с одной стороны, должна обеспечивать защиту важнейшей информации от внешних угроз и население страны от деструктивного информационного контента, а с другой стороны, включать активное использование инструментария «мягкой силы» для достижения своих целей в международных отношениях.

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В широком смысле информационная безопасность (*information security — infosec*) подразумевает защиту информации от несанкционированного доступа, являясь частью управления информационными рисками и включая меры по предотвращению или уменьшению вероятности несанкционированного доступа, использования, раскрытия, нарушения работы, удаления, повреждения, модификации, проверки или записи информации [13]. В случае нарушения безопасности информации сотрудники подразделения информационной безопасности разрабатывают меры по снижению негативного влияния события на компанию/общество/государство.

В российском законодательстве в данной сфере используется следующая терминология[1]:

- *информационная безопасность* Российской Федерации — «состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства» [14];
- «*обеспечение информационной безопасности* — осуществление взаимоувязанных правовых, организационных, оперативно-розыскных, разведывательных, контрразведывательных, научно-технических, информационно-аналитических, кадровых, экономических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления» [14];
- *информационная сфера* — совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети Интернет, сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также механизмов регулирования соответствующих общественных отношений.

Можно также выделить два специфических термина, применяемых в контексте информационной безопасности[2]:

- *событие информационной безопасности* (*information security event*) — идентифицированное возникновение состояния системы, услуги или сети, указывающее на возможное нарушение политики информационной безопасности, отказ от защитных мер, а также возникновение ранее неизвестной ситуации, которая может быть связана с безопасностью;
- *инцидент информационной безопасности* (*information security incident*) — любое непредвиденное или нежелательное событие, которое может нарушать деятельность или информационную безопасность.

Согласно ГОСТу Р ИСО/МЭК 27001–2006 инцидентами информационной безопасности являются:

[1] Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 05.12.2016 № 646. URL: http://www.scrf.gov.ru/security/information/document5/.

[2] ГОСТ Р ИСО/МЭК 27001–2006 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. URL: http://docs.cntd.ru.

• утрата услуг, оборудования или устройств;
• системные сбои или перегрузки;
• ошибки пользователей;
• несоблюдение политики или рекомендаций по информационной безопасности;
• нарушение физических мер защиты;
• неконтролируемые изменения систем;
• сбои программного обеспечения и отказы технических средств;
• нарушение правил доступа.

Очевидно, что основной задачей стратегии информационной безопасности является обеспечение конфиденциальности, целостности и доступности (*confidentiality, integrity and availability — CIA*) информации. Соответствующие отраслевые стандарты регламентируют формирование корпоративных паролей, использование брандмауэров и программного обеспечения для шифрования; содержат рекомендации и требования к антивирусному программному обеспечению; описывают нормы юридической ответственности.

Управление рисками в рамках обеспечения информационной безопасности представляет собой процесс, который:
• идентифицирует информацию и угрозы;
• оценивает риски;
• принимает решения об управлении выявленными рисками (избегать, смягчать, делиться или принимать);
• формирует и внедряет инструменты управления безопасностью;
• осуществляет мониторинг любых изменений и разработку решения проблем.

Угрозы информационной безопасности проявляются во многих формах, не ограничиваясь стихийными бедствиями, сбоями в работе компьютера или сервера и физической кражей. Все возрастающая зависимость государственных и частных структур от информационных систем привела к тому, что информационная безопасность стала ключевым фактором в управлении рисками кибербезопасности и вызвала потребность в специализированных специалистах по информационной безопасности [15], занимающихся вопросами безопасности данных, безопасности приложений, сетевой безопасности, компьютерной безопасности и физической безопасности, с учетом того, что данные, приложения и прочая информация распространяются далеко за пределы того, что традиционно считается компьютером. Смартфоны, планшеты и другие мобильные устройства представляют собой такой же компьютер, как сервер или мэйнфрейм, и подвержены злонамеренным кибератакам, позволяющим получать доступ к конфиденциальной информации, информационным ресурсам или контролю компьютерных систем.

Угрозы информационной безопасности могут проявляться во многих формах, включая атаки на программное обеспечение, кражу личных данных, саботаж, физическое хищение и вымогательство информации [16]:
• программные атаки на информационную безопасность, включающие вирусы и прочие вредоносные программы типа «черви», программы-вымогатели типа *WannaCry* или «троянских коней»;
• фишинговые электронные письма или вебсайты, часто имеющие целью кражу интеллектуальной собственности или регистрацию учетных данных для получения несанкционированного доступа;
• саботаж в виде отказа в обслуживании, нацеленный на снижение доступности ключевых информационных ресурсов, уменьшение доверия или продуктивности организации до тех пор, пока не будет получен платеж в обмен на возврат услуги организации;
• кража информации и оборудования;
• вымогательство информации, включающее получение доступа к конфиденциальной информации, а затем удержание ее до выкупа, пока не будет произведена оплата.

Существуют много способов защиты от кибератак, но угрозами номер один для любой организации являются ее пользователи или собственные сотрудники, которые подвержены воздействию посредством применения социальной инженерии или фишинга, что требует особых усилий руководства любой компании в сфере информационной безопасности.

Конфиденциальность, целостность и доступность информации, называемые триадой *CIA*, лежат в основе информационной безопасности[3]. При этом ведутся споры о том, достаточно ли триада *CIA* отвечает быстроменяющимся технологиям и требованиям бизнеса, а также взаимосвязи безопасности и конфиденциальности.

[3] Tunggal A.T. What is Information Security? // UpGuard, Inc. 2020. URL: https://www.upguard.com/blog/information-security.

Конфиденциальность (*confidentiality*) — это непредоставление информации или ее нераскрытие посторонним лицам, организациям или процессам. В английском языке этот термин похож на термин «персональные данные» (*privacy*), но не взаимозаменяем[4].

Персональные данные — это компонент конфиденциальности, который реализует меры безопасности для защиты от неавторизованных пользователей. Персональные данные пользователей становятся все более важной частью конфиденциальности, в том числе из-за нормативных требований.

Целостность (*integrity*) или *целостность данных* (*data integrity*) связана с поддержанием, гарантией, точностью и полнотой данных в течение всего их жизненного цикла. Это означает реализацию мер безопасности, которые гарантируют, что данные не могут быть изменены или удалены неуполномоченным лицом или необнаруженным способом.

Доступность (*availability*) подразумевает, что для того чтобы любая информационная система была полезной, она должна быть доступна при необходимости. Это означает, что компьютерные системы, которые хранят и обрабатывают информацию, средства безопасности, а также каналы связи, которые к ней получают доступ, должны функционировать по требованию.

Компании и их клиенты все больше полагаются на системы высокой доступности в режиме реального времени 24/7. Это означает, что профессионалы в области информационной безопасности все больше заботятся о том, чтобы обеспечить доступность к информации путем предотвращения перебоев в подаче электроэнергии, сбоя оборудования и атак типа отказ в обслуживании. Доступность часто рассматривается как наиболее важная часть успешной программы информационной безопасности, поскольку в конечном счете ее конечные пользователи должны иметь возможность использования информации.

Управление информационными рисками — это процесс выявления уязвимостей и угроз для информационных ресурсов, применяемых организацией, а также набор действий, которые необходимо предпринять для снижения риска до приемлемого уровня, основанного на значении информационной ценности для организации.

Выделяют два основных соображения в отношении любого процесса управления рисками[5]:

1) процесс управления рисками является непрерывным и повторяющимся по своей природе, и его необходимо повторять до бесконечности по мере появления новых угроз и уязвимостей;

2) выбор используемых контрмер или средств контроля должен обеспечивать баланс между производительностью, стоимостью, эффективностью и информационной ценностью защищаемого актива.

ДЕЯТЕЛЬНОСТЬ ГОСУДАРСТВА В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Роль государства в усилении информационной безопасности в системе национальной безопасности выражается в:

- нормативно-правовое регулировании на законодательном и подзаконном уровнях;
- реализации национальных проектов;
- регулировании на уровне исполнительной власти;
- организации взаимодействия государства и общества.

Если регулирование и взаимодействие носят системный и непрерывный характер, то реализация национальных проектов направлена на прорывное решение наиболее значимых задач.

Так, национальный проект «Цифровая экономика», реализуемый Минцифрой России, предусматривает выполнение нескольких подпрограмм по следующим направлениям:

1) кадры;
2) безопасность;
3) технологии;
4) государственное управление.

Их реализация рассчитана на период до 2024 г. В рамках подпрограммы «Информационная безопасность» планируется решение ключевых задач, призванных обеспечить устойчивое развитие национальной информационной инфраструктуры, подготовку кадров и развитие технологий, повысить экспортный потенциал отрасли, гарантировать полную защиту интересов государства и общества.

[4] Бартов Е. Понятия privacy и confidentiality — в чем разница? // BISA (Business Information Security Association). URL: https://bis-expert.ru/blog/5345/42577

[5] Tunggal A. T. What is Information Security? // UpGuard, Inc. 2020. URL: https://www.upguard.com/blog/information-security.

Национальной проект предусматривает[6]:

• предоставление поддержки 100 экспортно-ориентированным компаниям, что должно обеспечить устойчивое присутствие национальных информационных технологий на международной арене;

• маршрутизацию на территории России не менее 90% сетевого трафика (концепция суверенного Рунета);

• обеспечение использования не менее чем 97% населения средств защиты информации;

• снижение доли иностранного программного обеспечения, покупаемого или арендуемого государственными организациями, до 10% в структуре общей цены закупок.

В рамках подпрограммы с осени 2019 г. началось предоставление субсидий ряду исполнителей. На ее реализацию до 2024 г. планируется затратить 167 млрд руб.

Среди показателей в цифровом выражении, которых предполагается достичь к 2024 г.:

• снижение среднего времени простоев ГИС (государственных информационных систем) в результате информационных атак с 65 часов на конец 2018 г. до 1 часа в 2024 г., что должно сыграть ключевую роль в сфере защиты информации;

• повышение процента населения, применяющего отечественные средства защиты информации, с 86 до 97%;

• увеличение количества специалистов, подготовленных по направлению защиты информации, с 7 до 24 тысяч;

• уменьшение доли иностранного программного обеспечения в общей цене закупок государственными органами и компаниями с 50 до 10%.

Помимо показателей, которых планируется достичь, определены конкретные действия, которые должны быть реализованы в рамках национального проекта[7]:

1. Предполагается, что безопасность информационного пространства и сети Интернет недостаточно отрегулирована на уровне международного права, отсутствуют документы, которые позволяют устранять перевес сил в пользу отдельных государств. В рамках решения этой задачи в международные организации (ООН) внесены проекты соглашений и конвенций, направленных на реализацию принципа паритетности в сфере информационных технологий, равного участия государств в управлении интернетом. Так, Россия стала инициатором первой резолюции Генеральной ассамблеи ООН о «Достижениях в области информатизации и телекоммуникаций в контексте международной безопасности в 1998 г.» и намерена продолжать движение в этом направлении.

2. Нападения иностранных хакеров на сети электрообеспечения страны признаны одной из основных угроз национальной и экономической безопасности. Были проанализированы угрозы, составлена их модель и внесены предложения по изменению отраслевых стандартов и нормативно-правовых актов с целью создания единой устойчивой системы защиты объектов электросистемы, принадлежащих различным собственникам, что усложняет задачу создания единого пространства регулирования системы защиты от сетевых атак.

3. Обеспечение информационной безопасности требует преимущественной маршрутизации трафика в пределах границ Российской Федерации. Разработаны концепция и основные нормативные акты в направлении создания суверенного Рунета, началось их внедрение. Правовой статус российского сегмента интернета законодательно закреплен.

4. От устойчивости сетей связи зависит качество управления и взаимодействия государственных органов. Были законодательно закреплены требования к устойчивости и безопасности сетей связи и оборудования как для ГИС, так и для компаний различных организационно-правовых форм.

5. Сети общего пользования могут стать объектами направленных атак. Разработана и внедряется система мониторинга состояния сетей общего пользования. Изменены требования к проектированию сетей связи общего пользования с учетом действующей модели угроз. Новые общие и частные сети могут создаваться только при условии их соответствия разработанным параметрам.

6. Информационная безопасность призвана решать задачи обеспечения правопорядка. Разработан и принят комплекс решений по внедрению отечественных информационных технологий при реализации программы «Умный город».

---

[6] Паспорт национальной программы «Цифровая экономика Российской Федерации» // Правительство Российской Федерации. 2020. URL: http://government.ru/info/35568.

[7] Паспорт национальной программы «Цифровая экономика Российской Федерации» // Правительство Российской Федерации. 2020. URL: http://government.ru/info/35568.

Среди уже внедренных проектов, обеспечивающих защиту интересов государства и общества, особое значение имеет ГосСОПКА — федеральная информационная система по сбору и обмену данными о компьютерных атаках на территории Российской Федерации, задачей которой является обеспечение национальной безопасности в информационной сфере посредством[8]:

- прогнозирования рисков атак в информационном пространстве;
- обеспечения взаимодействия государства и компаний, которым принадлежат значимые информационные ресурсы, особенно обслуживающие критические объекты инфраструктуры, для выявления, предупреждения и ликвидации последствий цифровых атак;
- контроля и мониторинга уровня защищенности инфраструктуры от цифровых атак;
- расследования инцидентов информационной безопасности.

С точки зрения информационной архитектуры ГосСОПКА выглядит как единый, но территориально распределенный комплекс центров управления и мониторинга, обменивающихся между собой информацией о кибератаках. Задача системы — объединение критически важной инфраструктуры в единую сеть с целью обмена информацией о кибератаках. Если такая атака совершается на один из объектов, он передает ее параметры другим объектам, и те имеют возможность подготовиться к нападению.

Система состоит из центров трех уровней — федерального, регионального и местного, которые делятся на территориальные, ведомственные и корпоративные центры. Для борьбы с компьютерными атаками они должны иметь следующие программные и аппаратные средства:

1) *обнаружения*. Средства выявляют не инциденты, а именно значимые события информационной безопасности, чаще всего они реализуются по модели *SIEM*;

2) *предупреждения*. Механизм предупреждения, инвентаризации и мониторинга реализуется программными средствами класса *vulnerability scanner* или сканерами защищенности;

3) *ликвидации последствий* посредством реализации совместной работы участников системы над ликвидацией последствий компьютерных атак, реализуемой посредством расшифровки; обмена информацией; криптографической защиты каналов связи. В данном случае дополнительной разработки средств шифрования именно для ГосСОПКИ не потребовалось.

Разработка программных средств для их внедрения в центрах ГосСОПКА ведется крупнейшими компаниями — производителями программного обеспечения в стране, что является одним из проявлений взаимодействия государства и общества в сфере информационной безопасности как части национальной безопасности.

Современная концепция взаимодействия власти и общества в сфере информационной безопасности предполагает, что практически все нормативные акты, существенно затрагивающие общественные интересы, должны пройти стадию предварительного общественного обсуждения.

Вопросы информационной безопасности Российской Федерации могут быть решены только в тесном взаимодействии государства, бизнеса и общества, где заинтересованными участниками диалога становятся крупные корпорации и разработчики программного обеспечения.

ВЫВОДЫ

Информационная безопасность на национальном уровне обеспечивается формальными (административными) и неформальными (в том числе экономическими) методами. Формальные методы включают формирование национальной законодательной базы, которая регламентирует не только *правила использования* информации ограниченного доступа, ее обработки и передачи, но и *условия получения и/или использования* информационного контента населением с целью его защиты от воздействия недружественной «мягкой силы».

Неформальные методы включают методы государственного воздействия на пользователей информации в стране и за рубежом. В большинстве случаев это меры организационно-психологического и морально-этического воздействия на получателей информационного контента через средства массовой информации, интернет с использованием для этих целей социальных сетей, мессенджеров, видеохостингов и т.п. Основная цель такого воздействия — формирование общественного мнения, изменение/упрощение системы образования и т.п.

[8] Указ Президента Российской Федерации от 22.12.2017 № 620.

В настоящее время инструментарий «мягкой силы» с разной степенью активности и эффективности используется многими странами. Проблема грамотного противодействия новым информационным/цифровым угрозам становится одной из наиболее актуальных задач обеспечения национальной и глобальной безопасности. Сегодня противостоять деструктивному информационному контенту, поступающему из зарубежных стран, можно двумя путями: *во-первых*, защищая российское общество от внешней идейно-ценностной экспансии и деструктивного информационно-психологического воздействия; *во-вторых*, проводя более активную политику «мягкой силы», применяя формальные и неформальные методы.

СПИСОК ИСТОЧНИКОВ

1. Nye J. Jr. The paradox of american power: why the world's only superpower can't go it alone. N.Y.: Oxford University Press, 2002. DOI: 10.1093/0195161106.001.0001
2. Nye J. Jr. Soft power: the means to success in world politics. PublicAffairs, Apr 28, 2009 — Political Science — 208 p.
3. Nye, Joseph S. Get smart: combining hard and soft power. *Foreign Affairs*. 2009;88(4):160–63. URL: http://www.jstor.org/stable/20699631.
4. Crocker, Chester A.; Hampson, Fen Osler; Aall, Pamela R. leashing the dogs of war: conflict management in a divided world. US Institute of Peace Press, 2007:13.
5. Ким В.С., Бохан Я.А. Трансформация стратегии «мягкой силы» КНР в современных условиях // Вестник Челябинского государственного университета. Серия «Политические науки. Востоковедение».— 2012.— Т. 266.— № 12.— С. 17–20.— ISSN 1994–2796.
6. Русакова О.Ф. Концепт «мягкой» силы (Soft power) в современной политической философии // Антиномии: Научный ежегодник Института философии и права УрО РАН.—2010 — Вып. 10.— С. 173–192.— ISSN 1818–0566.
7. Радиков И.В., Лексютина Я.В. «Мягкая сила» как современный атрибут великой державы // Мировая экономика и международные отношения.— 2012.— № 2.— С. 20.—– ISSN 0131–2227.
8. Русаков Е.М. «…Держа в руках большую дубинку» // Азия и Африка сегодня.— 2011.— Т. 644.— № 3.— С. 25–33.— ISSN 0321–5075.
9. Rose, Andrew K. Soft power and exports. *Review of International Economics*. 2009;27.5:573–1590.
10. Василенко И.А. Роль символического капитала культуры в информационном обществе // Власть.— 2017.— Т. 25.— № 7.— С. 75–79.— ISSN 2071–5358.
11. Агеева А.В., Красноцветов Г.В. «Мягкая сила» в онлайн-пространстве: практический опыт применения технологий интернет-коммуникаций // Власть.— 2020.— Т. 28.— № 2.— С. 96–100.— ISSN 2071–5358.— DOI: 10.31171/vlast.v28i2.7140
12. Tsvetkova N. Russian digital diplomacy: A rising cyber soft power?. Russia's Public Diplomacy. Palgrave Macmillan, Cham, 2020. 103–117. DOI: 10.1007/978–3–030–12874–6
13. Lundgren, Björn, and Niklas Möller. Defining information security. *Science and engineering ethics*. 2009;25.2:419–441.
14. Тараскин М.М. Комплексная защита информации в организации: монография.— Москва: Русайнс, 2017.— 353 с.— ISBN 978–5–4365–1561–8.— URL: https://book.ru/book/922538.
15. Bada, Maria, Angela M. Sasse, and Jason RC Nurse. Cyber security awareness campaigns: Why do they fail to change behaviour? 2019; arXiv preprint arXiv:1901.02672.
16. Pärn, Erika & Edwards, David. (2019). Cyber threats confronting the digital built environment: common data environment vulnerabilities and block chain deterrence. *Engineering Construction & Architectural Management*. DOI: 10.1108/ECAM-03–2018–0101

REFERENCES

1. Nye J. Jr. The Paradox of american power: why the world's only superpower can't go it alone. N.Y.: Oxford University Press; 2002. DOI: 10.1093/0195161106.001.0001
2. Nye J. Jr. Soft power: the means to success in world politics. PublicAffairs, Apr 28, 2009 — Political Science. 208 p.

3. Nye, Joseph S. Get smart: combining hard and soft power. *Affairs Foreign Affairs*. 2009;88(4):160–63. URL: http://www.jstor.org/stable/20699631.
4. Crocker, Chester A.; Hampson, Fen Osler; Aall, Pamela R. leashing the dogs of war: conflict management in a divided world. US Institute of Peace Press, 2007:13.
5. Kim V.S., Bohan Ya.A. Transformation of the «soft power» strategy of the PRC in modern conditions. *Vestnik Chelyabinskogo gosudarstvennogo universiteta. Seriya «Politicheskie nauki. Vostokovedenie» = Bulletin of the Chelyabinsk state University. Series « Political science. Orientalism»*. 2012;266(12):17–20. (In Russ.).
6. Rusakova O.F. the Concept of «soft» power in modern political philosophy. *Antinomii: Nauchnyj ezhegodnik Instituta filosofii i prava UrO RAN = Antinomies: Scientific Yearbook of The Institute of philosophy and law of the Ural Branch of the Russian Academy of Sciences*. 2010;(10):173–192. (In Russ.).
7. Radikov I.V., Leksyutina Ya.V. «Soft power» as a modern attribute of the great power. *Mirovaya ekonomika i mezhdunarodnye otnosheniya = World economy and international relations.* 2012;(2):20. (In Russ.).
8. Rusakov E.M. «…Holding a big club». *Aziya i Afrika segodnya. = Asia & Africa today*. 2011;644(3):25–33. (In Russ.).
9. Rose Andrew K. Soft power and exports. *Review of International Economics*. 2019;27.5:1573–1590.
10. Vasilenko I.A. the Role of symbolic capital of culture in the information society. *Vlast' = The Authority*. 2017;25(7):75–79. (In Russ.).
11. Ageeva A.V., Krasnotsvetov G.V. «Soft power» in the online space: practical experience of using Internet communication technologies. *Vlast' = The Authority*. 2020;28(2):96–100. (In Russ.). DOI: 10.31171/vlast.v28i2.7140
12. Tsvetkova N. Russian digital diplomacy: A rising cyber soft power? Russia's Public Diplomacy. Palgrave Macmillan, Cham, 2020:103–117. DOI: 10.1007 / 978–3–030–12874–6
13. Lundgren Björn, and Niklas Möller. Defining information security. *Science and engineering ethics*. 2019;25.2:419–441.
14. Taraskin M.M. Complex information protection in the organization: monograph. Moscow: Rusajns, 2017:353. ISBN 978–5–4365–1561–8. URL: https://book.ru/book/922538 (In Russ.).
15. Bada, Maria, Angela M. Sasse, and Jason RC Nurse. *Cyber security awareness campaigns: Why do they fail to change behaviour*? 2019; arXiv preprint arXiv:1901.02672.
16. Pärn, Erika & Edwards, David. (2019). Cyber threats confronting the digital built environment: common data environment vulnerabilities and block chain deterrence. *Engineering Construction & Architectural Management*. DOI: 10.1108/ECAM-03–2018–0101

ИНФОРМАЦИЯ ОБ АВТОРЕ

Анна Геннадьевна Глебова — доктор экономических наук, доцент, профессор Департамента мировых финансов, Финансовый университет, Москва, Россия
AGGlebova@fa.ru

ABOUT THE AUTHOR

Anna G. Glebova — Dr. Sci. (Econ.), Assoc. Prof., Prof. at Department of World Finance, Financial University, Moscow, Russia
AGGlebova@fa.ru

Статья поступила 17.09.2020; принята к публикации 20.11.2020.
Автор прочитала и одобрила окончательный вариант рукописи.
The article was received 17.09.2020; accepted for publication 20.11.2020.
The author read and approved the final version of the manuscript.