УДК 070:004.056
ББК 76.004

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СТРАНЫ: ИНСТРУМЕНТЫ ДОМИНИРОВАНИЯ И ЗАЩИТЫ

Людмила Игоревна Михалева

Аспирант кафедры русской филологии и журналистики,
Волгоградский государственный университет
iryas@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. В статье представлен анализ средств обеспечения информационной безопасности страны. Рассмотрена история вопроса, технологии информационного доминирования и защиты, возможные угрозы интересам государства в информационной среде на фоне различных факторов. Определены задачи государства в области обеспечения информационной безопасности.

Ключевые слова: информационная безопасность, государство, цифровое пространство, информационное доминирование, информационное противоборство, доктрина информационной безопасности.

В век цифровых технологий без качественной информационной поддержки проводить в жизнь государственную политику и отстаивать интересы страны за рубежом невозможно. Противостояние государств на международной арене перешло с поля боя в цифровое пространство.

Российская Федерация – суверенное государство. У нас есть своя территория, своя банковская система, свои деньги, армия, власть, системы образования и здравоохранения, полиция, границы, таможня. Суверенитет бывает военный, дипломатический, экономический, политический, культурный и биологический. Но в последние десятилетия появился новый компонент – цифровой суверенитет, крайне актуальный в эпоху глобализации.

Как отмечает в своей монографии «Государственная информационная политика в особых условиях» профессор А.В. Манойло, «с появлением информационно-телекоммуникационных сетей границы между государствами приобрели прозрачность для перемещения главного ресурса информационного общества – информации» [4, с. 172]. Все более значимым становится проблема информационной безопасности – комплекса мер по защите информации от посторонних сил и чуждых социуму влияний.

Появление транснациональных корпораций-провайдеров превратило их, «наряду с традиционными государствами, в еще один субъект геополитических отношений» [1, с. 105]. Государство теряет экономический суверенитет, потому что на его территории действуют транснациональные корпорации. Их бюджеты подчас больше бюджета целой страны. У таких корпораций и больше возможностей: они могут покупать чиновников и диктовать им свою волю. В последние 20 лет слом суверенитета осуществляется ресурсами информационные войны.

Цифровой суверенитет – право государства определять свою информационную политику самостоятельно, распоряжаться инфраструктурой, ресурсами, обеспечивать информационную безопасность. Одна из категорий цифрового суверенитета – электронный суверенитет, который связан с защитой от кибе-

ратак. К нему относятся хакеры, DDoS-атаки, вирусы, спам. У большинства стран мира, к сожалению, с защитой электронного суверенитета большие проблемы.

Число успешных кибератак и результативность информационного давления показывают пугающую эффективность. По мнению президента Всероссийской полицейской ассоциации Юрия Жданова, ущерб мировой экономике от киберпреступности к 2030 г. достигнет 90 трлн долларов. По его словам, организация DDoS-атаки стоит в среднем 9 тыс. руб. в сутки, разработка нового вредоносного программного обеспечения – 20 тыс. руб., фишинговая кампания – 10 тыс. рублей. «На данный момент около 1,5 млн чел. совершили хотя бы одно преступное действие в Интернете», резюмирует Жданов [2]. Информационное противостояние будет продолжаться и обостряться, потому что идет борьба за будущий миропорядок. Его формирование пытаются подчинить себе, прежде всего, США, желающие сохранить и расширить свою политическую гегемонию, а без информационного превосходства гегемония установлена быть не может.

Так, профессор А.В. Манойло отмечает, что в современном информационном обществе артикулируются новые геополитические приоритеты в информационной деятельности государственных структур власти. Каждый из факторов информационного противоборства пытается выстроить в противовес противнику свою доминирующую коммуникацию. «Информационное доминирование, – по замечанию ученого, – может быть определено как способность назначить и поддерживать такой темп проведения операции, который превосходит любой возможный темп противника, позволяя доминировать во все время ее проведения, оставаясь непредсказуемым, и действовать, опережая противника в его ответных акциях» [4, с. 279].

Информационное доминирование непосредственно связано с информационно-телекоммуникационной экспансией. Это тоже один из терминов, который объясняет концепцию информационного противоборства, выдвинутую А.В. Манойло. Он формулирует это как «бесконфликтное проникновение в сферу социальных и духовных отношений общества» [4, с. 271]. По мнению А.В. Манойло, «происходит вытеснение положений национальной идеологии и национальной системы ценностей и замещение их собственными ценностями и идеологическими установками» [4, с. 278].

До 2000-х гг. в России практически не существовало ясной государственной позиции по этой проблеме, что, собственно, и привело к поражению СССР в Холодной войне. В результате к концу 80-х гг. советская молодежь готова была платить по 200 руб. (263 долл.) за джинсы *Montana*, в то время как в Америке стоимость одной пары была всего 30 долларов. Этот американский бестселлер, с фирменным орлом на металлической нашивке, в короткое время стал пропуском в мир богатых и модных. Очередь в фирменную секцию «Монтана» в универмаге «Московский» в начале 90-х была настолько велика, что огибала здание по периметру. Этот момент хорошо показан в фильме режиссера Сергея Ашкенази «Криминальный талант» 1989 года. В конце первой серии дочь главного героя, следователя Сергея Рябинина, выпрашивает у отца 200 руб. на модные джинсы. «Да, было ведь когда-то время, о шмотках думать не приходилось. Жила себе простой детской жизнью, забот не знала... А теперь, если джинсов нормальных импортных нет, в школе ведь засмеют. Ну или смотреть будут небрежно, без уважения», – так она объясняет отцу необходимость дорогой покупки. В джинсах у советской школьницы вся суть жизни.

Информационным оружием наших противников стало российское телевидение. Российские фильмы и программы заменили на иностранные, лучшее время для просмотра ТВ отдали под дешевые «мыльные оперы». В начале 90-х, сразу после американского сериала «Санта-Барбара», который смотрели всей страной в течение 10 лет, на канале РТР начиналась передача в стиле «магазин на диване». Она была в эфире ровно 15 минут. В ней рекламировался европейский бренд «leMonti». Под этой маркой продавали недорогую, качественную одежду и обувь. «LeMonti» предлагал довольно выгодные условия покупки – доставка в любой уголок страны и оплата наложенным платежом. Одеваться от «LeMonti» было престижно. Женщины в городах и селах России мечтали о знаменитых черных лаки-

рованных лодочках и платье с романтичным названием «День и ночь».

Но основной целью информационной войны было не освоение новых торговых территорий на постсоветском пространстве. За несколько лет удалось поменять сознание людей: каждый второй представитель советской молодежи мечтал уехать на Запад. Доминирующей информационной повестке не было реального противодействия. В стране был недостаток гуманитарных кадров – тех самых, из которых рекрутируются солдаты психологической войны. Если национальная культура крепка, то народ без оружия победит любого противника. Если же культура не доминирует в инфополе, то утрачивается национальное самосознание.

Первым представителем власти, который увидел эту проблему и заявил о ней, стал Владимир Путин. 9 сентября 2000 г., спустя всего четыре месяца после прихода к власти, Президент РФ подписал Доктрину информационной безопасности страны. В ней излагались официальные взгляды на цели, задачи, принципы и основные направления обеспечения информационной безопасности нашего государства. На первое место было поставлено обеспечение информационной безопасности индивидуального, группового и общественного сознания.

Во времена биполярного мироустройства этот вопрос особенного значения не имел, так как информационные пространства были разделены. Ненужная СССР или США информация просто не попадала в соответствующее информационное поле. Так, например, в США, в июле 1990 г. была принята «Национальная политика в телекоммуникационных и информационных сетях». Она, как и идеология в СССР, была направлена на защиту своего информационного пространства различными методами. Однако после разрушения СССР ситуация поменялась, так как США взяли на себя роль страны, управляющей мировым порядком. Были разработаны доктринальные документы, в которых особое место отводилось новым информационным технологиям.

К числу первых официальных документов Пентагона по этой проблеме можно отнести директиву МО США Т3600.1 от 21 декабря 1992 г. под названием «Информационная война» [6]. В этом документе впервые появляется термин «информационное противоборство». В 1993 г. в директиве Комитета начальников штабов № 30 уже были изложены основные принципы ведения информационной войны. Начиная с 1994 г. в США проводятся официальные научные конференции по информационной войне с участием видных представителей военно-политического руководства страны.

С этой целью в США уже создан Центр информационной стратегии и политики, задачей которого является изучение возможностей использования информационных технологий в военных конфликтах XXI века. В августе 1995 г. Центром разработки перспективных концепций и технологий управления Института национальных стратегических исследований Университета национальной обороны США была опубликована работа американского ученого Мартина Либики «What is information warfare?» [3]. К инструментарию войны относились не только сбор информации, всевозможные атаки на каналы связи и коммуникации, но и информационная обработка населения, целью которой являлся захват и подчинение информационного пространства. Либики выделил семь форм информационной войны:

1. Командно-управленческая – атака на каналы связи, когда основной целью является нарушение взаимодействия между командующими (или командными центрами) и их подчиненными.

2. Разведывательная – сбор значимой военной информации.

3. Психологическая – информационная обработка населения, их психики и сознания.

4. Хакерская – атака хакеров на узлы связи с целью выведения их из строя. Например, запуск вирусов.

5. Экономическая – под информационной блокадой понимается перекрытие каналов коммерции.

6. Электронная – выведение из строя электронных средств связи: компьютерных сетей, сотовых вышек, радиоузлов и т. д.

7. Кибервойна – в отличие от хакерской войны конечной целью является захват информации [3].

В 1996 г. в США появилась «Стратегия информационного противоборства. Новое лицо

войны», где вводилось понятие стратегической информационной войны, которая трактовалась как «использование киберпространства для того, чтобы оказывать влияние на стратегические военные операции и наносить урон национальной информационной инфраструктуре» противника [8]. Эти американские проекты в 1998 г. были сведены в «Объединенную доктрину информационных операций», в которой отразились элементы наступательных и оборонительных информационных компаний, позволяющих воздействовать на все киберпространство планеты, с целью нанесения серьезного урона «для систем государственного и военного управления, экономической и финансовой системы страны-мишени» [8]. Для реализации данной Доктрины 30 апреля 1999 г. в ЦРУ создано подразделение International Public Information, официальной задачей которого стало оказание влияния на иностранных зрителей с целью получения поддержки в вопросах американской внешней политики и противодействия пропаганде, исходящей от противников США.

Примечательно, что директивой президента PDD-68 от 30 января 1999 г. Белый дом создал новую структуру под названием Международная группа общественной информации – International Public Information Group (IPI). В задачи этой организации входит профессиональное использование разведывательной информации в целях оказания влияния на эмоции, мотивы, поведение иностранных правительств, организаций и отдельных граждан. Существенную роль в создании агентства сыграло разведсообщество, прежде всего ЦРУ. Таким образом, американские специалисты считают вполне возможным достижение в обозримом будущем подавляющего преимущества в информационной борьбе, что, по их мнению, позволит успешно разрешать конфликтные ситуации в свою пользу без вооруженного вмешательства.

Реакцией Российской Федерации на данные действия и стало утверждение 9 сентября 2000 г. «Доктрины информационной безопасности РФ», которая признала влияние информационных технологий на национальные интересы страны. Однако в ее преамбуле одним из оснований действия был прописан приоритет общепризнанных принципов и норм международного права и международных договоров РФ, которые в большей степени защищали интересы США. А так как данный документ не позволял в полной мере выполнять свои функции, то уже через полгода на заседании Межведомственной комиссии по информационной безопасности Совбеза РФ было объявлено о начале разработки новой редакции Доктрины. Правда, на этот процесс ушло целых 16 лет.

Тем временем в США продолжили укреплять свои позиции. Этому способствовали теракты 11 сентября 2001 года. После их осуществления была создана «Национальная стратегия защиты киберпространства». В феврале 2003 года ее утвердил президент Джордж Буш-младший. В октябре 2012 года американская Стратегия была дополнена директивой PPD 20 «Политика кибероперaций», первоначально носившая гриф «совершенно секретно». После этих дополнений политика США в сфере информационной войны перешла от защиты к нападению. Почти одновременно с принятием «Национальной стратегии безопасности в киберпространстве США» во Франции был создан Центр электроники и вооружений (CELAR), который по сути является продолжением американской политики в Европе, так как их объединяет НАТО.

Через подобные структуры США неоднократно брали под свой контроль информационное пространство интересующих их государств. Для этого в СМИ сначала велась активная пропаганда, через которую изменялись взгляды людей и традиционная идеология страны-мишени. Таким образом были проведены «цветные революции» в Югославии, Афганистане, Ираке, Ливии, Сирии, Киргизии, Грузии, на Украине.

Наша страна не может отказаться от своего статуса сверхдержавы. Она слишком большая и мощная, поэтому должна строить информационный суверенитет самостоятельно. Более мелким игрокам такое не под силу. Именно поэтому они вынуждены устраиваться к кому-то в кильватер.

Социальные сети – наиболее активная площадка геополитической конкуренции. Так, в октябре 2012 г. боевики движения «Талибан» совершили покушение на Малалу Юсуфзай, пакистанского подростка. Она вела блог в

защиту образования девочек. Малалу чудом осталась жива, поправилась и, несмотря на угрозы, продолжила борьбу за право девочек в Пакистане ходить в школу, наравне с мальчиками. Малалу в считанные дни стала одним из самых известных подростков в мире. В 2014 г. Юсуфзай была удостоена Нобелевской премии мира, став самым молодым лауреатом. Ей на тот момент исполнилось всего 15 лет [7]. Социальные сети были в значительной степени ответственны за ее стремительный взлет к мировой известности.

Еще один знаменательный случай: 7 января 2015 г. два исламистских боевика убили 10 сотрудников и двух полицейских в парижском офисе журнала «Je suis Charlie» в отместку за карикатуры на пророка Мухаммеда. В тот вечер сотни тысяч людей прошли маршем под лозунгами «Je suis Charlie» в знак солидарности с убитыми журналистами. К следующему вечеру этот слоган появился в Твиттере 3,4 млн раз в качестве хэштега. Три дня спустя два миллиона человек собрались в Париже, и почти 4 млн присоединились к демонстрациям по всей Франции. Солидарность стала глобальной, такова сила социальных медиа. Поэтому и простые граждане, пересылая посты, оставляя лайки, действуют как агенты рекламы микроуровня и работают в поддержку политических целей и организаций.

Один из базовых принципов информационной борьбы, который А.В. Манойло выделяет в своей работе «Государственная информационная политика в особых условиях», – информационная асимметрия. Она «основывается на многозначности информационного пространства. При блокировке любого из его элементов всегда возникает возможность воспользоваться другой свободной нишей» [4, с. 277]. Например, блокировка аккаунтов в социальных сетях и интернет-площадках действующего еще президента Дональда Трампа в январе 2021 года. Благодаря информационной асимметрии происходило не только уничтожение политического лидера, но и манипуляция общественным сознанием, определяющим политику и будущее страны. По логике информационного мира, человек исчезает из реальности, если отсутствует в виртуальном пространстве. Удаление из цифрового пространства влечет за собой лишение власти и влияния над большинством людей, для которых интернет стал основным, если не единственным источником информации. И не важно кто ты: простой обыватель или президент огромной страны.

Такое самовольное ограничение или лишение свободы и прав человека вполне соответствует новому понятию «цифровой диктатуры». Определенного рода асимметрии, когда один может все, а другой ничего. Насильственное выдавливание из информационного пространства и заполнение его угодными людьми, смыслами и идеями влечет за собой тотальный контроль над современным обществом.

Чаще всего американские и западные СМИ в ходе информационного противостояния пользовались достаточно простым приемом – в подаче новостей ссылались на неназванные источники или на пост частного лица в социальной сети. Так, информационное пространство накачивалось ложными данными и вызывало социальный протест. Яркий пример такой слаженной работы был проведен на территории Польши, в Telegram-канале белорусской оппозиции «Nexta» и «Nexta Live». В десятимиллионной стране они набрали почти 2 миллиона подписчиков после объявления официальных итогов президентских выборов, согласно которым победу одержал действующий президент страны Александр Лукашенко.

Акции протеста в Белоруссии начались в ночь с 9 на 10 августа 2020 года. В день выборов президента Белоруссии и в первые дни после них в стране практически не работал интернет. Власти утверждали, что все дело в кибератаках из-за рубежа. Независимые эксперты называли это «государственным интернет-шатдауном». У белорусов осталось два средства утоления информационного голода: государственное телевидение и Telegram. Мессенджер продолжал работать благодаря «антицензурным механизмам», о включении которых сообщил Павел Дуров.

В результате в самый разгар протестов «Nexta» и «Nexta Live» стали главными источником информации, в которой жителей страны призывали выходить на улицы, не признавать итоги выборов и свергнуть Лукашенко. Обе площадки в основном пересылали со-

общения друг друга. Но базовым являлся канал с приставкой *Live* в названии. Там появлялись самые «оперативные» видео с мест событий, большая часть которых была фальсификацией. Среди них ложь о прибытии российского спецназа для разгона демонстрантов в Минске. Также в разы преувеличивалось число протестующих на улицах. К реальным цифрам в 7 000–10 000 приписывались «нули».

В этой истории интересна судьба одного из основателей Telegram-канала «Nexta» Романа Протасевича. Для задержания оппозиционера Белоруссия пошла на беспрецедентный шаг – конфликт с Европейским союзом (ЕС) и США и принудительно посадила самолет «Ryanair» в Минске, на борту которого был Протасевич.

Сегодня, как заявляют правоохранители, Протасевич активно сотрудничает со следствием по обвинениям в «организации действий, грубо нарушающих общественный порядок», «организации массовых беспорядков» и «разжигании социальной вражды и розни». Ему грозит до 15 лет лишения свободы. Но уголовное дело не мешает журналисту появляться на государственных телеканалах и пресс-конференциях, пользоваться соцсетями и спокойно гулять по улицам Минска, несмотря на домашний арест. Вполне возможно, что Протасевич, пошедший на сделку с властью, избежит сурового наказания и станет козырем в большой игре Лукашенко. Судя по последней активности оппозиционера в социальных сетях, его могут рассматривать в качестве популярного провластного блогера. В Белоруссии была одержана своя победа в информационной войне.

Для обеспечения информационного доминирования в мире США не жалеют финансовых средств. На сегодняшний день для этой цели в стране задействованы сотни государственных и негосударственных организаций. Все они находятся в подчинении у правительства США. При этом документы по обеспечению информационной безопасности, принятые правительствами США при самых разных президентах, отражают их стремление к информационному превосходству и глобальному доминированию для сохранения статуса единственной сверхдержавы, в которых лидерство США трактуется как основной способ обеспечения национальной безопасности. Это уже само по себе является угрозой для национальных интересов России.

Реакцией на новую агрессивную американскую информационную политику стала разработка и утверждение новой, адекватной угрозам, «Доктрины информационной безопасности РФ», утвержденной Указом Президента РФ № 646 от 05.12.2016. Доктрина является, в первую очередь, частью общей Стратегии национальной безопасности Российской Федерации, соответствует новым требованиям, угрозам и реалиям.

По сравнению с предыдущим вариантом Доктрины, новый документ имеет более четкую и последовательную структуру. Среди стратегий предусмотрено следующее:

– противодействие угрозам безопасности;

– защита от применения информационных технологий как оружия в террористических и экстремистских целях;

– ослабление лидирующего положения иностранных технологий и продуктов, защита национальных интересов (импортозамещение).

Ликвидация зависимости от зарубежных технологий – новый пункт в Доктрине информационной безопасности страны. Основатель факультета кибернетики и информационной безопасности МИФИ, профессор Анатолий Малюк назвал это принципиально важным моментом, так как «состояние информационной безопасности страны сегодня характеризуется недостаточным уровнем развития конкурентоспособных информационных технологий и их использования для производства продукции и оказания услуг» [5, с. 54].

Государству, чтобы чувствовать себя защищенным в электронном смысле, нужен запуск полной технологической линейки. Начиная с процессоров, микросхем и заканчивая навигационными системами. Важно иметь собственную инфраструктуру – систему, в которой соединяются интернет, телевидение и СМИ. Собственная система пропаганды и ведения информационных войн сможет существовать эффективно, если у государства будет собственная идеология, вокруг которой можно выстраивать слои защиты.

Также в документе была отдельно выделена проблема «недостаточности кадрового обеспечения в области информационной

безопасности», которая за 16 лет не только не была решена, но и обострилась. Правовые аспекты обеспечения информационной безопасности тоже претерпели изменения. Новшеством является то, что теперь информационную безопасность должны обеспечивать не только органы власти, но и СМИ, операторы связи, образовательные организации, организации финансовой, банковской сфер, провайдеры. В их задачи входит обнаружение, предупреждение и ликвидация компьютерных атак и реакция на компьютерные инциденты. Для этого глава государства обязал компании создать специальные структурные подразделения или возложить обязанности на уже существующие. Согласно Указу Президента РФ № 250 от 01.05.2022 «О дополнительных мерах по обеспечению информационной безопасности РФ», отвечать за информационную безопасность теперь должны персонально руководители компаний.

Информационное противодействие терроризму – тоже новый пункт в Доктрине информационной безопасности РФ 2016 года. Главной задачей государственной политики для борьбы с этой угрозой Доктрина ставит защиту собственных информационных сфер от внешних тенденций, противодействие информационным угрозам, в частности информационной войне, которая вполне способна перерасти в реальный военный конфликт.

В нашей стране многое делается для строительства информационного суверенитета. Создается единая инфраструктура: собственные поисковые системы, социальные сети, свои мессенджеры, блоги, контентные ресурсы. Появляются собственные средства мониторинга персональной среды и фильтрации трафика. Для защиты от кибервойн в 2014 г. министром обороны России Сергеем Шойгу был подписан приказ о создании войск информационных операций в составе Генштаба ВС России. Основная задача подразделения заключается в защите системы управления от несанкционированного вмешательства.

Таким образом, в информационную эпоху СМИ и социальные сети, изначальная цель которых – информировать общественность о важных событиях в жизни страны и мира, стали инструментом воздействия на сознание аудитории. И в зависимости от того, кто этим инструментом пользуется, цель эта может быть не всегда благой. Сегодня влияние СМИ и Интернета настолько велико, что часто люди сами становятся заложниками убеждений и мыслей, которые им преподносят. Поэтому информационная безопасность страны – это не только четкое исполнение пунктов Доктрины информационной безопасности РФ. Это еще и постоянный коммуникационный акт с аудиторией, рассказ о вреде, который приносят информационные войны обществу и каждому человеку.

Задача государственных институтов – создавать такие структуры и принимать такие законы, которые будут направлены на защиту информационного и цифрового суверенитета нашего государства от атак других стран. СМИ и интернет-пространство должны находиться под контролем не иностранных компаний, не государства и не частных лиц, а именно народа. Усилиями истинно гражданского общества будут проводиться частые инспекции таких СМИ, проверки их на надежность, а также участие самого гражданского общества в создании и распространении максимально правдивой информации как на федеральном, так и на местном уровнях.

СПИСОК ЛИТЕРАТУРЫ

1. Бухарин, В. Сравнительный анализ нормативной базы по обеспечению информационной безопасности в США и РФ / В. Бухарин // Вестник Иркутского государственного технического университета. – 2016. – Т. 20. – С. 101–108.

2. В Минобороны РФ создали войска информационных операций // Сайт ИА Интерфакс. – 2017. – 22 февр. – Электрон. текстовые дан. – Режим доступа: https://www.interfax.ru/russia/551054

3. Либики, М. Что такое информационная война? / М. Либики // Плюриверсум. – Электрон. текстовые дан. – Режим доступа: https://pluriversum.org/opinion/strategy/chto-takoe-informatsionnaya-vojna

4. Манойло, А. Государственная информационная политика в особых условиях / А. Манойло. – М. : МИФИ, 2003. – 388 с.

5. Малюк, А. Комментарии к Доктрине информационной безопасности российской федерации / А. Малюк. – М. : Горячая линия – Телеком, 2018. – 213 с.

6. Микрюков, В. Ю. Безопасность жизнедеятельности / В. Ю. Микрюков. – Ростов н/Д : Феникс, 2006. – 425 с.

7. Самая юная нобелевская лауреатка: чем прославилась Малала Юсуфзай // Сайт компании «Chips Jornal». – 2021. – 12 июля. – Электрон. текстовые дан. – Режим доступа: https://chips-journal.ru/reviews/malala-usufzaj

8. Стратегия информационного противоборства. Новое лицо войны // Сайт компании «Rand Corporation». – Электрон. текстовые дан. – Режим доступа: https://www.rand.org

INFORMATION SECURITY OF THE COUNTRY: TOOLS OF DOMINATION AND PROTECTION

Ludmila I. Mikhaleva

Postgraduate Student, Department of Russian Philology and Journalism,
Volgograd State University
iryas@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Abstract. The article presents an analysis of the means of ensuring the information security of the country. The history of the issue, technologies of information dominance and protection, possible threats to the interests of the state in the information environment against the background of various factors are considered. The tasks of the state in the field of information security are determined.

Key words: information security, state, digital space, information dominance, information confrontation, information security doctrine.