**Дата поступления рукописи в редакцию: 06.02.2026 г.**
**Дата принятия рукописи в печать: 10.03.2026 г.**
DOI: 10.24412/2076-1503-2026-2-375-381

***МУРАЕВ Николай Павлович,***
*канд. пед. наук, доцент,*
*профессор кафедры безопасности в ЧС,*
*Уральский институт ГПС МЧС России,*
*г. Екатеринбург, Россия,*
*e-mail: mail@law-books.ru*

***КАРАПУЗИКОВ Александр Анатольевич,***
*канд. пед. наук, доцент,*
*начальник кафедры безопасности в ЧС,*
*Уральский институт ГПС МЧС России,*
*г. Екатеринбург, Россия,*
*e-mail: mail@law-books.ru*

# ПРОБЛЕМА ПОЛУЧЕНИЯ ЛОЖНЫХ СИГНАЛОВ ОПОВЕЩЕНИЯ НАСЕЛЕНИЕМ ОТДЕЛЬНЫХ РЕГИОНОВ В УСЛОВИЯХ ВЕДЕНИЯ СПЕЦИАЛЬНОЙ ВОЕННОЙ ОПЕРАЦИИ

**Аннотация**. *В настоящей статье рассматривается вопрос несанкционированного вмешательства в системы городского оповещения, вследствие чего происходит ложное оповещение граждан о чрезвычайных ситуациях и различных опасностях. Подобные события носят негативный характер и направлены на дестабилизацию работы органов власти и жизнедеятельности населения соответствующих муниципальных образований. Основной посыл статьи – рассмотреть события, имевшие место быть по несанкционированному оповещению населения, выявить причины их возникновения и сформулировать предложения по недопущению подобных случаев впредь.*

**Ключевые слова:** *защита информации в системе оповещения, оповещение населения, сигналы оповещения, системы защиты систем оповещения населения.*

***MURAEV Nikolay Pavlovich,***
*Candidate of Pedagogical Sciences, Docent,*
*Professor of the Department of Safety in Emergency Situations,*
*Ural Institute of the State Emergency Service of the Ministry of Emergency Situations of Russia, Ekaterinburg, Russia*

***KARAPUZIKOV Alexander Anatolievich,***
*Candidate of Pedagogical Sciences, Docent,*
*Head of the Department of Safety in Emergency Situations,*
*Ural Institute of State Emergency Situations Ministry of Emergency Situations of Russia, Ekaterinburg, Russia*

# THE PROBLEM OF RECEIVING FALSE WARNING SIGNALS BY THE POPULATION OF CERTAIN REGIONS IN THE CONTEXT OF A SPECIAL MILITARY OPERATION

**Annotation**. *This article examines the issue of unauthorized interference in urban notification systems, resulting in false notification of citizens about emergency situations and various hazards. Such events are negative in nature and are aimed at destabilizing the work of the authorities and the livelihoods of the population of the relevant municipalities. The main message of the article is to con-*

*sider the events that took place due to unauthorized notification of the population, identify the causes of their occurrence and formulate proposals to prevent such cases in the future.*

**Key words:** *information protection in the notification system, public notification, warning signals, public notification systems protection systems.*

**Введение**

24 февраля 2022 года по приказу Верховного Главнокомандующего Вооруженные силы Российской Федерации начали специальную военную операцию (далее – СВО) на территории Украины. Данное столкновение носит характер вооруженного противостояния.

В этих условиях риски для жизни граждан отдельных регионов страны значительно повышаются вследствие нанесения ударов противником различными средствами поражения по объектам экономики и социальной инфраструктуры.

Указанное обстоятельство накладывает серьезный отпечаток на деятельность органов государственной власти на местах, органов повседневного управления единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций (далее – РСЧС), телевизионных и радиовещательных компаний, а также территориальных органов МЧС России, отвечающих за своевременное и достоверное информирование населения о возникающих угрозах.

В то же время в средствах массовой информации время от времени появляются сведения о несанкционированном запуске систем оповещения и доведении до населения ложных сообщений о событиях и опасностях, которые либо вовсе не имели места, либо лишь потенциально могут возникнуть в ближайшее время. Подобные информационные вбросы преследуют цель нарушить слаженную работу местных органов власти и органов повседневного управления РСЧС, а также посеять неразбериху и панику в обществе [1].

Принимая во внимание вышеизложенное, в качестве целевой установки исследования можно определить проведение анализа событий несанкционированного срабатывания систем оповещения населения, определения причин их возникновения и выработку предложений по недопущению подобных случаев.

**Основная часть**

Прежде всего следует подчеркнуть, что государственная политика и нормативное регулирование в сфере оповещения и информирования населения, а также создания, поддержания в состоянии готовности и использования систем оповещения осуществляются на основе требований, действующих законодательных и иных нормативных правовых актов

Правовую основу организации оповещения населения составляют нормативно-правовые акты такие как: федеральные законы; указы Президента Российской Федерации; постановления Правительства Российской Федерации; нормативные правовые акты федеральных органов исполнительной власти (далее – ФОИВ); правовые акты органов государственной власти субъектов Российской Федерации (далее – ОГВ) и органов местного самоуправления (далее – ОМСУ); решения Правительственной комиссии по чрезвычайным ситуациям и обеспечению пожарной безопасности (далее – КЧС и ОПБ); решения Рабочей группы Правительственной КЧС и ОПБ по координации создания и поддержания в постоянной готовности систем оповещения населения; национальные стандарты; планы действий по предупреждению и ликвидации чрезвычайных ситуаций (далее – ЧС); планы гражданской обороны и защиты населения.

К основным нормативным правовым актам, регламентирующим рассматриваемую область, относятся федеральные законы Российской Федерации, определяющие основы гражданской обороны, защиты населения и территорий от чрезвычайных ситуаций, а также регулирования в сфере связи [2-8].

Уместно отметить, что в соответствии с Положением о системах оповещения населения такие системы создаются на различных уровнях (региональном, муниципальном, объектовом) функционирования единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций. Решение о приведении в действие региональных, муниципальных и локальных систем оповещения принимается, соответственно, высшими должностными лицами субъектов Российской Федерации (руководителями высших исполнительных органов государственной власти субъектов РФ), руководителями органов местного самоуправления (главами местных администраций), а также руководителями организаций [8].

Другими словами, процесс оповещения населения строго регламентирован. Проблема, рассматриваемая в статье, кроется в его технической составляющей, а именно в тех элементах системы с помощью которых происходит передача информации населению, озвучивание и визуализация событий. Указанные элементы являются составной частью структуры системы оповещения, представляющей собой совокупность взаимодействующих компонентов, включающих специальные программно-технические средства оповещения, средства комплексной системы экстренного оповещения населения,

общероссийской комплексной системы информирования и оповещения населения в местах массового пребывания людей, громкоговорящие средства на подвижных объектах, мобильные и носимые средства оповещения, а также обеспечивающие ее функционирование каналы и линии связи, сети передачи данных единой сети электросвязи Российской Федерации.

Для обеспечения своевременной передачи населению сигналов оповещения и экстренной информации в комплексе могут использоваться: сети электрических и электронных сирен, а также мощные акустические системы; сети проводного радиовещания; сети уличной радиофикации; сети кабельного телерадиовещания; сети эфирного телерадиовещания; сети подвижной радиотелефонной связи; сети местной телефонной связи, включая таксофоны, предназначенные для оказания универсальных услуг телефонной связи с функцией оповещения; сети связи операторов связи и ведомственные сети; сети систем персонального радиовызова; информационно телекоммуникационная сеть «Интернет»; громкоговорящие средства на подвижных объектах, а также мобильные и носимые средства оповещения [8].

При этом основным способом оповещения населения является передача сигналов оповещения и экстренной информации по сетям связи, предназначенным для распространения программ телевизионного и радиовещания, так как это значительно сокращает время распространения информации и позволяет быстро сориентировать граждан о том, что случилось и какие действия необходимо предпринять немедленно. В свою очередь это не может полностью исключать возможность использования сетей всесторонней коммуникации, в первую очередь теле- и радиоэфиров, для умышленного дезинформирования населения относительно произошедших или перспективных опасных событиях, чрезвычайных ситуациях, наступление которых может создать угрозу для жизни и здоровья людей и серьезно нарушить условия их жизнедеятельности. Благодаря этому, сегодня, в условиях проведения специальной военной операции, системы оповещения населения ряда регионов России становятся объектами хакерских атак, что еще несколько лет назад было немыслимо.

Актуальность обозначенной проблемы можно проследить по ряду событий, имевших место быть на территории страны в период с 2023 по 2025 годы.

1 марта 2023 года.

По сообщению МЧС России, комплексная проверка готовности систем оповещения на всей территории Российской Федерации была перенесена на неопределенный срок в связи с хакерскими атаками. Планировалось, что 1 марта состоится проверка с запуском электросирен и временным замещением программ теле- и радиовещания, однако накануне злоумышленникам удалось вывести в эфир ложные сообщения о воздушной тревоге. Причем подобные сообщения были зафиксированы в нескольких субъектах Российской Федерации. В Подмосковье, Ленинградской области, Казани, Саратове и ряде других городов в эфире телеканалов 2х2 и ТНТ4 вместо привычного вещания транслировалось предупреждение о ракетной угрозе, а в Крыму, а также в Белгородской и Воронежской областях аналогичные сообщения были переданы по радио [10].

Москва, 12 августа 2025 г.

Хакеры взломали систему оповещения одного из московских перевозчиков. Пассажирам автобусного маршрута № 191 объявили, о готовящейся ядерной атаке со стороны Украины, и попросили срочно проследовать в ближайшее защитное сооружение. Позже выяснилось, что неизвестные хакеры взломали систему оповещения коммерческого перевозчика ООО «Трансавтолиз» и пытались дезориентировать жителей данной информацией.

Новороссийск, 24 ноября 2025 г.

По сообщению мэра города Андрея Кравченко, во время атаки дронов на объекты инфраструктуры города в муниципальной системе оповещения произошел технический сбой, в результате которого в некоторых районах города прозвучало некорректное сообщение о радиационной, химической опасности и штормовой угрозе, хотя в реальности таких угроз не было. Давая комментарий случившемуся, глава города заявил: «Произошло несанкционированное вмешательство в систему городского оповещения».

И это далеко неполный список городов и событий, где были зафиксированы подобные случаи.

Возникает вопрос, кто за этим стоит, каким образом и почему это стало возможным и что делать, чтобы подобные случаи больше не повторялись?

По мнению специалистов, занимающихся научными разработками в области создания телекоммуникационных систем с большой долей вероятности «взлом был осуществлен не без участия иностранных спецслужб так как, взломать подобные системы — дело достаточно трудоемкое, но для них это не составляет большого труда. Явно прослеживается то, что взломали системы опове-

щения, которые находились в зоне ответственности коммерческих телекомпаний и радиокомпаний» [10].

С технической стороны, процесс вмешательства в системы городского вещания (а он может быть санкционированный и несанкционированный) называется «перехват». В данном случае «перехват телевизионного цифрового сигнала со спутника произошел при помощи мощной антенны с Земли». Если точнее, то «спутник воспринимает сигналы от телеканалов только с определенными техническими параметрами и мощностью (*рис. 1*). При этом спутник технически не может определить, откуда именно поступает сигнал. Поэтому, если с внешней антенны — в том числе расположенной на территории другого государства — отправить на спутник сигнал с такими же параметрами, как у телеканала, но большей мощности, произойдёт подмена оригинального сигнала.

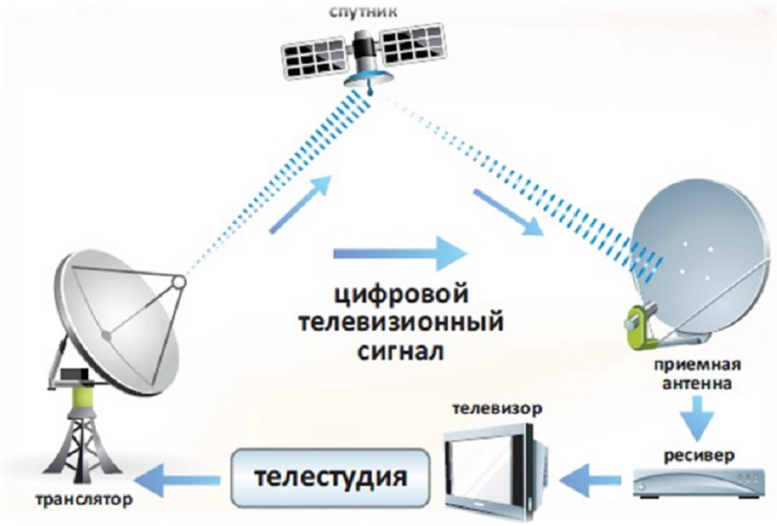


Рис.1. Трансляция телевизионного цифрового сигнала со спутника
(источник: https://museumgagarin.ru/news/iskusstvennyy_sputnik_zemli_televizionnogo_veshchaniya_ekran/?utm_medium=organic&utm_source=yandexsmartcamera)

Объективности ради стоит отметить, что сигналы телеканалов шифруются для защиты от несанкционированного вмешательства, однако уровень применяемого шифрования может отличаться. В итоге именно от этого уровня зависит, насколько трудно подменить сигнал на спутнике. В случаях, описанных в статье, нарушители наверняка действовали там, где уровень технической защиты систем был достаточно низкий. То есть данные системы были не категорированы и не защищены должным образом.

Есть еще один нюанс на который указывают эксперты по информационной безопасности. События, о которых речь шла выше, стали возможными потому, что в нашей стране системы оповещения на протяжении долгого времени создавались практически без учета требований безопасности: защита обеспечивалась на минимальном уровне. Предполагалось, что это коммерческая инфраструктура и ее безопасность будут обеспечивать сами владельцы ресурсов, однако они, разумеется, старались на этом экономить. Поэтому отчасти неудивительно, что и сегодня на телеканалах и радиостанциях требования информационной безопасности, как правило, реализованы слабо. Этими вопросами занимаются сотрудники IT-подразделений при почти полном отсутствии отдельный специалистов, отвечающих именно за информационную безопасность [11]. Последствия налицо.

**Результаты и их обсуждения**

Исследование фактов и причин взлома систем оповещения в ряде субъектов РФ позволяет сформулировать вопрос - в чью компетенцию входят вопросы защиты систем оповещения населения, и кто должен сделать выводы из случившегося?

За ответом, в первую очередь, обратимся к положениям Федерального закона № 68, в содержании которого представлены полномочия органов государственной власти субъектов Россий-

ской Федерации и органов местного самоуправления в области защиты населения и территорий от чрезвычайных ситуаций [3]. Данный документ определяет, что в компетенции органов государственной власти субъектов Российской Федерации и органов местного самоуправления находятся вопросы предоставления имеющихся технических устройств для распространения продукции средств массовой информации, выделении эфирного времени в целях своевременного оповещения и информирования населения о чрезвычайных ситуациях и подготовки населения в области защиты от чрезвычайных ситуаций; создания и поддержания в постоянной готовности систем оповещения и информирования населения о чрезвычайных ситуациях.

Иными словами, на органы власти возлагается обязанность по созданию и поддержанию в постоянной готовности систем оповещения. Для этого они организуют и проводят комплексные и технические проверки их работоспособности и готовности к использованию.

Что касается вопросов обеспечения безопасности, то они отражены в Приложении 1 Положении о системах оповещения, где в требованиях к функциям систем прописано, что они должны обладать защитой от несанкционированного доступа. По сути, это требование к телекоммуникационному оборудованию, программному обеспечению, каналам связи, которое должно быть реализовано при создании технического проекта системы, выбора оборудования и т.д. Здесь важно иметь ввиду то, что непосредственно Разработка системы защиты системы оповещения населения организуется государственным заказчиком-координатором и выполняется генеральным подрядчиком (исполнителем) в соответствии с техническим заданием на создание системы оповещения и системы её защиты, с учётом требований ГОСТ Р 59793 2021, ГОСТ Р 51583 2014, а также нормативных актов субъекта РФ.

Процесс разработки системы защиты включает два этапа: 1) проектирование системы защиты системы оповещения населения; 2) подготовку эксплуатационной документации на систему защиты.

При проектировании определяются объекты защиты, к которым относятся: информация о параметрах (состоянии) технических средств оповещения (ТСО) и процесса оповещения (входная и выходная, управляющая, контрольно-измерительная и иная критически важная технологическая информация); сами ТСО: технические средства (АРМ, промышленные серверы, телекоммуникационное оборудование, каналы связи, ПЛК, исполнительные устройства, за исключением оконечных средств оповещения — громкоговорителей и электросирен), программное обеспечение (микропрограммное, общесистемное, прикладное), а также средства защиты информации.

К вышеизложенному стоит добавить еще один важный пункт. В 2021 году вступило в силу Положение о системах оповещения населения. Пункт 6 данного Положения вводит новые требования к обеспечению информационной безопасности в системах оповещения населения. Теперь необходимо обеспечивать защищенность систем оповещения населения согласно Приказам ФСТЭК России № 17 и 31 в зависимости от уровня значимости обрабатываемой в системе информации.

Пункт 6 «Требования к защите информации» указанного Положения определяет классы защищенности для систем оповещения:

– РАСЦО и КСЭОН должны соответствовать классу защищенности не ниже 2.
– Муниципальные и локальные системы оповещения (МАСЦО и ЛСО) населения должны соответствовать классу защищенности не ниже 3.

Таким образом органы государственной власти субъектов Российской Федерации и органы местного самоуправления в большинстве своем придерживаются выполнения требований законодательства в области обеспечения информационной безопасности систем оповещения, используя при этом системы оповещения в защищенном исполнении или как их еще называют категорированные системы оповещения, имеющие достаточную высокую степень защиты. И надо отметить, что на сегодняшний момент успешных попыток взломов таких систем не зафиксировано.

Другое дело коммерческие и негосударственные компании и организации, которые оказывают услуги по оповещению населения в рамках официально заключенных договоров (соглашений) о взаимодействии с органами власти и где вопросы обеспечения безопасности систем оповещения целиком и полностью относятся к их компетенции и решаются как видно из проведенного выше анализа не всегда успешно.

В этой связи постоянно действующие органы управления территориальных подсистем РСЧС, организации – владельцы систем оповещения, а также организации и операторы связи, телерадиокомпании и редакции средств массовой информации обязаны на регулярной основе проводить комплекс организационных и технических мероприятий, направленных на недопущение несанкционированного задействования систем оповещения и передачи сигналов оповещения и экстренной информации населению, привлекая для выполнения таких мероприятий специалистов, обладающих необходимой компетенцией в дан-

ных областях. Такая, качественно проведенная работа, позволит исключить совсем или минимизировать последствия от возможной реализации угроз несанкционированного вмешательства в системы муниципального оповещения.

Каковы могут быть последствия от непринятия должных мер по недопущению стороннего вмешательства в системы оповещения?

Даже непериодическое успешное повторение подобных хакерских атак на системы оповещения может в перспективе принести достаточно неприятный эффект, а именно:

1) граждане попросту утратят доверие к городским системам оповещения;
2) старт получит процесс нарастания критической ситуации в сфере доверия населения к органам власти, медиа и негосударственным организациям;
3) у злоумышленников появляются дополнительные возможности по расширению сферы и видов провокаций, что в перспективе может привести к снижению эффективности реагирования на возникающие чрезвычайные ситуации и опасности.

Среди возможных решений проблемы нам представляется следующее:

1) усиление контроля за обеспечением кибербезопасности телеканалов и радиостанций со стороны регуляторов;
2) использование более современных методов и средств защиты систем оповещения. Например, активное внедрение системы обнаружения вторжений (IDS), для выявления несанкционированной и вредоносной активности в компьютерных сетях [11].
3) внедрение мультифакторной аутентификации пользователей при доступе к любым информационным ресурсам и сетевой инфраструктуре компаний, имеющим договора на распространение информации по оповещению населения.
4) включение в штат органов и организаций, в ведении которых находятся системы оповещения, специалистов по информационной безопасности и наделение их полномочиями в объеме решаемых ими задач.
5) повышение требований к категорированию систем оповещения населения.

**Список литературы:**

[1] Положение о системах оповещения населения // Гражданская защита. – 2021. – № 2(546). – С. 35-38. – EDN NKKZFK.

[2] Федеральный закон Российской Федерации от 12.02.98 г. № 28 «О гражданской обороне» [Электронный ресурс]. Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_17861/. (Дата обращения: 16.01.2026г.).

[3] Федеральный закон Российской Федерации от 21.12.1994 г. №68 «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера» [Электронный ресурс]. Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_5295/. (Дата обращения: 16.01.2026г.).

[4] Федеральный закон Российской Федерации от 07.07.2003 г. № 126 «О связи». [Электронный ресурс]. Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_43224/. (Дата обращения: 16.01.2026г.).

[5] Указ Президента Российской Федерации от 13.11.2012 г. № 1522 «О создании комплексной системы экстренного оповещения населения об угрозе возникновения или о возникновении чрезвычайных ситуаций». [Электронный ресурс]. Режим доступа: http://www.kremlin.ru/acts/bank/36332. (Дата обращения: 16.01.2026г.).

[6] Постановление Правительства Российской Федерации от 28.12.2020 г. №2322 «О порядке взаимодействия федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, органов местного самоуправления с операторами связи и редакциями средств массовой информации в целях оповещения населения о возникающих опасностях» [Электронный ресурс]. Режим доступа: https://base.garant.ru/400165402/. (Дата обращения: 16.01.2026г.).

[7] Постановление Правительства Российской Федерации от 17.05.2023 г. №769 «О порядке создания, реконструкции и поддержания в состоянии постоянной готовности к использованию систем оповещения населения» (вместе с «Правилами создания, реконструкции и поддержания в состоянии постоянной готовности к использованию систем оповещения населения») [Электронный ресурс]. Режим доступа: https://42.mchs.gov.ru/uploads/resource/2024-01-31/5-1-2-postanovleniya-pravitelstva-rf_170667113461871060.pdf. (Дата обращения: 16.01.2026г.).

[8] Приказ МЧС России, Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 31.07.2020 г. №578/365 «Об утверждении Положения о системах оповещения населения» [Электронный ресурс]. Режим доступа: https://www.garant.ru/products/ipo/prime/doc/74723317/. (Дата обращения: 16.01.2026г.).

[9] Приказ МЧС России, Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 31.07.2020 г. №579/366 «Об утверждении Положения по организации эксплуатационно-технического обслуживания систем

оповещения населения» [Электронный ресурс]. Режим доступа: https://base.garant.ru/74812884/. (Дата обращения: 16.01.2026г.).

[10] Проверку систем оповещения в России отложили из-за хакерских атак [Электронный ресурс]. Режим доступа: https://news.rambler.ru/disasters/50295203/?utm_content=news_media&utm_medium=read_more&utm_source=copylinkhttps://news.rambler.ru/disasters/50295203-proverku-sistem-opovescheniya-v-rossii-otlozhili-iz-za-hakerskih-atak/. (Дата обращения: 16.01.2026г.).

[11] Опять ложная тревога: теперь взломали спутник медиа-холдинга «Газпром». В Саратове МЧС отменило сирены [Электронный ресурс]. Режим доступа: https://www.business-vector.info/opyat-lozhnaya-trevoga-teper-158431/. (Дата обрат щения: 16.01.2026г.).

**References:**

[1] Regulation on public warning systems//Civil protection. – 2021. – № 2(546). - S. 35-38. – EDN NKKZFK.

[2] Federal Law of the Russian Federation of 12.02.98 No. 28 “On Civil Defense” [Electronic Resource]. Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_17861/. (Accessed 16.01.2026).

[3] Federal Law of the Russian Federation of 21.12.1994 No. 68 “On the Protection of the Population and Territories from Natural and Man-Made Emergencies” [Electronic Resource]. Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_5295/. (Accessed 16.01.2026).

[4] Federal Law of the Russian Federation No. 126 dated 07.07.2003 “On Communications.” [Electronic resource]. Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_43224/. (Accessed 16.01.2026).

[5] Decree of the President of the Russian Federation of 13.11.2012 No. 1522 “On the creation of an integrated system for emergency notification of the population about the threat or occurrence of emergency situations.” [Electronic resource]. Access mode: http://www.kremlin.ru/acts/bank/36332. (Accessed 16.01.2026).

[6] Decree of the Government of the Russian Federation of 28.12.2020 No. 2322 “On the Procedure for Interaction of Federal Executive Bodies, Executive Bodies of Constituent Entities of the Russian Federation, Local Self-Government Bodies with Telecom Operators and Editorial Offices of the Media in Order to Notify the Population of Emerging Dangers” [Electronic Resource]. Access mode: https://base.garant.ru/400165402/. (Accessed 16.01.2026).

[7] Decree of the Government of the Russian Federation of 17.05.2023 No. 769 “On the procedure for creating, reconstructing and maintaining in a state of constant readiness for the use of public warning systems” (together with “Rules for creating, reconstructing and maintaining in a state of constant readiness for the use of public warning systems”) [Electronic resource]. Access mode: https://42.mchs.gov.ru/uploads/resource/2024-01-31/5-1-2-postanovleniya-pravitelstva-rf_170667113461871060.pdf. (Accessed 16.01.2026).

[8] Order of the Ministry of Emergency Situations of Russia, the Ministry of Digital Development, Communications and Mass Media of the Russian Federation of 31.07.2020 No. 578/365 “On Approval of the Regulation on Public Warning Systems” [Electronic Resource]. Access mode: https://www.garant.ru/products/ipo/prime/doc/74723317/. (Accessed 16.01.2026).

[9] Order of the Ministry of Emergency Situations of Russia, the Ministry of Digital Development, Communications and Mass Media of the Russian Federation of 31.07.2020 No. 579/366 “On approval of the Regulation on the organization of operational and technical maintenance of public warning systems” [Electronic resource]. Access mode: https://base.garant.ru/74812884/. (Accessed 16.01.2026).

[10] Verification of warning systems in Russia was postponed due to hacker attacks [Electronic resource]. Режим доступа: https://news.rambler.ru/disasters/50295203/?utm_content=news_media&utm_medium=read_more&utm_source=copylinkhttps://news.rambler.ru/disasters/50295203-proverku-sistem-opovescheniya-v-rossii-otlozhili-iz-za-hakerskih-atak/. (Дата обращения: 16.01.2026г.).

[11] False alarm again: now the satellite of the Gazprom media holding has been hacked. In Saratov, the Ministry of Emergency Situations canceled sirens [Electronic resource]. Access mode: https://www.business-vector.info/opyat-lozhnaya-trevoga-teper-158431/. (Accessed 16.01.2026).