УДК 351.862
Научная специальность: 5.2.3
EDN: KKMQSK

Возможные направления снижения риска информационных угроз для населения Российской Федерации

ISSN 1812-5220

Горячева Е.В.,
Малышев В.П.*,
Всероссийский научно-исследовательский институт по проблемам гражданской обороны и чрезвычайных ситуаций МЧС России (федеральный центр науки и высоких технологий), 121352, Россия, г. Москва, ул. Давыдковская, д. 7

Аннотация
В статье рассмотрены основные информационные угрозы для населения России, исходящие от стран коллективного Запада, а также меры по противодействию им. Целями исследования являлись анализ характера возможных информационных угроз для населения и определение комплекса мер по противодействию этим угрозам. В рамках оценки многообразных форм информационных угроз, основное внимание было уделено их влиянию на морально-психологическое состояние граждан. Учитывая, что в соответствии с Указом Президента Российской Федерации от 11.07.2004 № 868 на МЧС России возложена функция оказания экстренной психологической помощи пострадавшему населению в зонах чрезвычайных ситуаций, предложены возможные направления участия МЧС России в снижении риска информационных угроз и в обеспечении информационно-психологической поддержки населения.

Ключевые слова: возможные риски информационных угроз; способы воздействия на сознание людей; системы информационной безопасности; меры защиты и профилактики.

Для цитирования: Горячева Е.В., Малышев В.П. Возможные направления снижения риска информационных угроз для населения Российской Федерации // Проблемы анализа риска. 2025. Т. 22. № 3. С. 76–89. — EDN: KKMQSK.

Авторы заявляют об отсутствии конфликта интересов

Possible Directions for Reducing the Risk of Information Threats to the Population of the Russian Federation

Elena V. Goryacheva,
Vladlen P. Malyshev*,
All-Russian Scientific Research Institute for Civil Defence and Emergencies of the EMERCOM of Russia (Federal Science and High Technology Center), Davydkovskaya str., 7, Moscow, 121352, Russia

Abstract
The article examines the main information threats to the population of Russia, carried out by the countries of the collective West, and measures to counter them. The objectives of the research were to analyze the nature of possible information threats to the population and determine the composition of measures to counter these threats. In assessing the various forms of information threats, the main attention was paid to the information impact on the moral and psychological state of the population. Considering that in accordance with the Decree of the President of the Russian Federation of 11.07.2004 No. 868, the Ministry of Emergency Situations of Russia is entrusted with the function of providing emergency psychological assistance to the affected population in emergency zones, possible areas of participation of the Ministry of Emergency Situations of Russia in reducing the risk of information threats and providing information and psychological support to the population are proposed.

Keywords: possible risks of information threats; methods of influencing people's consciousness; information security systems; protective and preventive measures.

For citation: Goryacheva E.V., Malyshev V.P. Possible directions for reducing the risk of information threats to the population of the Russian Federation // Issues of Risk Analysis. 2025;22(3):76–89. (In Russ.). — EDN: KKMQSK.

The authors declare no conflict of interest

Содержание

Введение

Стремительные темпы развития компьютеризации и информатизации общества неизбежно приводят к созданию единого мирового информационного пространства, в котором будут аккумулированы все средства сбора, накопления, обработки, хранения и обмена информацией между отдельными людьми, организациями и государствами.

В XXI веке основу мирового информационного пространства могут составить национальные информационно-управляющие инфраструктуры развитых государств, таких как США, Китай, страны Западной Европы и Япония. При этом уже сейчас создаются предпосылки значительного роста политического, экономического и военного превосходства развитых индустриальных стран за счет их лидирующей роли в компьютеризации и информатизации.

Это наглядно продемонстрировали такие события, как «цветные революции» на постсоветском пространстве и «арабская весна» на Ближнем Востоке. Посредством Интернета велась активная пропаганда с целью свержения правящих режимов в ряде бывших советских республик и ближневосточных странах. Все революции в бывших советских республиках (Грузии, Украине, Киргизии и Армении) совершались по методичке Шарпа «От диктатуры к демократии». Согласно ей в странах формировалась многочисленная сеть неправительственных организаций, подконтрольных ЦРУ, развертывались радиоэлектронные системы управления и связи, и организовывалась подготовка боевиков, с помощью которых проводились акции по свержению законно избранной власти.

В Указе Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» определено следующее понятие: «угроза информационной безопасности Российской Федерации — совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере».

1. Основные информационные угрозы для населения России, осуществляемые странами коллективного Запада

Успехи в создании информационно-коммуникационных технологий позволяют высокоразвитым странам Запада вести полномасштабные агрессивные действия в информационной сфере. Главными направлениями использования современных информационных технологий и средств для нанесения ущерба национальным интересам России являются попытки дезорганизации общественных устоев страны, нарушения функционирования ключевых военных, промышленных, административных объектов , а также информационно-психологическое воздействие на военно-политическое руководство, вооруженные силы и население [1].

Беспрецедентное развитие и распространение информационно-коммуникационных технологий позволяет вести информационные агрессии на принципиально новом уровне и использовать их для кардинального изменения социально-политической обстановки в стране. Как известно, национальная сеть электросвязи является составной частью глобальной информационной инфраструктуры, базирующейся во многом на сети Интернет. Основная часть корневых сегментов сети Интернет находится во владении юридических лиц, подчиняющихся органам власти Западных государств. В случае возникновения политических осложнений эти государства используют свои возможности по управлению корневыми сегментами сети Интернет в качестве средства оказания давления на население Российской Федерации.

В интересах достижения определенных целей, используя свои преимущества в создании информационно-коммуникационных технологий, информационные службы Запада внедряются в радиоэлектронные системы управления и связи, собирают необходимую информацию, предпринимают целенаправленные наступательные действия подрывного или уничтожающего характера и нарушают работу органов государственного и военного управления. Одновременно при помощи средств массовой информации и интернет-ресурсов ведется целенаправленная кампания по дестабилизации общественного сознания в нашей стране. Эта кампания включает в себя провокации на этнической и религиозной почве, распространение дезинформации с целью посеять сомнения, хаос и подорвать доверие к государственным институтам. Кроме того, предпринимаются попытки вербовки уязвимых слоев населения, таких как молодежь и пожилые люди, в террористические организации.

Следует отметить, что подобные тактики использовались странами Запада в середине 1980-х годов

с целью содействия распаду Советского Союза. В частности, после аварии на Чернобыльской АЭС, имевшей серьезные последствия, пропагандистские акции, проводимые западными и некоторыми отечественными СМИ, эффективно демонстрировали неспособность советской власти гарантировать надлежащий уровень безопасности в сфере атомной энергетики. Это, в свою очередь, привело к снижению доверия населения к системе управления страной и поспособствовало развалу Советского Союза.

В информационной сфере выделяются следующие виды угроз: систематическое распространение в СМИ информационных акций лживого, провокационного характера; проведение психолого-информационных операций; активизация различных видов киберпреступности и кибертерроризма [2]. Эти угрозы отличаются по масштабам, целям и задачам, а также используемым способам, силам и средствам. Основные виды угроз представлены на рис. 1.

Использование этих видов угроз может быть классифицировано по трем основным направлениям воздействия [3]:

- влияние на сознание. Такое направление предполагает воздействие на индивидуальные, групповые

Рис. 1. Основные виды информационных угроз для населения Российской Федерации

Figure 1. Main types of information threats to the population of the Russian Federation

и массовые умонастроения населения с использованием СМИ;

• влияние на системы принятия решений. Это направление предназначено для воздействия на процессы принятия решений в ключевых сферах деятельности: политической, экономической, военной, научно-технической и социальной;

• влияние на информационные системы. Направление включает в себя действия по управлению, блокированию и изъятию обрабатываемой информации из информационных систем.

Основные цели направлений [4]:

• подрыв безопасности государства, общества и личности путем разрушения систем принятия решений на уровне государственного управления;

• нарушение работы финансово-хозяйственной системы, транспорта и связи;

• информационно-психологическое воздействие на население страны, создание атмосферы неуверенности, паники и страха;

• вывод из строя системы управления вооруженными силами страны, иными войсковыми соединениями и формированиями;

• провоцирование социальных, политических, национальных и религиозных столкновений.

В последние годы в США формируется новый особый вид межгосударственного противоборства — стратегическая информационная война, которая в настоящее время ведется против Российской Федерации [4]. США вместе со своими союзниками добились значительных успехов в проведении информационных кампаний, направленных на подрыв общественного согласия и доверия к государственным институтам в некоторых бывших советских республиках и странах Ближнего Востока. В настоящее время западные страны предпринимают попытки привлечь Грузию, Армению и Молдавию к борьбе против России. Предпринимаются попытки повлиять на ключевые группы населения в приоритетных географических регионах России с целью разжигания антигосударственных настроений и провоцирования «цветной революции» для последующего прихода к власти прозападных политиков. Запад активно транслирует всему миру негативный образ России как «тиранического» и «отсталого» государства, стремясь к ее максимальной политической и экономической изоляции.

Наибольшими возможностями для проведения подобных акций располагают информационные службы США и Великобритании. В рамках функционирования специальных правительственных органов они активно занимаются вмешательством во внутренние дела многих стран, применяя способ «мягкой силы». Так в США с 1961 г. функционирует Агентство по международному развитию (United States Agency for International Development, USAID), в котором работают свыше 10 тыс. сотрудников, две трети из которых находятся за рубежом в 130 странах мира [5]. В свете проводимой Россией специальной военной операции, агентство USAID активизировало свою деятельность на Украине. С февраля 2022 г. Конгресс США выделил более 46 млрд долл. для реализации этим агентством 380 проектов на Украине. Эти проекты направлены на пропагандистское воздействие на местное население, а также на дестабилизацию ситуации в Российской Федерации.

В отличие от США, Великобритания в этой области имеет более значительный исторический опыт. Еще в XVIII веке дипломаты Великобритании способствовали убийству руководителя русского посольства в Тегеране А. Грибоедова и императора Павла I в Санкт-Петербурге. В настоящее время дипломаты и сотрудники секретной разведывательной службы Великобритании MI6, оснащенные самыми современными методичками и соответствующими техническими средствами, способны осуществлять психолого-информационные операции во многих странах мира. Неслучайно трех наиболее активно действующих дипломатов выслали из России в прошлом году.

В. Е. Лепский выделяет следующие основные задачи обеспечения информационно-психологической безопасности дипломатов:

«…выявление, анализ и оценка источников негативных информационно-психологических воздействий;

оценка и прогнозирование последствий негативных информационно-психологических воздействий на персонал, отдельных лиц, групп и других социальных образований, вовлеченных реально (потенциально) в дипломатическую деятельность (партнеры, клиенты и др.), а также информацию и информационные потоки, обеспечивающих дипломатическую деятельность;

разработка нормативно-правовой и методической базы обеспечения информационно-психологической безопасности дипломатической деятельности;

разработка и реализация комплекса мероприятий (системы) предотвращения и нейтрализации негативных информационно-психологических воздействий…» [6].

В своей информационной борьбе с Россией страны Запада в последние десятилетия, помимо собственных специальных служб и СМИ, активно используют как спонсируемые ими силы внутри России (несистемную оппозицию, русофобские СМИ), так и антироссийски настроенные элиты и СМИ некоторых соседних с Россией стран (Польши, Украины, Эстонии, Латвии, Литвы, Грузии). Все это направлено на содействие уничтожению гражданского населения в приграничных с Украиной регионах. С целью блокирования поступления объективной информации о злодеяниях украинских властей организована массовая террористическая охота на активно выступающих политических деятелей и журналистов Российской Федерации.

При оценке возможного ущерба от информационных угроз были рассмотрены факторы, способствующие распаду Советского Союза. Важную роль в этом процессе сыграло активное внедрение в сознание советских граждан искаженных представлений о свободе и демократии, характерных для Запада. Запад, получив превосходство в информационной борьбе, смог добиться ряда ключевых преимуществ [4]:

- распад Советского Союза на 15 независимых государств, на территории которых периодически возникают военные или социальные конфликты;
- ослабление главного военного противника за счет одностороннего разоружения;
- уступки по всем внешнеполитическим вопросам;
- выход на огромный, беззащитный постсоветский рынок;
- приток квалифицированных и образованных мигрантов;
- бесплатный доступ к природным ресурсам республик бывшего СССР.

В настоящее время информация занимает ключевое место в функционировании структур государственной власти, национальной безопасности и общественных институтов. Широкое применение информационных технологий открывает возможности для воздействия на различные сферы общественной жизни, что обусловливает необходимость проведения системных исследований для выработки эффективных мер противодействия этим угрозам.

2. Меры противодействия информационным угрозам в различных сферах общественной жизни

Меры противодействия информационным угрозам включают несколько направлений деятельности, позволяющих достичь необходимого уровня защиты от угроз противника [7].

Первым направлением является совершенствование законодательной базы по вопросам регулирования информационно-коммуникационной деятельности с целью эффективного противодействия современным информационным угрозам в различных сферах общественной жизни. Существующие правовые документы в области информационной безопасности, такие как Указы Президента, федеральные законы, Гражданский кодекс РФ, не в полной мере решают эту задачу[1].

Второе направление включает две составляющие: проведение мероприятий по противодействию информационным угрозам и по защите отечественных информационных коммуникаций от воздействия противника. Мероприятия информационного противодействия включают формирование сети технико-коммуникационных систем мониторинга, которые с помощью технического контроля систем связи выявляют и блокируют дезинформацию на всех этапах информационных действий противника, включая физическое уничтожение носителей информации. Мероприятия по второй составляющей обеспечивают защиту информации, средств ее хранения, обработки, передачи и автоматизации этих процессов от воздействий информационных служб противника. Успешной реализации этого направления препятствует технологическое отставание России в создании комплектующих изделий и программных средств для информационно-коммуникационных систем [8]. Для обеспечения суверенитета России в этой сфере деятельности необходимо наращивать информационные

[1] Указ Президента Российской Федерации от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы»; Указ Президента Российской Федерации от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации»; Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»; Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 №230-ФЗ (глава 70 «Авторское право»); Федеральный закон от 21.09.1993 № 182 «О государственной тайне».

возможности в рамках принятых Правительством Российской Федерации решений по созданию отечественных информационных систем.

Третье направление должно заключаться в том, что государственные органы и институты гражданского общества должны сосредоточить свои усилия на мероприятиях, направленных на повышение уровня защищенности населения от информационно-психологического воздействия. К таким мерам относятся:

- противодействие распространению информации лживого и провокационного характера;
- культурно-образовательная сфера;
- создание условий для этно-социальной толерантности;
- формирование социально значимых ценностей в обществе;
- организация индивидуальной работы с лицами, попавшими под влияние вражеской пропаганды и проявляющими склонность к экстремистским действиям.

Предлагаемый порядок организации мер по противодействию информационным угрозам приведен на рис. 2.

Одним из наиболее острых и опасных вызовов с точки зрения стратегической безопасности является возможное применение информационно-коммуникационных технологий (ИКТ), в том числе сети Интернет, в целях, противоречащих задачам обеспечения национальной стабильности и безопасности. Важнейшей угрозой в этой сфере видится возможность враждебного использования ИКТ против критически важной инфраструктуры. Нельзя допустить, чтобы сфера ИКТ превратилась в новую площадку межгосударственного противоборства.

Рис. 2. Предлагаемый порядок организации мер по противодействию информационным угрозам

Figure 2. Proposed procedure for organizing measures to counter information threats

В качестве примера можно привести политику Китайской народной республики (КНР) в области Интернета, которая уже служит образцом для других государств [9]. Система контроля и регулирования интернет пространства в КНР создавалась еще в 1990-х гг. Министерство общественной безопасности КНР, действуя под эгидой информационного бюро Госсовета КНР, регулярно организовывало поездки специалистов в Сингапур и Гонконг для изучения передового опыта контроля сети Интернет, перехвата электронной почты, обеспечения безопасности компьютерных сетей и регулирования распространяемой информации (табл. 1) [10].

Наличие всеобъемлющего контроля за информацией, размещаемой в Интернете или передаваемой с помощью мобильных телефонов, также способствует самоцензуре со стороны пользователей, которые вынуждены отказываться от передачи политически острой информации. В целом же, как отмечают эксперты, созданная в Китае беспрецедентная система контроля над действиями интернет-пользователей успешно введена в действие. На данный момент Пекину официально удается контролировать содержание масштабного китайского сегмента глобальной сети, придерживаясь открытой модели развития.

Для построения систем информационной безопасности необходимы средства защиты программно-технического уровня, представляющие собой:

- межсетевые экраны, обеспечивающие ограничение доступа в информационную сеть;
- средства идентификации, позволяющие отсеивать «чужаков» и точно определять источник поступления информации;
- средства мониторинга сети на всех уровнях, позволяющие выявлять подозрительную активность и осуществлять оперативное реагирование на действия злоумышленников.

Желательно также экранировать как оборудование, так и помещение, в котором оно находится, а в качестве каналов связи по возможности использовать волоконно-оптические линии.

Таблица 1. Основные органы контроля и регулирования Интернет-пространства в Китае [10]
Table 1. Main control and regulation bodies of the Internet space in China

Контролирующий орган	Выполняемые функции	Особенности деятельности
Бюро информации и общественного мнения при общественном отделении Коммунистической партии Китая (далее – КПК)	Анализ информации по важным темам и представление ее в Центральный комитет (далее – ЦК КПК)	Проведение опросов общественного мнения в Интернете, их еженедельного анализа и обсуждения. Итоги опросов направляются руководству общественного отделения, Министру общественной безопасности и всем членам Политбюро ЦК КПК
Центр изучения общественного мнения при информационной службе Государственного совета КНР	Надзор и регулирование информации в Интернете; мониторинг общественного мнения	Проведение Интернет-мониторинга и анализа информационных Интернет-услуг
Бюро Государственного совета КНР по контролю за информацией	Анализ информации, размещенной в социальных сетях, блогах и форумах, Интернет-сайтах	Наблюдение и контроль за содержанием Интернет-новостей
Административное бюро Интернет-пропаганды	Надзор и регулирование информации в Интернете	Контроль за применением регулирующих требований к публикуемым новостям в Интернете, которые применяются ко всем СМИ
Государственное управление по кинематографии, радио и телевидению	Контроль аудиовизуального содержания сайтов китайского сегмента Интернета	Все сервисы по обмену видеофайлами, согласно распоряжению управления, должны принадлежать государству
Главное управление прессы и печатных изданий	Регулирование деятельности Интернет-СМИ	Создание групп Интернет-рецензентов, которые осуществляют оценку новостей и цензуру в Интернете и готовят отчеты для КПК
Отделения Государственного ведомства Интернет-пропаганды	Регулирование деятельности Интернет-СМИ на региональном уровне	Определение подцензурных тем
Государственная канцелярия Интернет-информации КНР	Блокировка сайтов, распространяющих нежелательные для властей сведения; административное лицензирование бизнес-проектов, связанных с Интернетом; контроль за развитием игровой индустрии в Интернете	Первая в стране организация, которая осуществляет цензурный и надзорный контроли

Недавно израильские спецслужбы использовали новый способ массового терроризма: закладку взрывчатых веществ в мобильные телефоны и подрыв их с помощью информационных технологий. Для борьбы со способами кибертерроризма, основанного на использовании вражеских закладок в импортной бытовой технике, целесообразно усилить таможенный контроль с привлечением представителей специальных служб для оценки опасности, поступающей в Российскую Федерацию бытовых устройств.

В информационно-психологической борьбе главными объектами защиты являются психика личного состава силовых структур и населения крупных городов, которые могут принять участие в масштабных несанкционированных акциях, а также системы формирования общественного мнения и принятия решений. Такая борьба ведется методами и средствами информационно-психологического воздействия на сознание населения. Целенаправленные и многократно повторяемые в информационных сетях искаженные сведения или провокационные посылы, могут вызвать неадекватную реакцию у значительной части населения. Наблюдаемый в настоящее время рост протестного движения в Сербии служит ярким примером подобного явления.

Как и всякое другое оружие, используемое в реальном мире, средства информационно-психологического воздействия постоянно модифицируются в зависимости от изменяющихся условий и применяемых средств защиты.

В связи с этим представляется целесообразным, наряду с использованием эффективных методов контроля сети Интернет, перехвата электронной почты и обеспечения безопасности компьютерных сетей по опыту КНР, предусмотреть разработку перспективных форм и методов противодействия ложной информации и негативной пропаганде.

В то же время блокирование вражеской информации не должно влиять на функционирование отечественных информационных систем [11]. На основе отечественных разработок в оборонной области должны быть разработаны технологии, надежно определяющие свою и чужую информацию. По мнению ряда экспертов, наиболее уязвимыми точками инфраструктуры России являются энергетика, телекоммуникации, авиационные диспетчерские системы, финансовые электронные системы, правительственные информационные системы, а также автоматизированные системы управления войсками и оружием. Например, в атомной энергетике изменение информации или блокирование информационных центров может повлечь за собой ядерную катастрофу или прекращение подачи электроэнергии в города и критически важные объекты. Искажение информации или блокирование работы информационных систем в финансовой сфере может привести к кризису, а выход из строя электронно-вычислительных систем управления войсками и оружием приведет к непредсказуемым последствиям.

Информационно-разъяснительные меры профилактики информационных угроз могут включать [12]:

- работу по разъяснению сущности и опасности психолого-информационного воздействия;
- информирование населения по вопросам противодействия и профилактики терроризма;
- воспитание у населения устойчивости к психофизиологическому воздействию;
- преодоление негативных установок населения в области межэтнического общения;
- формирование у граждан законопослушного поведения и внутренней потребности неприятия идеологии экстремизма, потребности активного противодействия проявлениям экстремизма.

Особую угрозу представляют протестные акции против существующего строя и высших руководителей страны. Информационными технологиями подготовки таких акций прекрасно владеют специальные службы стран Запада. При оценке угроз любых протестных акций, которые обычно проходят в крупных городах, целесообразно учитывать два основных показателя:

- частоту возникновения;
- количество участников.

Для анализа опасности этих угроз предлагается следующий подход к ранжированию территории городов по уровню реагирования на возникшие протестные акции, основанный на использовании матрицы, в которой оценка проводится на основе анализа величин вышеприведенных показателей (см. табл. 2).

Величины, приведенных в табл. 2 показателей, носят ориентировочный характер и могут быть уточнены в зависимости от степени опасности протестных акций и численности населения, проживающего в городе.

Таблица 2. Матрица ранжирования городов по уровню реагирования на возникшие протестные акции
Table 2. Ranking matrix of cities by the level of response to the protests that have arisen

Частота возникновения протестных акций за месяц	Степени участия людей в протестных акциях			
	1 степень (до 100 чел.)	2 степень (до 300 чел.)	3 степень (до 1000 чел.)	4 степень (свыше 1000 чел.)
От 1 и выше	Территория	Территория	требующая	срочных мер реагирования
от 1 до 0,3		повышенного		
менее 0,3 до 0,1	Территория		внимания	
менее 0,1 до 0,01		приемлемого		к людским протестам
менее 0,01			риска	

3. Возможные направления участия МЧС России в противодействии информационным угрозам

В соответствии с Положением о Министерстве Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий (МЧС России), утвержденным Указом Президента Российской Федерации от 11.07.2004 № 868, а так же федеральными законами от 12.02.1998 № 28-ФЗ «О гражданской обороне», от 21.12.1994 № 68-ФЗ «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера», от 21.12.1994 № 69-ФЗ «О пожарной безопасности» МЧС России является федеральным органом исполнительной власти, который осуществляет управление, координацию, контроль и реагирование в области гражданской обороны, защиту населения и территорий от чрезвычайных ситуаций, обеспечение пожарной безопасности и безопасности людей на водных объектах. Следовательно, эти области являются основными направлениями государственной деятельности МЧС России в сфере обеспечения национальной безопасности Российской Федерации. При возникновении чрезвычайных ситуаций (ЧС), пожаров или применении боевых средств поражения одной из главных задач по защите населения является своевременное информирование граждан об опасности поражения [13].

В условиях роста информационных угроз возникает необходимость пересмотра подходов к дальнейшему развитию систем информирования и оповещения. Повышение надежности информирования населения с помощью систем централизованного оповещения может быть достигнуто за счет обеспечения современными средствами защиты от несанкционированного проникновения в каналы сбора и передачи данных оперативной обстановки в зоне ЧС [2].

Повышение оперативности систем оповещения и информирования населения об угрозе возникновения или факте возникновения ЧС может быть достигнуто путем автоматизации процессов оповещения и минимизации влияния человеческого фактора на их передачу. При выполнении других задач по защите населения и территорий необходимо предусматривать меры защиты от возможных информационных угроз. Некоторые из возможных мероприятий обеспечения информационной безопасности применительно к системе МЧС России приведены в табл. 3.

Кроме вышеприведенных направлений деятельности, в соответствии с Указом Президента Российской Федерации от 11.07.2004 № 868 на МЧС России возложена функция по оказанию экстренной психологической помощи пострадавшим в зонах ЧС и при пожарах гражданам. Для выполнения этой функции в 1999 г. создан Центр экстренной психологической помощи МЧС России (ЦЭПП МЧС России).

ЦЭПП МЧС России — организация системы МЧС России, оказывающая экстренную психологическую помощь населению, пострадавшему при ЧС, и обеспечивающая психологическое сопровождение личного состава МЧС России. В настоящее время на территории Российской Федерации открыто восемь филиалов ЦЭПП МЧС России, расположенных в административных центрах федеральных округов и в городе федерального значения — Севастополь. Специалисты центра оказывают психологическую помощь населению в круглосуточном режиме по телефону доверия и онлайн-помощь на официальном сайте организации [13].

Таблица. 3. Мероприятия обеспечения информационной безопасности применительно к системе МЧС России [2]

Table 3. Information security measures applicable to the EMERCOM of Russia system [2]

Информационные угрозы и объекты воздействия	Основные мероприятия обеспечения информационной безопасности
Негативное информационное воздействие на мировое общественное мнение с целью дискредитации основ политики России в области защиты населения и территорий в ЧС	Систематическое выявление угроз и их источников, структуризация целей обеспечения информационной безопасности в сфере ГО и определение соответствующих практических задач. Снижение эффективности информационного воздействия противника
Информационное воздействие деструктивного характера на массовое сознание и морально-психологическое состояние населения и личного состава формирований ГО, их психологическую готовность к выполнению мероприятий по ГО и защите от ЧС	Формирование и поддержание традиционных мировоззренческих основ, целей, ценностей, национальных интересов России в информационном пространстве (глобальном, региональном, национальном), а также противодействие попыткам манипулирования восприятием информации населением со стороны деструктивных сил, противодействие внедрению целей, мотивов и смыслов деятельности, чуждым национальным интересам государства
Психологическое воздействие на население и личный состав формирований ГО и РСЧС в условиях ЧС	Совершенствование подходов в области обеспечения информационно-психологической безопасности населения и личного состава формирований ГО и РСЧС. Формирование психологической готовности и повышение психологической устойчивости населения и личного состава формирований ГО и РСЧС к действиям в условиях ЧС.
Несанкционированный доступ к системе сбора, обработки и передачи оперативной информации в зоне ЧС	Совершенствование средств защиты информации от несанкционированного доступа, развитие защищенных систем связи и управления, повышение надежности специального программного обеспечения. Оптимизация структуры функциональных органов системы обеспечения информационной безопасности в сфере ГО и координация их взаимодействия
Несанкционированный доступ к системам принятия решений по оперативным действиям (реакциям), связанным с развитием ЧС и ходом ликвидации их последствий	Повышение надежности систем обработки и передачи информации, обеспечивающих деятельность федеральных органов исполнительной власти. Хакерские атаки на управленческие программно-аппаратные комплексы. Проведение сертификации общего и специального программного обеспечения, пакетов прикладных программ и средств защиты информации в существующих и создаваемых автоматизированных системах управления связи

Структуру психологической службы МЧС России составляют Управление медико-психологического обеспечения, ЦЭПП МЧС России и его филиалы, а также специалисты психологической службы территориальных органов и учреждений МЧС России.

В соответствии с Приказом МЧС России от 20.09.2011 № 525 «Об утверждении Порядка оказания экстренной психологической помощи пострадавшему населению в зонах чрезвычайных ситуаций и при пожарах» задачами специалистов психологической службы при оказании экстренной психологической помощи пострадавшим в условиях ЧС являются:

- создание психологической обстановки, обеспечивающей оптимальные условия для проведения АСДНР;
- снижение интенсивности острых реакций на стресс у пострадавших, а также у родственников и близких погибших и пострадавших, оптимизация их актуального психического состояния;
- снижение риска возникновения массовых негативных реакций;
- профилактика возникновения у пострадавших, а также у родственников и близких погибших и пострадавших отдаленных психических последствий в результате воздействия травмирующего события;
- внесение предложений заинтересованным органам по планированию и организации мероприятий с участием пострадавших, а также родственников и близких погибших и пострадавших в ЧС, с учетом социально-психологических рисков.

В условиях гуманитарного реагирования при ведении военных конфликтов МЧС России осуществляет необходимые меры жизнеобеспечения населения, включая меры по психологической поддержке пострадавших [14].

Информационно-психологическая поддержка населению в условиях ЧС должна быть направлена на:

- стабилизацию морально-психологического состояния;
- своевременное и качественное информирование населения о развитии ЧС, способах защиты и возможностях получения необходимой медицинской, психологической, социальной, гуманитарной, волонтерской и других видов помощи;

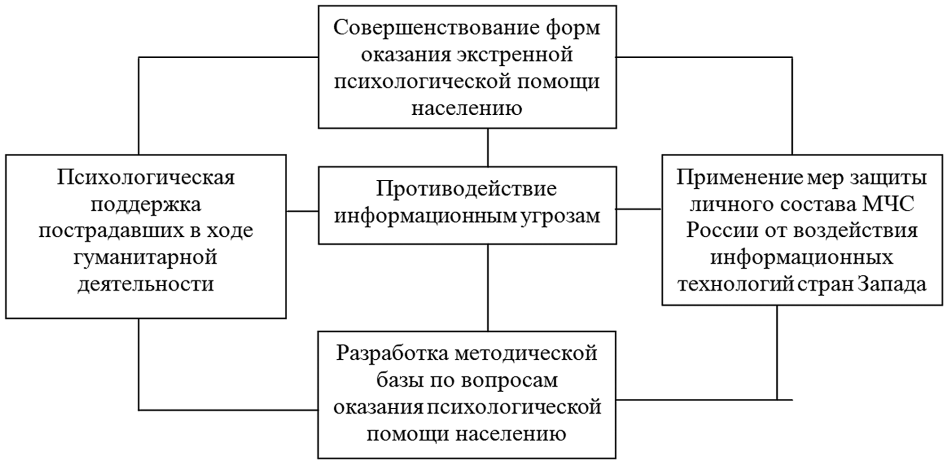

Рис. 3. Предлагаемые направления возможного участия МЧС России в противодействии информационным угрозам

Figure 3. Proposed directions of possible participation of EMERCOM of Russia in countering information threats

• предотвращение развития массовых негативных поведенческих, психоэмоциональных и панических реакций;

• повышение общей психологической грамотности, готовности и устойчивости населения в условиях ЧС.

Предлагаемые направления возможного участия МЧС России в противодействии информационным угрозам приведены на рис. 3.

Организация деятельности по предлагаемым направлениям участия МЧС России в противодействии информационным угрозам требует скоординированной работы с другими органами государственной власти, а также с общественными организациями и объединениями, в целях обеспечения информационной безопасности страны.

Заключение

Новые вызовы и угрозы информационного характера по своим масштабам могут быть сопоставимы с угрозами военного характера. Незавершенность формирования комплексной системы обеспечения информационной безопасности в России, а также законодательной базы в сфере информационно-компьютерных преступлений, а массовое использование зарубежных комплектующих изделий и программных средств обуславливает высокий уровень уязвимости России в этой области [15, 16].

В целях противодействия информационным угрозам целесообразно:

• планировать разработку правовых документов, обеспечивающих эффективное противодействие современным информационным угрозам в различных сферах общественной жизни;

• усилить контроль за распространением ложной информации провокационного характера;

• организовать широкую информационно-образовательную кампанию по разъяснению опасности психолого-информационного воздействия на человека;

• обеспечить устойчивость функционирования отечественных информационно-коммуникационных ресурсов и систем государственного управления, в случае воздействия существующих и перспективных средств информационной борьбы.

В современных реалиях внимание и поддержка со стороны общества оказывают соответствующее влияние на эффективное развитие МЧС России в вопросах защиты населения от информационных угроз. Поэтому необходимо проводить более активную работу с участием добровольческого и волонтерского движений по формированию комплекса мер, направленных на организацию профилактических мероприятий по защите населения от негативного информационно-психологического воздействия в СМИ, на Интернет-ресурсах и социальных медиа. Необходимо раскрывать социальные и гуманные функции помощи населению

в различных кризисных ситуациях. Особо следует подчеркнуть социальную значимость культуры когнитивной безопасности в части пропаганды и формирования у населения психологической устойчивости в условиях возникновения угроз информационного характера.

Список источников [References]

1. XXI век — вызовы и угрозы / В. А. Акимов, В. А. Владимиров, В. П. Малышев [и др.]; Под общей редакцией В. А. Владимирова. М.: Ин-октаво, 2005. 304 с. ISBN 5-98738-026-X.— EDN UCTFSF [XXI century — challenges and threats / V. A. Akimov, V. A. Vladimirov, V. P. Malyshev [et al.]; ed. by V. A. Vladimirov. M.: In-octavo, 2005. 304 p. ISBN 5-98738-026-X.— EDN UCTFSF. (In Russ.)]
2. Фалеев М. И., Черных Г. С. Угрозы национальной безопасности государства в информационной сфере и задачи МЧС России в этой области деятельности // Стратегия гражданской защиты: проблемы и исследования. 2014. Т. 4. № 1(6). С. 21–34.— EDN SCHGGZ [Faleev M. I., Chernykh G. S. Threats to the national security of the state in the information sphere and the tasks of the EMERCOM of Russia in this area of activity // Civil Protection Strategy: Problems and Research. 2014;4(1):21–34.— EDN SCHGGZ. (In Russ.)]
3. Вострецова Е. В. Основы информационной безопасности: учебное пособие / Е. В. Вострецова. Екатеринбург: Уральский федеральный университет имени первого Президента России Б. Н. Ельцина, 2019. 204 с. ISBN 978-5-7996-2677-8.— EDN TBHRSS [Vostretsova E. V. Fundamentals of information security: a textbook / E. V. Vostretsova. Yekaterinburg: Ural Federal University named after the first President of Russia B. N. Yeltsin. 2019. 204 p. ISBN 978-5-7996-2677-8.— EDN TBHRSS. (In Russ.)]
4. Панарин И. Н. Информационная война и Россия / И. Н. Панарин. Москва: Мир безопасности, 2000. 159 с. ISBN 5-89258-026-1 [Panarin I. N. Information War and Russia / I. N. Panarin. Moscow: World of Security, 2000. 159 p. ISBN 5-89258-026-1. (In Russ.)]
5. Тулин С. Н. Вооруженные силы США: сценарии глобальных ударов неядерными средствами // Зарубежное военное обозрение. 2015. № 3. С. 3–10 [Tulin S. N. U.S. armed forces: scenarios for global non-nuclear strikes // Foreign Military Review. 2015;(3):3–10. (In Russ.)]
6. Лепский В. Е. Информационно-психологическая безопасность субъектов дипломатической деятельности / Дипломатический ежегодник-2002. Сборник статей. Колл. авторов. М.: Научная книга. 2003. С. 233–248 [Lepsky V. E. Information and psychological security of subjects of diplomatic activities / Diplomatic Yearbook-2002. Collection of articles. Call. authors. M.: Scientific book. 2003. P. 233–248. (In Russ.)]
7. Бартош А. А. Вопросы теории гибридной войны. М.: Горячая линия — Телеком, 2023. 324 с. [Bartosz A. A. Hybrid warfare theory questions. M.: Hot line — Telecom. 2003. 324 p. (In Russ.)]
8. Мишин Е. Т. Современные средства и системы обеспечения информационного противодействия. М., 2018. [Mishin E. T.. Modern means and systems for ensuring information counteraction. M., 2018. (In Russ.)]
9. Чернобай А. И. Противодействие распространению негативной информации в сети Интернет: опыт Китая // Идеологические аспекты военной безопасности. 2016. № 3. С. 44–48 [Chernobay A. I. Countering the spread of negative information on the Internet: the experience of China // Ideological Aspects of Military Security. 2016;(3): 44–48. (In Russ.)]
10. Киселев А. А. «Великая китайская спина»: система государственной интернет-цензуры в Китае // Вестник Пермского университета. Серии: История и Политология. 2009. № 3(7 Политология — 10 История). С. 40–46.— EDN LANHFN [Kiselev A. A. «The Great Chinese Back»: a system of state Internet censorship in China // Bulletin of Perm University. Series: History and Political Science. 2009. № . 3 (7 Political Science — 10 History). P. 40–46. EDN LANHFN. (In Russ.)]
11. Войны XXI века: теоретический труд. М.: Военная академия Генерального штаба ВС РФ, 2000. [Wars of the XXI century: theoretical work. M.: Military Academy of the General Staff of the RF Armed Forces, 2000. (In Russ.)]
12. Крысько В. Г. Секреты психологической войны (цели, задачи, методы, формы, опыт) / Под общ. ред. А. Е. Тараса. Минск: Харвест, 1999. 448 с. [Krysko V. G. Secrets of psychological war (goals, objectives, methods, forms, experience) / ed. By A. E. Taras. Minsk: Harvest, 1999. 448 p. (In Russ.)]
13. Арефьева Е. В., Бабусенко М. С. Проблемы защиты населения и территорий в чрезвычайных ситуациях в условиях современных вызовов и угроз: Справочное пособие / Е. В. Арефьева, М. С. Бабусенко, Е. М. Барышев [и др.]; Всероссийский научно-исследовательский институт по проблемам гражданской обороны и чрезвычайных ситуаций МЧС России; Под общей редакцией И. В. Сосунова. Москва: Всероссийский научно-исследовательский институт по проблемам гражданской

обороны и чрезвычайных ситуаций МЧС России, 2017. 452 с. ISBN 978-5-93970-215-7.— EDN OSQAFV [Arefieva E. V., Babusenko M. S. Problems of protecting the population and territories in emergency situations in the context of modern challenges and threats: Reference manual / E. V. Arefieva, M. S. Babusenko, E. M. Baryshev [et al.]; All-Russian Research Institute for Civil Defense and Emergencies EMERCOM of Russia; ed. by I. V. Sosunova. Moscow: All-Russian Research Institute for Civil Defense and Emergencies EMERCOM of Russia, 2017. 452 p. ISBN 978-5-93970-215-7.— EDN OSQAFV (In Russ.)]

14. Фалеев М. И., Мингалеев С. Г. Гражданская оборона России в системе международного гуманитарного реагирования в Исламской республике Афганистан, Южной Осетим, Сирии. М.: ЦСИ ГЗ МЧС России, 2018. [Faleev M. I., Mingaleev S. G. Civil defense of Russia in the system of international humanitarian response in the Islamic Republic of Afghanistan, South Ossetia, Syria. M. PKU TsSI GZ, EMERCOM of Russia. 2018. (In Russ.)]
15. Середа И. М., Ступина С. А. К вопросу об уголовно-правовых средствах противодействия информационно-психологическому воздействию // Евразийский юридический журнал. 2023. № 2(177). С. 272–274.— EDN JNMNZD [Sereda I. M., Stupina S. A. On the issue of criminal legal means of countering information and psychological influence // Eurasian Law Journal. 2023;(2):272–274. .— EDN JNMNZD. (In Russ.)]
16. Зарипов Р. И. Вербальные и невербальные приемы в технологии информационно-психологического воздействия // Вестник Московского государственного лингвистического университета. Гуманитарные науки. 2023. № 3(871). С. 46–54. https://doi.org/10.52070/2542-2197_2023_3_871_46.— EDN KTREDV [Zaripov R. I. Verbal and nonverbal techniques in information-psychological impact technology // Vestnik of Moscow State Linguistic University. Humanities. 2023;(3):46–54. (In Russ.). https://doi.org/10.52070/2542-2197_2023_3_871_46.— EDN KTREDV]

Сведения об авторах

Горячева Елена Викторовна: кандидат психологических наук, ведущий научный сотрудник 21 научно-исследовательского отдела «Информационно-аналитического обеспечения гражданской обороны» 2 научно-исследовательского центра «Развития гражданской обороны» ФГБУ ВНИИ ГОЧС (ФЦ)
Количество публикаций: более 40
Область научных интересов: проблемы обеспечения безопасности в чрезвычайных ситуациях
ORCID: 0000-0003-0354-9640
ScopusID: 57216205563
ResearcherID: HMO-9541-2023
SPIN-код: 8403-7379
Контактная информация:
Адрес: 121352, г. Москва, ул. Давыдковская, д. 7
goryacheva@vniigochs.ru

Малышев Владлен Платонович: доктор химических наук, профессор, заслуженный деятель науки Российской Федерации, главный научный сотрудник 2 научно-исследовательского центра «Развития гражданской обороны» ФГБУ ВНИИ ГОЧС (ФЦ)
Количество публикаций: более 316
Область научных интересов: проблемы обеспечения безопасности в чрезвычайных ситуациях
SPIN-код: 2163-3798
Контактная информация:
Адрес: 121352, г. Москва, ул. Давыдковская, д. 7
Vlad1936.malyshev@yandex.ru

Статья поступила в редакцию: 17.03.2025
Одобрена после рецензирования: 09.04.2025
Принята к публикации: 07.05.2025
Дата публикации: 30.06.2025

The article was submitted: 17.03.2025
Approved after reviewing: 09.04.2025
Accepted for publication: 07.05.2025
Date of publication: 30.06.2025