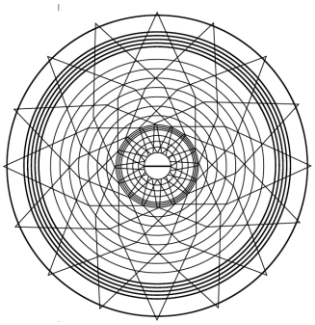




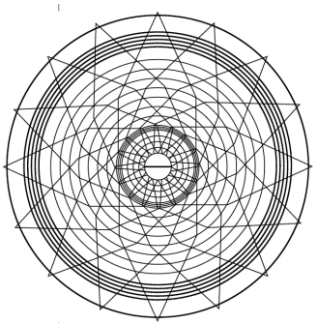
# ЭВОЛЮЦИЯ РОЛИ МЕДИА В ДОКТРИНАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ 2000 И 2016 ГОДОВ

**Кочкин А. В.**
аспирант программы «Коммуникации и медиа»
Национального исследовательского университета
«Высшая школа экономики»
(Москва, Россия)
*andrey_kochkin@mail.ru*

**Аннотация:**

В статье рассматривается актуальная проблема определения роли медиа в стратегических документах информационной политики России. В частности, анализируются две доктрины информационной безопасности, принятые с интервалом в шестнадцать лет, что позволяет выявить эволюцию понимания государством роли медиа в системе национальной безопасности. Методология исследования основана на системном подходе и включает в себя методы общенаучной группы (анализ, синтез, индукция, дедукция), а также ряд специальных методов: историографический анализ научной литературы по теме исследования; политико-правовой анализ содержания документов стратегического характера; метод сопоставительного анализа. По итогу проведенного исследования автор статьи пришел к следующим выводам: в период с 2000 по 2016 годы произошли глобальные геополитические изменения, приведшие к пересмотру государством роли медиа в обеспечении информационной безопасности. Однако, в законодательстве Российской Федерации не появилось новых определений, которые необходимы для проведения четкой информационной политики: отсутствуют такие значимые категории, как «информационный суверенитет», критерии его границ, а также нет четко прописанных понятий «внутреннее информационное пространство» и «конвергентные медиа», что не позволяет проводить системную политику по обеспечению информационной безопасности на современном этапе.

**Ключевые слова:** средства массовой информации, медиаресурс, информационная безопасность, информационное пространство, суверенитет, государственная информационная политика



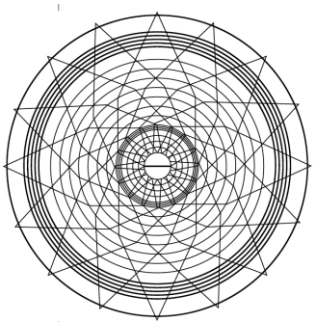
**Введение**

Актуальность темы исследования обусловлена такими процессами, как геополитическая нестабильность, быстро развивающиеся и новые технологии, нехватка доступных талантов и растущая конфликтогенность международных отношений в современном мире. В ежегодном докладе Всемирного экономического форума «Global Cybersecurity Outlook» (2023) высказываются «опасения по поводу все более фрагментированного и непредсказуемого мира», а повышение киберустойчивости во всем мире признается «одним из ключевых приоритетов всех развитых стран» (Global Cybersecurity Outlook», 2023). Эксперты Всемирного экономического форума также отмечают, что за последние пять лет «изменился характер киберугроз, поскольку произошло их смещение в информационное пространство» (Global Cybersecurity Outlook», 2023). Информационная безопасность при этом рассматривается как часть более широкого поля исследований – кибербезопасности.

**Исторические этапы развития концепции кибербезопасности**

Как научно-прикладная концепция информационная безопасность прошла очень долгий путь, который можно условно разделить на несколько крупных этапов:

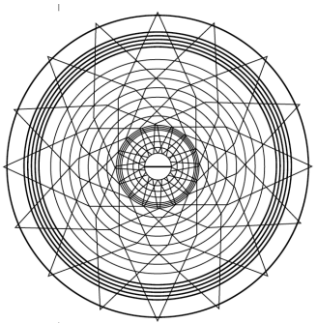
1. Начальная стадия развития, 1960-е годы, когда кибербезопасность исчерпывалась защитой паролем, а организации впервые начали более защищать свои компьютеры. В то время не было Интернета, поэтому безопасность была в основном сосредоточена на физических мерах и предотвращении доступа к работе с компьютером (Tigranovich, 2017, с. 340).
2. В 1970-е в сфере кибербезопасности возник исследовательский проект, который тогда был известен как «ARPANET» и представлял собой сеть агентств перспективных исследовательских проектов. Исследователь по имени Б. Томас создал компьютерную программу «CREEPER», которая смогла перемещать сеть ARPANET, оставляя небольшой след. Еще один исследователь, Р. Томлинсон, который изобрел электронную почту, также разработал программу, которая вывела «CREEPER» на новый уровень, сделав его самовоспроизводящимся первым в истории компьютерным вирусом. К счастью, затем он написал еще одну программу под названием «REAPER», которая удалила вирус, став примером первого в мире антивирусного программного обеспечения (Duben, 2023, с. 28). Эти первые программы послужили служили очень важной цели, выявив ряд





недостатков в сетевой безопасности «ARPANET». В то время это вызывало огромную озабоченность, так как многие крупные организации и правительства подключали свои компьютеры через телефонные линии для создания своих собственных сетей. Преступные группы также начали осознавать это, ища способы проникнуть в эти линии и украсть важные данные. Таким образом, в 1970-х годах проблема информационной безопасности появилась впервые в неотъемлемой связи с кибербезопасностью.

3. В 1980-е сеть «ARPANET» стала более широко известна как Интернет, а начиная с 1989 года стала доступна для широкой общественности. В этот период компьютеры становились все более и более связанными, компьютерные вирусы – более совершенными, а системы информационной безопасности постоянно отставили от инновационных подходов преступников, специализирующихся на взломе и краже информации. В 1988 году появилась компьютерная вирусная программа «червь Морриса» (по имени разработчика Р. Морриса), ставшая, по мнению исследователей, одним из главных поворотных моментов в истории информационной безопасности, нанеся огромный ущерб американским компаниям (Asmadi et all., 2023, с. 96). Разработчик программы стал первым человеком, которому было предъявлено обвинение в соответствии с Законом о компьютерном мошенничестве и неправомерном использовании. В результате также была сформирована «Группа реагирования на компьютерные инциденты» (CERT), целью которой стало предотвращение подобных киберинцидентов (Asadova, 2016, с. 51–67).
4. Начало 1990-х годов было отмечено следующей тенденцией: по мере того, как Интернет становился доступным для общественности, все больше и больше людей начали размещать свою личную информацию в Интернете. Организованные преступные группы увидели в этом потенциальный источник дохода, поэтому, как отмечают исследователи, к середине 1990-х годов угрозы сетевой безопасности возросли в геометрической прогрессии. Для защиты данных началась разработка первых программ защиты (Реймов, 2022, с. 555).
5. В начале 2000-х годов правительства начали пресекать преступность хакерства, вынося гораздо более серьезные приговоры виновным, включая длительное тюремное заключение и большие штрафы (Riehle, 2022). Информационная безопасность продолжала развиваться по мере роста Интернета. Преступники в ответ создали вирусы, нацеленные не



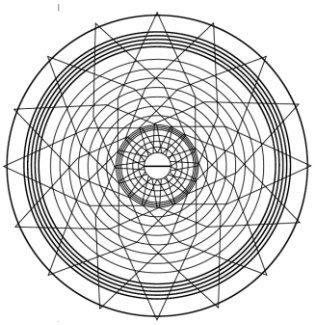
только на конкретные организации, но и на целые города, штаты и даже континенты. С 2013 года, отмеченного первой крупной утечкой информации, так называемое «дело Сноудена»[1], началась новая эпоха в развитии концепции информационной безопасности, когда меры по ее обеспечению стали приоритетом государства, вопросом суверенитета и в более широком смысле – национальной безопасности.

6. В настоящее время концепция информационная безопасность постоянно совершенствуется не только на уровне частных компаний, но и на уровне государственной политики по обеспечению национальной безопасности. К числу объектов, которые подвергаются постоянному риску утечки информации, исследователи относят современные медиаресурсы. В связи с этим можно констатировать необходимость научного осмысления доктринальных документов с точки зрения роли медиа в системе национальной безопасности (на самом широком уровне), а также в ряду конкретных мер обеспечения информационной политики. Ретроспективный анализ Доктрин информационной безопасности 2000 и 2016 годов позволяет выявить эволюцию понимания государством роли медиа в обеспечении информационной безопасности.

По мнению большинства исследователей, информационная безопасность на государственном уровне охватывает те процессы и процедуры, которые позволяют поддерживать государственный суверенитет в области информационного пространства (Грачева, 2023, с. 60).

Доктринальное выражение информационной политики включает в себя комплекс мер по предотвращению информационных угроз и рисков, которые могут нанести реальный или потенциальный вред конкретному социуму. И если на микроуровне (предприятие, домохозяйства и личные данные), информационная безопасность ограничивается в основном защитой конфиденциальной информации от несанкционированных действий, то на макроуровне государство должно предотвращать не только посягательства извне на конфиденциальность данных, но и попытки наполнить информационное пространство страны вредоносным контентом. Здесь законодатель сталкивается с необходимостью четкого определения, по крайней мере, трех ключевых понятий:

[1] Эдвард Сноуден — бывший сотрудник ЦРУ и подрядчик правительства США — скопировал и выложил во всеобщий доступ секретную информацию из Агентства национальной безопасности (АНБ), подчеркнув тот факт, что правительство фактически «шпионило» за общественностью. Для одних его считают героем, а для других — предателем.





1. Медиа (или синоним в русской научной мысли – средства массовой информации).
2. Внутреннее информационное пространство.
3. Вредоносный информационный контент.

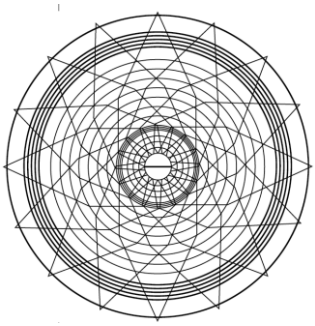
Тем не менее, четкое определение на данный момент дано только для средств массовой информации (далее – СМИ) в Федеральном законе о средствах массовой информации[2], синонимом которого в зарубежной историографии является термин «медиа», который также получил широкое распространение и в отечественной науке. В поправках к статьям 7 и 11 Федерального закона «О средствах массовой информации», принятых в 2023 году[3], появилось пояснение о том, кто именно может выступать в качестве учредителя СМИ (при запрете на такую деятельность для нерезидентов и лиц без гражданства), а также была уточнена ответственность СМИ за распространение материалов экстремистского характера и за осуществление экстремистской деятельности. Однако, для обеспечения информационной безопасности этих пояснений явно недостаточно несмотря на то, что они свидетельствуют о понимании значения медиаконтента для информационной ситуации в стране.

В рамках исследуемой проблематики также необходимо уточнить, что информационная безопасность отличается от кибербезопасности как по объему, так и по назначению. В отечественной науке эти два термина часто используются взаимозаменяемо (Левда, 2023, с. 551), однако по своей сути кибербезопасность является подкатегорией информационной безопасности. Кибербезопасность в первую очередь направлена на устранение угроз, связанных с технологиями, с помощью методов и инструментов, которые могут предотвратить или смягчить их.

Другой важной категорией является безопасность данных, которая фокусируется на защите данных организации от случайного или злонамеренного воздействия на посторонние стороны. Учитывая приведенные выше различия в терминологии, в нашем исследовании рассматривается широкое определение информационной безопасности на макроуровне, то есть на уровне государства. Большинство исследователей сходятся во мнении, что политика информационной безопасности на государственном уровне должна быть представлена набором четких правил, которыми руководствуются СМИ при работе с информацией (Piper,

[2] Закон РФ от 27 декабря 1991 г. № 2124-I «О средствах массовой информации». (1992). Гарант. https://base.garant.ru/10164247/

[3] Федеральный закон от 13 июня 2023 г. № 227-ФЗ «О внесении изменений в статьи 7 и 11 Закона Российской Федерации «О средствах массовой информации». (2023). Гарант. https://www.garant.ru/products/ipo/prime/doc/406931048/



2023). Речь идет не о цензуре, как полагают некоторые западные исследователи (Collier, Morton, Alharthi, Kleiner, 2023), а именно о наборе регуляторных принципов, следование которым должно отслеживаться, поощряться, а нарушение должно наказываться как в рамках административного, так и уголовного кодексов. При этом необходима четко выстроенная законодательная работа по определению границ внутреннего информационного пространства, выявлению новых вызовов и потенциальных угроз (Willie, 2022).

Некоторые авторы включают в рамки внутреннего информационного пространства все социальные сети, телеканалы, интернет-ресурсы, которые обслуживают языковую аудиторию титульной нации, исключая этнические меньшинства, для которых существуют программы на их национальных языках (Демина, 2018, с. 176). В то же время исследователи полагают, что исключать из информационного пространства этнические меньшинства нельзя, поскольку возникают информационные лакуны, заполняемые в том числе и вредоносным контентом (Грачева, 2023, с. 58; Хуа Ли, 2019).

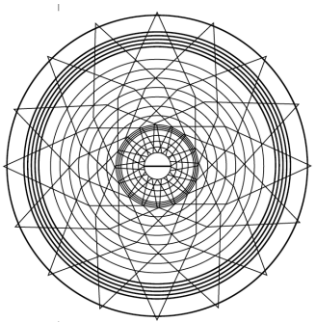
В России разработка законодательного обеспечения мер для формирования системы информационной безопасности началась с принятия в 2000 году «Доктрины информационной безопасности Российской Федерации»[4] и была развита в аналогичном документе, принятом в 2016 году[5]. При этом трактовка роли медиа в обществе с позиций обеспечения национальной безопасности претерпела важные качественные изменения, требующие отдельного изучения для понимания государственной политики в отношении СМИ.

**Обзор литературы**

Историография темы достаточно обширна и включает в себя работы как отечественных, так и зарубежных авторов. В частности, общетеоретические положения, касающиеся определения, структуры и методов обеспечения информационной безопасности на уровне государства, рассмотрены в работах таких авторов, как Е. А. Грачевой (Грачева, 2023), М. В. Левды (Левда, 2017), Н. В. Сидельникова, Т. В. Беседина (Сидельникова, Беседина, 2018), А. Д. Чесноков (Чесноков, 2022), Ф. М. Мухтаров (Mukhtarov, 2022) и др. Например, в исследованиях Н. В. Кардавы (2018) поднимается проблема терминологии, обеспечивающей научные изыскания в исследуемой теме: определяется сущность терминов «киберпространство» и «информационное пространство»,

[4] Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ от 9 сентября 2000 г. N° Пр-1895). (2000). Гарант. https://base.garant.ru/182535/

[5] Указ Президента РФ от 5 декабря 2016 г. N° 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». (2016). Гарант. https://base.garant.ru/71556224/



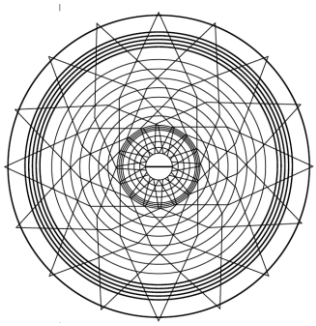


причем основное отличие в данном случае проводится на основе иерархии между первым и вторым понятием. Так, киберпространство, в отличие от информационного, включает в себя не только цифровые (виртуальные), но и физические объекты. Информационное пространство государства рассматривается при этом как новая политическая и социально-экономическая реальность (Кардава, 2018, с. 159).

Методологические подходы к миссии и целям медиа в контексте политических процессов и геополитических тенденций рассматриваются в работе И. Н. Деминой (Демина 2018), а также в исследованиях Р. И. Милешевич (Милешевич, 2014), А. Ю. Суворовой (Суворова, 2017), Г. С. Мельник, С. Б. Никонова (Мельник, Никонова, 2019) и др. В частности, в работе И.Н. Деминой отмечается такой важный методологический аспект, как выбор подхода к исследованию роли медиа в обеспечении информационной безопасности, поскольку в современных условиях медиа можно рассматривать и как инструмент обеспечения информационной безопасности, и как потенциальную площадку для утечки важных данных» (Демина, 2018, с. 174).

Зарубежные авторы в основном уделяют внимание эмпирическим исследованиям информационной безопасности. Так, среди белорусских исследований интерес вызывает работа Е. В. Артеменко, в которой проанализированы ответные меры на вызовы информационной безопасности белорусских законодателей (Artiomenko, 2020), чей опыт может быть ценен для российской практики.

С позиций культурологического подхода проблемы информационной безопасности рассматривают Н. Коллиер, Ч. Мортон, Д. Альхарти, Дж. Кляйнер (Collier, Morton, Alharthi, Kleiner, 2023). Вопросы обеспечения государственной информационной безопасности через призму внутреннего информационного пространства проанализированы в работах Дж. Даунинга (Downing, 2023; Downing, 2023). Автор пытается решить, в частности, проблему определения границ информационного пространства страны, применяя языковой критерий: русскоязычное, англоязычное, немецкоязычное и т. п. информационное пространство. Данный критерий может быть, с одной стороны, спорным, по причине опоры на ограниченную языковым признаком целевую аудиторию, что недостаточно для широты охвата современных медиа. С другой стороны, данный критерий может быть востребован законодателем с такой позиции, как отслеживание вредоносного информационного контента, распространяемого через медиаресурсы на языке титульной нации или на государственных языках. Отдельно возникает вопрос о соотношении цензуры и свободы СМИ, который



поднимается в работах таких исследователей, как З. А. Азадова (Asadova, 2016), А. Асмади, Х. Альмутахар (Asmadi, Almutahar, Sukamto, 2023). Моделирование поведения руководителей СМИ в области цифровой безопасности для противодействия манипуляциям в социальных сетях рассмотрено в исследовании К. Маатуиса и С. Чокалингама (Maathuis, Chockalingam, 2023), причем в данной работе представлены конкретные прикладные инструкции по обеспечению безопасности пользователей сетевых сообществ.

Тем не менее, несмотря на довольно обширную историографию, проблематика восприятия роли медиа в обеспечении информационной безопасности России, исходя из декларируемых принципов в доктринальных документах стратегического характера, требует дополнительного изучения.

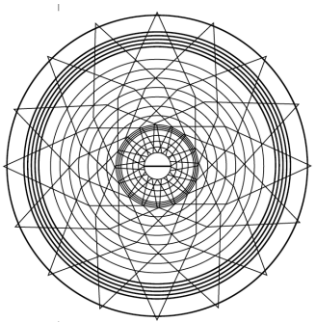
Методология исследования основана на системном подходе и включает в себя группу общенаучных методов (анализ, синтез, индукция, дедукция). Системный подход предполагает рассмотрение информационной безопасности как системы государственных и частных мер, все элементы которой взаимосвязаны друг с другом и нацелены на единую функцию – выполнение защиты данных (информации).

В рамках проведенного исследования был также использован ряд специальных методов:

- историографический анализ научной литературы по теме исследования, который позволил выявить основные теоретические подходы к исследованию феномена «информационная безопасность» в современной отечественной и зарубежной политико-правовой литературе;
- нормативно-правовой анализ, который заключался в сопоставлении двух документов, имеющих доктринальный характер и концептуализирующих отношение государства к проблеме обеспечения информационной безопасности;
- метод текстологического анализа, который позволяет на базе сопоставления выявить основные положения, идеи и определения, отраженные в двух документах.

Отражение роли медиа в Доктринах информационной безопасности Российской Федерации 2000 и 2016 годов

Среди стратегически важных актов, регулирующих сферу информационной государственной политики, в качестве объекта анализа представляют интерес «Доктрина информационной безопасности РФ» 2000 года и одноименный документ, принятый в 2016 году.





В Доктрине 2000 года основной акцент делается на кибератаках как на наиболее распространенной в то время угрозе информационной безопасности[6]. В новом документе дана более широкая трактовка информационных угроз, а под информационной безопасностью Российской Федерации понимается «состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз»[7]. Под субъектами угроз информационной безопасности понимаются не только криминальные структуры, но и «общественные организации, коммерческие учреждения, и правительственные органы зарубежных стран»[8].

В Доктрине 2016 года отмечаются такие угрозы, как фальсификация исторических событий, направленная на «подрыв исторических основ и патриотических традиций, связанных с защитой Отечества», а также тот факт, что «российские СМИ зачастую подвергаются за рубежом дискриминации, российским журналистам создаются препятствия для осуществления их профессиональной деятельности»[9]. При этом, в новом документе уже появляется понимание того факта, что задачи обеспечения информационной безопасности осложняются отсутствием границ самого информационного пространства. Однако, сопоставительный анализ двух доктрин показал, что в обоих документах отсутствуют такие понятия, как внутреннее информационное пространство, информационный суверенитет, а также нет самого термина «медиа», вместо него используется понятие «средства массовой информации».

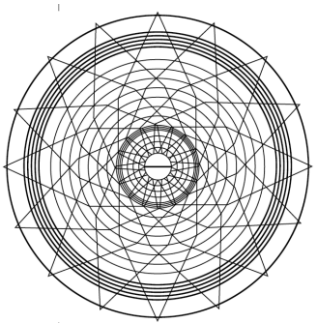
То есть, на уровне государственной стратегии не проводится различие между СМИ и медиа несмотря на то, что в некоторых отечественных исследованиях делаются попытки искусственно разграничить данные понятия, при более широкой трактовке категории «медиа» (Мельник, Никонов 2014; Суворова 2017). В Доктрине информационной безопасности Российской Федерации, разработанной в 2016 году с учетом изменившихся реалий, отмечается, что развитие информационных технологий является одновременно «ключевым фактором

[6] Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ от 9 сентября 2000 г. N° Пр-1895). (2000). Гарант. https://base.garant.ru/182535/

[7] Указ Президента РФ от 5 декабря 2016 г. N° 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». (2016). Гарант. https://base.garant.ru/71556224/

[8] Указ Президента РФ от 5 декабря 2016 г. N° 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». (2016). Гарант. https://base.garant.ru/71556224/

[9] Указ Президента РФ от 5 декабря 2016 г. N° 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». (2016). Гарант. https://base.garant.ru/71556224/



экономического роста и повышения качества работы министерств и ведомств и создает новые угрозы информационной безопасности глобального характера»[10].

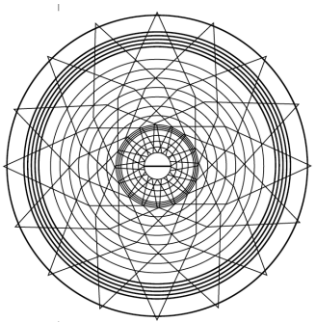
В документе 2016 года особенно подчеркивается, что информация не имеет границ, ее распространению невозможно помешать на уровне национального законодательства. Для определения вредоносного контента в Доктрине 2016 года введено такое понятие, как «трансграничный трафик информации», который используется для нанесения ущерба государству в геологическом, военном, социально-экономическом отношениях[11].

Согласно Доктрине 2016 года, нанесением ущерба государственному суверенитету занимаются не только криминальные структуры, но и недружественные государства, которые находятся в состоянии геополитического соперничества с Россией»[12]. Отметим, что в обоих документах не упоминается прямо перечень тех стран, которые своей информационной политикой наносят или стремятся нанести Российской Федерации геополитический, военный или социально-экономический ущерб.

В Доктрине 2016 года также отмечается, что социально безответственное внедрение информационных технологий при низком уровне их безопасности становится серьезным риском для информационных утечек в большем объеме, особенно в экономической среде. В сфере медиа на национальном уровне в Доктрине 2016 года, в отличие от предыдущего документа, определены следующие основные угрозы:

- повышение потенциала иностранных государств в области информационных технологий, используемых для воздействия на ключевую инфраструктуру России в военных целях;
- увеличение использования спецслужбами этих стран средств информационно-психологического воздействия на граждан Российской Федерации для подрыва внутренней стабильности;
- активная критика России в западных СМИ, подрыв ее авторитета на международной арене, противодействие работе российских СМИ;
- усиление воздействия на молодежь, направленное на обесценивание морально-этических ценностей, вовлечение их в деятельность деструктивных субъектов;

[10] Указ Президента РФ от 5 декабря 2016 г. N° 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». (2016). Гарант. https://base.garant.ru/71556224/
[11] Указ Президента РФ от 5 декабря 2016 г. N° 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». (2016). Гарант. https://base.garant.ru/71556224/
[12] Указ Президента РФ от 5 декабря 2016 г. N° 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». (2016). Гарант. https://base.garant.ru/71556224/





- использование экстремистскими группировками средств массовой информации и ресурсов для разжигания межнациональной и межконфессиональной розни;
- увеличение количества преступлений в сфере компьютерных технологий, прежде всего в сфере финансово-кредитных отношений.

В качестве угрозы информационной безопасности также рассматривается «комплекс действий иностранных государств направлен на подрыв суверенитета России и укрепление собственных геополитических позиций» [13].

Медленное развитие отечественных информационных технологий и электронной промышленности становится самостоятельной угрозой. Наряду с этим, в России наблюдается отставание в научных исследованиях и образовании, слабый кадровый потенциал, низкий уровень подготовки IT-специалистов. С точки зрения прав человека информационная безопасность личности находится под угрозой из-за недостаточной информированности граждан о реальных опасностях и их возможностях по защите своих прав и интересов.

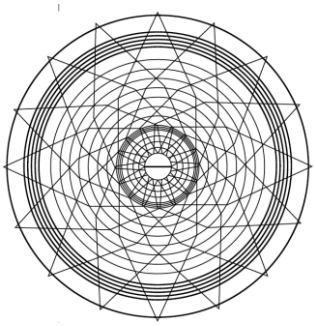
В рамках выявленных угроз Доктрина 2016 года определяются следующие цели:

а) в области обороны – защита интересов личности, общества и государства от любых посягательств военно-политического характера, наносящих ущерб суверенитету и геополитической стабильности России. Средствами достижения этой цели являются стратегическое сдерживание, совершенствование системы информационной безопасности, прогнозирование угроз, нейтрализация психологического воздействия, защита интересов союзников России в идеологической войне;

б) в сфере внутренней политики – защита суверенитета, поддержка общественно-политической стабильности, противодействие угрозам, исходящим от экстремистских организаций, защита критической информационной инфраструктуры. Среди применяемых средств – противодействие враждебной идеологии, пресечение преступлений, совершаемых в сфере информационной безопасности, усиление защиты информационной инфраструктуры;

в) в экономической сфере – минимизация негативного влияния информационных факторов на развитие экономики, на разработку и внедрение новых компьютерных технологий, а также повышение

[13] Указ Президента РФ от 5 декабря 2016 г. N° 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». (2016). Гарант. https://base.garant.ru/71556224/



конкурентоспособности российской электронной промышленности и сферы разработки программного обеспечения;

г) в области науки и техники – повышение качества научных исследований и разработок, наращивание кадрового потенциала.

Планомерная реализация этих целей должна привести к обеспечению информационной безопасности Российской Федерации в полном объеме.

Таким образом, можно констатировать, что новая Доктрина информационной безопасности Российской Федерации, вступившая в силу 6 декабря 2016 года, имеет существенные отличия от предыдущей версии документа, которая была принята в 2000 году. Исследователи отмечают, что концентрация основных положений документа вокруг стратегических интересов страны, а не вокруг угроз, позволила добиться более четкого, целостного и системного изложения концепции безопасности.

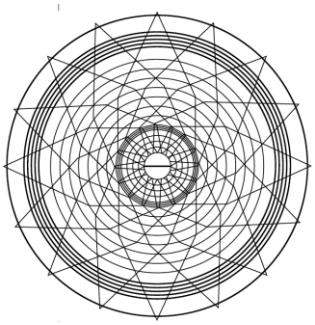
Информационные технологии в версии 2000 года рассматривались как фактор, влияние которого на внутреннюю и внешнюю политику растет. В новой редакции они рассматриваются уже не как фактор, а как среда, в которой происходит реализация национальных интересов.

Среди совершенно новых концептуальных положений Доктрины информационной безопасности:

- необходимость импортозамещения в электронной промышленности и в разработке программных продуктов;
- появление на нормативном уровне понятия критической информационной инфраструктуры;
- противодействие кибератакам.

Риски, связанные с монополизацией средств массовой информации, источников формирования и распространения информационных сообщений, полностью исчезли из Доктрины. Развитие сети информационных агентств и российских электронных СМИ снизило значимость этой угрозы национальной безопасности Российской Федерации. Также в предыдущей версии документа акцентировалось внимание на недостаточном правовом регулировании сферы информационных технологий и информационной безопасности. За прошедшие годы опасные пробелы в законодательстве были закрыты путем принятия системообразующих законов, например, Федеральный закон РФ «Об информации, информационных технологиях и о защите информации» [14] ,

[14] Федеральный закон от 27 июля 2006 г. N° 149-ФЗ «Об информации, информационных технологиях и о защите информации». (2006). Гарант. https://base.garant.ru/12148555/





Федеральный закон РФ «О персональных данных»[15], а также целым рядом подзаконных актов, определяющих методологию их применения.

Существенным нововведением стало появление в Доктрине новых субъектов, помимо органов государственной власти, на которых возложены задачи по обеспечению национальной информационной безопасности. Оно:

- собственники объектов критической информационной инфраструктуры, их арендаторы или юридические лица, эксплуатирующие их на иных законных основаниях;
- печатные и электронные средства массовой информации;
- участники финансового рынка;
- операторы связи и Интернет-провайдеры;
- собственники и операторы объектов, входящих в состав информационных систем;
- образовательные и научные организации, работающие в области информационной безопасности;
- общественные объединения, осуществляющие деятельность в сфере гражданского общества.

Все они играют свою роль в обеспечении национальных интересов, а также защите прав и свобод личности.

Результаты сопоставительного анализа представлены в Таблице 1 на следующей странице.

С точки зрения роли СМИ в контексте национальной безопасности особый интерес представляют статьи 15 и 23 Доктрины 2016 года, в которых появляется четкое представление государства о роли СМИ как инструмента негативного внешнего влияния на состояние общества:

«Статья 15. Состояние информационной безопасности в области обороны страны характеризуется увеличением масштабов применения отдельными государствами и организациями информационных технологий в военно-политических целях, в том числе для осуществления действий, противоречащих международному праву, направленных на подрыв суверенитета, политической и социальной стабильности, территориальной целостности Российской Федерации и ее союзников и представляющих угрозу международному миру, глобальной и региональной безопасности» [16].

[15] Федеральный закон от 27 июля 2006 г. N° 152-ФЗ «О персональных данных». (2006). Гарант. https://base.garant.ru/12148567/

[16] Указ Президента РФ от 5 декабря 2016 г. N° 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». (2016). Гарант. https://base.garant.ru/71556224/

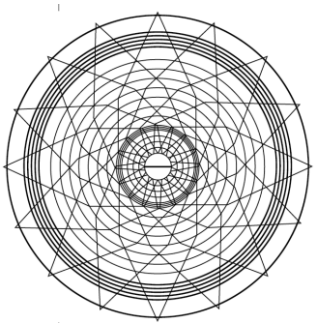
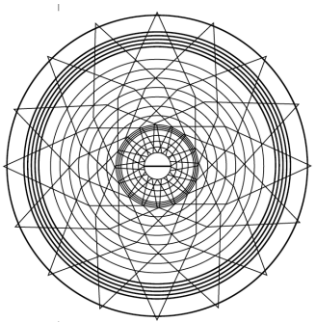


**Таблица 1.** Роль медиа в доктринах информационной безопасности

| **Наименование документа** | **Роль медиа** |
|---|---|
| Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ от 9 сентября 2000 г. N° Пр-1895) // Российская газета. – 2000. – N° 187. | СМИ (медиа) рассматривается как часть стратегии государства для позиционирования патриотических ценностей. Отмечается влияние информационных технологий на национальные интересы государства. Информационные технологии не анализируются с позиций расширения влияния зарубежных СМИ.<br>Фактически данный документ развивал положения о СМИ, декларированные в Концепции национальной безопасности РФ, без разграничений на иностранное и отечественное производство информационных потоков.<br>Технологический аспект информационной политики рассматривается как часть общего технического прогресса. То есть, в данном документе отсутствует определение конвергентных СМИ. Не отмечена роль медиа в оборонной сфере. |
| Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ от 5 декабря 2016 г. N° 646) // Собрание законодательства Российской Федерации. – 2016. – N° 50. – Ст. 7074. | Сфера информационных технологий рассматривается как непосредственная часть жизни общества. Понятие информационная безопасность расширено до первого приоритета государственной информационной политики.<br>Выведены четкие принципы реализации информационной политики в отношении:<br>- угроз нарушения безопасности и устойчивости функционирования критической информационной<br>- инфраструктуры РФ;<br>- деятельности, которая связана с использованием информационных и коммуникационных технологий в экстремистской деятельности.<br>СМИ рассматриваются как инструмент, а не только объект информационной политики.<br>Конвергентные СМИ не рассматриваются как отдельная область государственного регулирования, однако отмечается, что расширение внедрения цифровых технологий, помимо экономической пользы, приносит и новые риски информационных угроз. Отмечается, что СМИ могут использоваться враждебными государствами как инструмент для |





| **Наименование документа** | **Роль медиа** |
|---|---|
| | наращивания негативного влияния на молодежь с целью разрушения традиционных ценностей. |

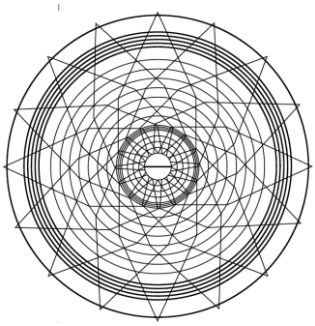
В статье 23 в качестве основного направления обеспечения информационной безопасности названо противодействие «использованию информационных технологий для пропаганды экстремистской идеологии, распространения ксенофобии, идей национальной исключительности в целях подрыва суверенитета, политической и социальной стабильности, насильственного изменения конституционного строя, нарушения территориальной целостности Российской Федерации; пресечение деятельности, наносящей ущерб национальной безопасности Российской Федерации, осуществляемой с использованием технических средств и информационных технологий специальными службами и организациями иностранных государств, а также отдельными лицами» [17].

Также в Доктрине 2016 года декларируется необходимость повышения «защищенности критической информационной инфраструктуры и устойчивости ее функционирования, развитие механизмов обнаружения и предупреждения информационных угроз и ликвидации последствий их проявления, повышение защищенности граждан и территорий от последствий чрезвычайных ситуаций, вызванных информационно-техническим воздействием на объекты критической информационной инфраструктуры» [18].

Тем не менее, в статье 23 (пункты д, г, е) уже наблюдается некая путаница понятий, поскольку в прочих пунктах речь идет уже не о информационной, а о кибербезопасности, различие между которыми мы отмечали выше: речь фактически идет о защите данных государственных оборонных предприятий, объектов критической инфраструктуры В этом ряжу также перечисляются категории информации, которые подлежат защите: сведения, составляющие государственную тайну, иную информацию ограниченного доступа и распространения, в том числе за счет повышения защищенности

[17] Федеральный закон от 13 июня 2023 г. N° 227-ФЗ «О внесении изменений в статьи 7 и 11 Закона Российской Федерации «О средствах массовой информации». (2023). Гарант. https://www.garant.ru/products/ipo/prime/doc/406931048/

[18] Федеральный закон от 13 июня 2023 г. N° 227-ФЗ «О внесении изменений в статьи 7 и 11 Закона Российской Федерации «О средствах массовой информации». (2023). Гарант. https://www.garant.ru/products/ipo/prime/doc/406931048/



соответствующих информационных технологий[19]. То есть, половина доктрины посвящена проблеме обеспечения кибербезопасности в рамках более широкой концепции безопасности информационной. При этом в двух доктринах отсутствуют ключевые понятия, связанные с реальными мерами, необходимыми для обеспечения безопасности. В итоге за декларативными принципами остается неясным, что, от кого и каким именно образом необходимо защищать и какую роль играют в такой политике СМИ.

Организационные основы и пути реализации положений Доктрины информационной безопасности РФ 2016 года

По сравнению с документом 2000 года, реализация новой Доктрины информационной безопасности Российской Федерации происходит на трех уровнях: нормативном, экономическом и организационном. В каждом из направлений выделяются векторы интенсивного и ускоренного развития, позволяющие реализовать приоритетные национальные интересы.

В сфере законотворческой деятельности в сферах информационной безопасности взят курс на выявление отдельных объектов защиты. Так, был принят Закон об объектах критической инфраструктуры [20], в котором законодатель установил нормы и правила, определяющие требования к информационной безопасности этих объектов.

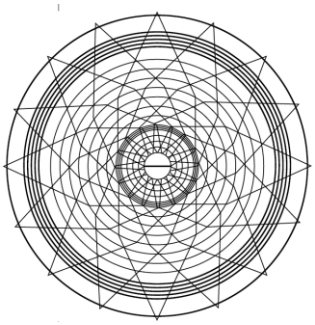
Еще одним важным документом стал закон о фейковых новостях. Его принятие должно обеспечить попадание в информационную среду только достоверных сообщений, не допустить использования средств массовой информации и публикуемых в них ложных сообщений для дестабилизации обстановки в России, разжигания межнациональной и межконфессиональной розни.

Еще одной сферой, которая затронута Доктриной 2016 года, является стратегия импортозамещения в производстве компонентов для электронной промышленности и программных продуктов основана на необходимости автаркии, или полной независимости, в критической области информационной безопасности.

Отсутствие самостоятельности было не единственной причиной стремления к импортозамещению. По мнению некоторых исследователей, в период

[19] Федеральный закон от 13 июня 2023 г. N° 227-ФЗ «О внесении изменений в статьи 7 и 11 Закона Российской Федерации «О средствах массовой информации». (2023). Гарант. https://www.garant.ru/products/ipo/prime/doc/406931048/

[20] Федеральный закон от 26 июля 2017 г. N° 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (с изменениями и дополнениями). (2017). Гарант. https://base.garant.ru/71730198/





очередного обострения отношения с Западом, для суверенитета России само по себе использование зарубежных программных продуктов представляет потенциальную опасность (Бердникова, Лукьянчикова, 2019). Также исследователи отмечают, что некоторые виды процессоров были запрещены к закупке МВД или Минобороны (Грачева, 2023, с. 58). Таким образом, можно констатировать, что импортозамещение, только обозначенное как стратегическая цель в версии 2000 года, вышло на первый план в новой Доктрине 2016 года. В целях реализации этой части стратегии создаются преференции для отечественных разработчиков программных продуктов и средств защиты информации, в том числе с участием в госзаказах.

В рамках реализации стратегии были приняты решения по поддержке компаний:

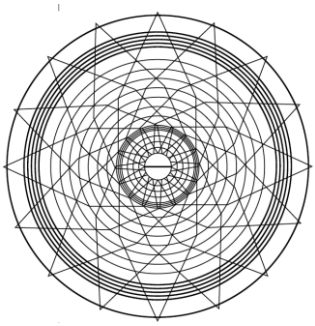
- оказание услуг в области информационной безопасности как для Российской Федерации в целом, так и для бизнеса и граждан;
- разработка и производство программно-технических средств обеспечения информационной безопасности;
- государственные и частные учреждения и организации, осуществляющие научную и образовательную деятельность в этих областях.

Создание благоприятных условий для деятельности российских ИТ-компаний становится одним из основных экономических методов реализации положений Доктрины информационной безопасности Российской Федерации. Достижению этой цели способствуют гранты на развитие, создание инновационных центров и кластеров, льготные налоговые режимы для компаний-резидентов зон опережающего развития.

Российская продукция в области информационной безопасности, благодаря улучшенному качеству и надежности, уже стала экспортной статьей.

**Организационные методы реализации Доктрины информационной безопасности РФ 2016 года**

Среди важнейших организационных мероприятий, посвященных реализации положений Доктрины 2016 в сфере информационной безопасности, можно выделить создание единой системы государственного управления в этой сфере. Перед государственными органами стоит задача укрепления вертикали управления в том числе – критической информационной инфраструктурой. В то же время, из содержания документа на совсем ясно, какая именно информационная инфраструктура понимается как критически важная для национальной безопасности. Данное определение было представлено на год



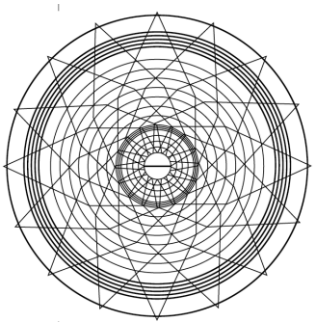
позднее, в вышеупомянутом Федеральном законе «О безопасности критической информационной инфраструктуры Российской Федерации» 2017 года[21].

В обоих документах, однако, указывается на важность углубления сотрудничества и взаимодействия всех сил, служб и государственных органов, ответственных за обеспечение информационной безопасности. В Доктрине 2016 года оговорено, что данный параметр обеспечения информационной безопасности должен достигаться в том числе путем проведения учений. Тем не менее, не указывается, в компетенции каких ведомств и на каких именно площадках или полигонах должны проводиться такого рода учения. В новой Доктрине, в отличие от документа 2000 года, также предлагается совершенствовать «инструментарий анализа» и углублять научные исследования в области информационной безопасности, привлекать бизнес и структуры гражданского общества к сотрудничеству с государством в этой сфере. научных исследований в области информационной безопасности;

Среди проектов, уже реализованных в России на основе положений и принципов Доктрины 2016 года, можно выделить следующие:

1. Создана система «ГосСОПКА»22 для предотвращения, обнаружения и ликвидации неблагоприятных последствий атак на информационные системы. На основании указа президента координационные центры «ГосСОПКА» создаются на базе как государственных органов, так и корпоративных систем. За проект отвечает ФСБ России. Все владельцы объектов критической информационной инфраструктуры должны подключаться к системе;
2. Создано специальное подразделение Центрального банка России под названием «ФинЦЕРТ»23, отвечающее за защиту информационных систем финансовых организаций от кибератак;
3. Сформирован аппаратно-программный комплекс «Безопасный город»24 в рамках профильного Министерства чрезвычайных ситуаций, который представляет собой информационную систему, предназначенную для

[21] Федеральный закон от 26 июля 2017 г. N° 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (с изменениями и дополнениями). (2017). Гарант. https://base.garant.ru/71730198/
[22] ГосСОПКА. Информзащита. (2023). https://www.infosec.ru/glavnye-temy/gossopka/
[23] ФинЦЕРТ. Банк России. (2023). https://www.cbr.ru/information_security/fincert/
[24] Аппаратно-программный комплекс Безопасный город. (2023). https://mchs.gov.ru/dokumenty/gosudarstvennye-i-federalnye-celevye-vedomstvennye-programmy/apparatno-programmnyy-kompleks-bezopasnyy-gorod





существенного снижения количества техногенных и информационно-индуцированных аварий в городской среде.

Помимо вышеперечисленного, для реализации доктринальных положений 2016 года на государственной уровне планируется решить такие задачи, как:

- наращивание количества высокопрофессиональных кадров, поскольку Россия уже нуждается почти в миллионе специалистов в области информационных технологий и информационной безопасности;
- реализация стратегии суверенного Рунета. Законопроект пока находится на стадии обсуждения.

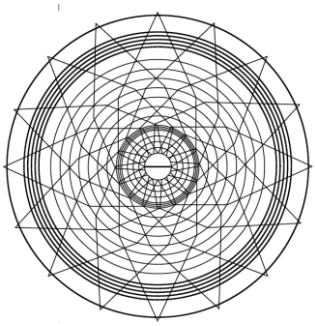
Реализация положений новой Доктрины информационной безопасности призвана не только защитить информационную инфраструктуру Российской Федерации от посягательств, а бизнес и граждан от ущемления их интересов, но и усилить влияние России на геополитические процессы на основе международного права. Тем не менее, до сих пор не предпринято специальных мер для обеспечения фильтрации вредоносного информационного трафика в русскоязычном информационном пространстве. Ограничения деятельности медиаресурсов, которые распространяют такой трафик, в основном нацелены на участие иностранного капитала в структуре медиакомпаний (например, присвоение статуса «иностранный агент»). Однако, для нейтрализации такой угрозы необходим более тщательно разработанный комплекс мер по пресечению негативного информационного воздействия.

**Заключение**

Проведенный анализ Доктрин информационной безопасности РФ 2000 и 2016 года позволяет сформулировать следующие выводы:

За шестнадцать лет, прошедших со времени принятия первой доктрины, произошли глобальные геополитические сдвиги, приведшие к переходу Крыма под юрисдикцию России, к обострению отношений с Украиной, к началу полномасштабной информационной войны с западными державами. Поэтому положения, актуальные на 2000 год, были пересмотрены после событий 2014 года, и впервые средства массовой информации были рассмотрены государством как существенный ресурс в гибридной войне. При этом, по сравнению с документом 2000 года, в новой Доктрине 2016 года не появилось новых определений, которые необходимы для проведения четкой информационной политики.

1. Для развития положений, декларированных в Доктрине 2016 года, необходимо системное проведение государственной политики в области формирования внутреннего информационного пространства. Более того, необходимо внедрение и соответствующее законодательное разъяснение термина «информационный суверенитет», что позволит разграничить деятельность иностранных СМИ, медиаресурсов с иностранным капиталом



и работу отечественных информационных каналов как игроков в информационном поле и выявить границы их деятельности в рамках внутреннего информационного пространства страны. Основным критерием для выделения такого пространства должен стать русский язык, как основной ресурс коммуникации на территории Российской Федерации.

2. С целью реализации заявленных в Доктрине 2016 года положений, необходимо также цензурирование тех программ, которые выходят на государственных каналах или на каналах с участием государственного капитала, с позиций проверки журналистской этики, нравственности и профессиональной адекватности. В то же время, необходимо обеспечить максимальную прозрачность источников финансирования медиаресурсов, работающих в русскоязычном информационном пространстве. Особенно это касается конвергентных СМИ, которые обладают широким вещанием на масштабные целевые аудитории. В противном случае, информационный суверенитет так и останется недостижимым для российского информационного пространства.

**БИБЛИОГРАФИЯ**

Бердникова, Э. Н., Лукьянчикова, М. В. (2019). Медиаобразование как важнейший фактор обеспечения безопасности конфиденциальных данных. Российская школа связей с общественностью, (12), 128–141.

ГосСОПКА. Информзащита. 2023. https://www.infosec.ru/glavnye–temy/gossopka/

Грачева, Е. А. (2023). Информационная безопасность. The Newman in Foreign policy, (5), 57–60.

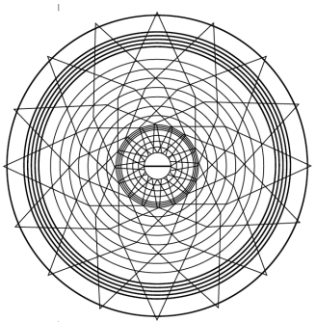
Демина, И. Н. (2018). Методологические подходы к миссии и целям медиасистемы. Вопросы теории и практики журналистики, (1), 172–182.

Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ от 9 сентября 2000 г. N° Пр–1895) (2000). Российская газета, 187.

Закон РФ от 27 декабря 1991 г. N° 2124–I «О средствах массовой информации» (1992). Российская газета, 32.

Кардава, Н. В. (2018). Киберпространство как новая политическая реальность: вызовы и ответы. История и современность, (2), 152–166.

Левда, М. В. (2017). Информационная безопасность РФ. Форум молодых ученых, (11), 549–554.





Мелешевич, Р. И. (2019). Конвергенция в медиасреде: к вопросу определения понятия. Труды БГТУ. Серия 4: Принт– и медиатехнологии, (1), 83–88.

Мельник, Г. С., Никонов, С.Б. (2014). Медийный компонент в доктрине информационной безопасности. Управленческое консультирование, (1), 18–28.

Реймов, Б. Е. (2022). Киберпреступность: современное состояние и актуальные проблемы. Ta'lim fidoyilari, (7), 555–561.

Сидельникова, Н. В., Беседина, Т. В. (2018). Информационная безопасность. Образование. Карьера. Общество, (1), 71–78.

Суворова, А. Ю. (2017). Роль новых медиа в контексте медиатизации политических процессов. Коммуникология, (1), 69–78.

Указ Президента РФ от 5 декабря 2016 г. N° 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» (2016). Собрание законодательства Российской Федерации, 50, 7074.

Федеральный закон от 13 июня 2023 г. N° 227–ФЗ «О внесении изменений в статьи 7 и 11 Закона Российской Федерации «О средствах массовой информации» (2023). Собрание законодательства Российской Федерации, 25, 4416.

Федеральный закон от 26 июля 2017 г. N° 187–ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (с изменениями и дополнениями). (2017). Гарант. https://base.garant.ru/71730198/

Федеральный закон от 27 июля 2006 г. N° 149–ФЗ «Об информации, информационных технологиях и о защите информации». (2006). Гарант. https://base.garant.ru/12148555/

Федеральный закон от 27 июля 2006 г. N° 152–ФЗ «О персональных данных». (2006). Гарант. https://base.garant.ru/12148567/

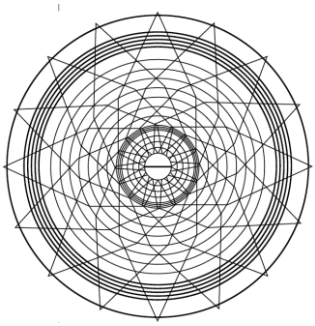
ФинЦЕРТ. Банк России. (2023). https://www.cbr.ru/information_security/fincert/

Хуа, Ли (2019). Кибербезопасность в России в свете Доктрины информационной безопасности РФ 2016 года. Мир русскоговорящих стран, (2), 11–21.

Чесноков, А. Д. (2022). Информационная безопасность. student, (1), 478–489.

Artiomenko, E. (2020). Mass media: responses to information security challenges. Belarusian Yearbook, 124–132.

Asadova, Z. A. (2016). Information security in the countries of Central Asia: the case of Kazakhstan. MGIMO Review of International Relations, (6), 51–67.



Asmadi, A., Almutahar, H., Sukamto, S. (2023). Digital Information Security Policy in the National Security Strategy, International Journal of Multidisciplinary Approach Research and Science, (1), 96–103.

Collier, H., Morton, Ch., Alharthi, D., Kleiner, J. (2023). Cultural Influences on Information Security. University of Colorado Colorado Springs, 188 p.

Downing, J. (2023). Social Media, Digital Methods and Critical Security Studies. In book: Critical Security Studies in the Digital Age, 71–108.

Downing, J. (2023). Social Media, Security and Democracy in the Digital Age. In book: Critical Security Studies in the Digital Age, 179–207.

Duben, A.K. (2023). Experience of international cooperation in the field of information security: problems and prospects. International Law and International Organizations, 3, 22–34.

Global Cybersecurity Outlook (2023). https://initiatives.weforum.org/global–cyber–outlook/home

Maathuis, C., Chockalingam, S. (2023). Modelling Responsible Digital Security Behaviour for Countering Social Media Manipulation. Indian Institute for Energy Technology, 203 p.

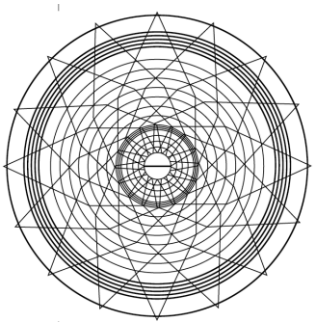
Mukhtarov, F. M. (2022). Analysis of current information security policy. Research Focus, (1), 33–41.

Piper, S. G. (2023). Independent research in the field of national security. National political studies, (3), 102–134.

Riehle, K. (2022). Information Power and Russia's National Security Objectives. The Journal of Intelligence Conflict and Warfare, (4), 62–83.

Tigranovich, N. V. (2017). The role of cybersecurity in world politics. International Relations, (2), 339–348.

Willie, N. R. (2022). National Security Strategies of Canada and the United States: A Comparative Doctrinal Analysis, (3), 88–135.





# THE EVOLUTION OF THE ROLE OF THE MEDIA IN THE INFORMATION SECURITY DOCTRINES OF THE RUSSIAN FEDERATION IN 2000 AND 2016

**Kochkin A. V.**
Student of the Doctoral Programme
"Communication and Media" at the HSE University
(Mosow, Russia)
*andrey_kochkin@mail.ru*

**Abstract:**

Contemporary critical discourse studies tend to be based on structuralist and post-structuralist approaches. The author connects this state of affairs with the dominance of linguistics in the discourse analysis, while the very goal of criticizing discourse requires understanding it as a "folded" social activity, an inverted form of culture. For the cultural-historical approach, which the author proposes to use as a method of criticizing discourse, discourse is a reflection of social relations in speech form, a linguistic activity objectified in the text with non-linguistic motives, goals and means. The discourse does not form objective knowledge about reality, but its distorted sensual image, limited by the dialectical interposition of the subject and the environment. Thus, discourse becomes an ideological projection of social activity. Inequality in society is reflected in discourse. The task of cultural-historical discourse research is to reveal the hegemonic meaning of ideological discourse. To do this, the ideological text must be compared with the objective actual conditions of the life of the society in which this text is created and distributed.

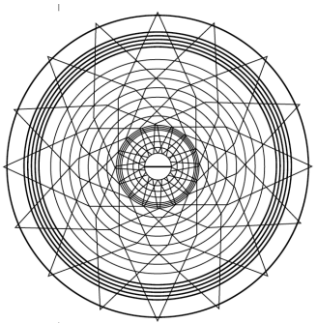
**Keywords:** mass media, media resource, information security, information space, sovereignty, state information policy

## REFERENCES

Artiomenko, E. (2020). Mass media: responses to information security challenges. Belarusian Yearbook, 124–132.

Asadova, Z. A. (2016). Information security in the countries of Central Asia: the case of Kazakhstan. MGIMO Review of International Relations, (6), 51–67.

Asmadi, A., Almutahar, H., Sukamto, S. (2023). Digital Information Security Policy in the National Security Strategy, International Journal of Multidisciplinary Approach Research and Science, 1, 96–103.



Berdnikova, E. N., Luk'yanchikova, M. V. (2019). Mediaobrazovanie kak vazhnejshij faktor obespecheniya bezopasnosti konfidencial'nyh dannyh. Rossijskaya shkola svyazej s obshchestvennost'yu, (12), 128–141.

Chesnokov, A. D. (2022). Informacionnaya bezopasnost'. student, (1), 478–489.

Collier, H., Morton, Ch., Alharthi, D., Kleiner, J. (2023). Cultural Influences on Information Security. University of Colorado Colorado Springs, 188 p.

Demina, I. N. (2018). Metodologicheskie podhody k missii i celyam mediasistemy. Voprosy teorii i praktiki zhurnalistiki, (1), 172–182.

Doktrina informacionnoj bezopasnosti Rossijskoj Federacii (utv. Prezidentom RF ot 9 sentyabrya 2000 g. N° Pr-1895) (2000). Rossijskaya gazeta, 187.

Downing, J. (2023). Social Media, Digital Methods and Critical Security Studies. In book: Critical Security Studies in the Digital Age, 71–108.

Downing, J. (2023). Social Media, Security and Democracy in the Digital Age. In book: Critical Security Studies in the Digital Age, 179–207.

Duben, A. K. (2023). Experience of international cooperation in the field of information security: problems and prospects. International Law and International Organizations, (3), 22–34.

Federal'nyj zakon ot 13 iyunya 2023 g. N° 227-FZ «O vnesenii izmenenij v stat'i 7 i 11 Zakona Rossijskoj Federacii «O sredstvah massovoj informacii» (2023). Sobranie zakonodatel'stva Rossijskoj Federacii, 25, 4416.

Federal'nyj zakon ot 26 iyulya 2017 g. N° 187-FZ «O bezopasnosti kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii» (s izmeneniyami i dopolneniyami). (2017). Garant. https://base.garant.ru/71730198/

Federal'nyj zakon ot 27 iyulya 2006 g. N° 149-FZ «Ob informacii, informacionnyh tekhnologiyah i o zashchite informacii». (2006). Garant. https://base.garant.ru/12148555/

Federal'nyj zakon ot 27 iyulya 2006 g. N° 152-FZ «O personal'nyh dannyh». (2006). Garant. https://base.garant.ru/12148567/

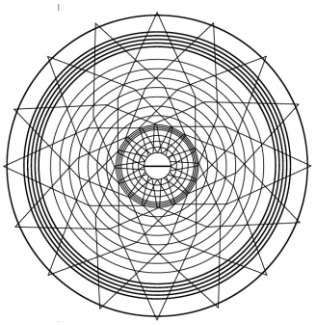
FinCERT. Bank Rossii. (2023). https://www.cbr.ru/information_security/fincert/

Hua, Li (2019). Kiberbezopasnost' v Rossii v svete Doktriny informacionnoj bezopasnosti RF 2016 goda. Mir russkogovoryashchih stran, (2), 11–21.

Global Cybersecurity Outlook (2023). https://initiatives.weforum.org/global-cyber-outlook/home

GosSOPKA. Informzashchita. 2023. https://www.infosec.ru/glavnye-temy/gossopka/

Gracheva, E. A. (2023). Informacionnaya bezopasnost'. The Newman in Foreign policy, (5), 57–60.





Kardava, N. V. (2018). Kiberprostranstvo kak novaya politicheskaya real'nost': vyzovy i otvety. Istoriya i sovremennost', (2), 152–166.

Levda, M. V. (2017). Informacionnaya bezopasnost' RF. Forum molodyh uchenyh, 11, 549–554.

Maathuis, C., Chockalingam, S. (2023). Modelling Responsible Digital Security Behaviour for Countering Social Media Manipulation. Indian Institute for Energy Technology, 203 p.

Meleshevich, R. I. (2019). Konvergenciya v mediasrede: k voprosu opredeleniya ponyatiya. Trudy BGTU. Seriya 4: Print- i mediatekhnologii, (1), 83–88.

Mel'nik, G.S., Nikonov, S.B. (2014). Medijnyj komponent v doktrine informacionnoj bezopasnosti. Upravlencheskoe konsul'tirovanie, (1), 18–28.

Mukhtarov, F. M. (2022). Analysis of current information security policy. Research Focus, (1), 33–41.

Piper, S. G. (2023). Independent research in the field of national security. National political studies, (3), 102–134.

Rejmov, B. E. (2022). Kiberprestupnost': sovremennoe sostoyanie i aktual'nye problemy. Ta'lim fidoyilari, (7), 555–561.

Riehle, K. (2022). Information Power and Russia's National Security Objectives. The Journal of Intelligence Conflict and Warfare, (4), 62–83.

Sidel'nikova, N. V., Besedina, T.V. (2018). Informacionnaya bezopasnost'. Obrazovanie. Kar'era. Obshchestvo, (1), 71–78.

Suvorova, A. Yu. (2017). Rol' novyh media v kontekste mediatizacii politicheskih processov. Kommunikologiya, (1), 69–78.

Tigranovich, N. V. (2017). The role of cybersecurity in world politics. International Relations, 2, 339–348.

Ukaz Prezidenta RF ot 5 dekabrya 2016 g. N° 646 «Ob utverzhdenii Doktriny informacionnoj bezopasnosti Rossijskoj Federacii» (2016). Sobranie zakonodatel'stva Rossijskoj Federacii, 50, 7074.

Willie, N. R. (2022). National Security Strategies of Canada and the United States: A Comparative Doctrinal Analysis, (3), 88–135.

Zakon RF ot 27 dekabrya 1991 g. N° 2124-I «O sredstvah massovoj informacii» (1992). Rossijskaya gazeta, 32.