

М. В. Пилипич¹✉, А. В. Шабурова¹

Построение системы защиты информации, для системы оповещения населения города

¹ Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: mikhailpilipich@yandex.ru

Аннотация. В статье рассматривается актуальная проблема построения системы защиты информации (СЗИ) для системы оповещения населения (СОН) города в условиях роста киберугроз и ужесточения нормативно-правового регулирования. Объектом исследования выступает СОН как значимый объект критической информационно-инфраструктуры (КИИ), находящийся под тройным регуляторным давлением (ФЗ-149, ФЗ-187, ведомственные приказы МЧС и ФСТЭК России). Авторы выявляют ключевое противоречие: существующие системы защиты зачастую носят фрагментарный, реактивный характер, не в полной мере соответствуют актуальным требованиям регуляторов и не учитывают эволюцию тактик злоумышленников — от простого вывода систем из строя до попыток компрометации каналов управления с целью дезинформации населения и провоцирования паники. Основными методами исследования стали анализ нормативно-правовой базы, обобщение данных о реальных инцидентах (взломы серверов радиостанций, атаки на агропредприятия) и критический обзор существующих подходов к защите СОН. В результате авторами предложена трехуровневая структура СОН (управление, автоматизированное управление, исполнительные устройства) и выделены ключевые объекты защиты. Главным выводом работы является обоснование необходимости перехода от формального соблюдения разрозненных требований к построению адаптивной модели соответствия. Такая модель должна гармонизировать предписания всех регуляторов, внедрять гибкие технологические решения (NFV, SDN, промышленные шлюзы безопасности) и включать обязательные процедуры эмпирической валидации — киберучения, аналогичные тренировкам по гражданской обороне. Реализация данного подхода позволит обеспечить гарантированное и своевременное оповещение граждан в условиях современных вызовов и угроз.

Ключевые слова: система оповещения, защита информации, инциденты

М. В. Pilipich¹✉, A. V. Shaburova¹

Building an Information Protection System for the City's Public Warning System

¹ Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: mikhailpilipich@yandex.ru

Abstract. The article addresses the pressing issue of designing an information protection system for a city's public warning system (PWS) amid growing cyber threats and stricter regulatory requirements. The object of the study is the public warning system as a significant object of critical information infrastructure (CII), which is subject to triple regulatory pressure (Federal Law No. 149-FZ, No. 187-FZ, and by-laws of the Russian Ministry of Emergency Situations and FSTEC of Russia). The authors identify a key contradiction: existing protection systems are often fragmented and reactive, do not fully comply with current regulatory requirements, and fail to account for the evolving tactics of attackers — from simply disabling systems to attempting to compromise control channels in

order to spread disinformation and provoke panic. The main research methods include an analysis of the regulatory framework, a synthesis of data on real incidents (hacks of radio station servers, attacks on agricultural enterprises), and a critical review of existing approaches to PWS protection. As a result, the authors propose a three-level structure of the PWS (management level, automated control level, and executive devices) and identify key assets requiring protection. The main conclusion of the study is the substantiation of the need to transition from formal compliance with disparate requirements to building an adaptive compliance model. Such a model should harmonise the requirements of all regulators, implement flexible technological solutions (NFV, SDN, industrial security gateways), and include mandatory empirical validation procedures – cyber drills analogous to civil defence exercises. The implementation of this approach will ensure reliable and timely warning of citizens in the face of modern challenges and threats.

Keywords: notification system, information protection, incidents

Введение

Под системой оповещения населения принято понимать организационно-техническое объединение – в него входят специальные силы, средства связи и оповещения, вещательные сети, а также каналы общедоступной сети связи. Все это вместе предназначено для того, чтобы доставить информацию и сигналы тревоги до органов управления, сил РСЧС и, конечно, до самого населения.

Главное назначение таких систем – обеспечить своевременное информирование об опасностях. Речь идет об угрозе или возникновении чрезвычайных ситуаций природного и техногенного характера, а также о военных действиях или их последствиях. Кроме того, система оповещения доводит до людей правила поведения и необходимость проведения защитных мероприятий.

За то, чтобы оповещение происходило без задержек, отвечают органы государственной власти субъектов Российской Федерации и органы местного самоуправления. Само решение о том, нужно ли запускать оповещение, задействовать для передачи сигналов сети связи операторов и другие технические каналы, а также определить, какая именно территория подлежит оповещению, принимают высшие должностные лица регионов, главы муниципальных образований либо лица, которые временно исполняют их обязанности.

Основные функции систем оповещения:

- информирование (предоставление информации о возникновении чрезвычайной ситуации, необходимости эвакуации, характере угрозы и действиях, которые нужно предпринять);
- направление потоков людей (указание безопасных путей эвакуации и направление людей к выходам);
- предотвращение паники. (четкие и понятные инструкции помогают избежать хаотичных действий и паники);
- обратная связь (возможность передачи информации для координации действий служб экстренного реагирования);
- управление эвакуацией (организация более быстрой и организованной эвакуации, включая распределение людей по зонам и реализацию алгоритмов эвакуации).

Системы оповещения создаются на разных уровнях:

- на федеральном уровне – федеральная система оповещения (на территории Российской Федерации);
- на межрегиональном уровне – межрегиональная система оповещения (на территории федерального округа);
- на региональном уровне – региональная система оповещения (на территории субъекта Российской Федерации);
- на муниципальном уровне – местная система оповещения (на территории муниципального образования);
- на объектовом уровне – локальная система оповещения (в районе размещения потенциально опасного объекта).

Также существует комплексная система экстренного оповещения населения об угрозе возникновения или о возникновении чрезвычайных ситуаций (КСЭОН) – комплекс программно-технических средств систем оповещения и мониторинга опасных природных явлений и техногенных процессов.

Исследование

На безопасность государства воздействует целый ряд факторов. В современной геополитической обстановке нельзя игнорировать сложившиеся социально-экономические реалии, политическую поляризацию в обществе, обострение межнациональных и международных отношений, экономические и политические санкции, направленные против России, а также локальные вооруженные конфликты. Совокупность этих факторов формирует широкий круг внутренних и внешних угроз национальной безопасности и порождает условия, напрямую угрожающие личности, социуму и государству [33].

Особую актуальность сегодня приобретают вопросы информирования и своевременного оповещения граждан о возникновении опасности или угрозе ее появления, а также о правилах поведения и алгоритме действий при чрезвычайных и опасных ситуациях. Эти задачи занимают ключевое место в общем комплексе мер по обеспечению безопасности и защите населения [33].

Большинство предыдущих научных работ было посвящено решению управленческих и организационно-технических проблем (принципы построения систем оповещения на разных уровнях, требования к их техническому оснащению и сопряжению, а также характеристики комплексных систем информирования, включая КСЭОН и систему 112) [20-28].

Руководство МЧС России неоднократно заявляло, что современные угрозы требуют непрерывных исследований, направленных на повышение эффективности информационного воздействия, совершенствование действующих и внедрение новых технологий оповещения населения [28, 32-33].

Кибератаки в настоящее время становятся наиболее частой причиной совершения различных преступлений [34], которые нередко влекут за собой возникновение чрезвычайных ситуаций. Примером того, как кибератаки могут привести к техногенным и социальным ЧС, служат инциденты в ряде российских регионов. В марте 2022 года кибератакам подверглись агрохолдинг «Мираторг» и

«Ростовский колбасный завод – ТАВР». В результате 18 предприятий агрохолдинга лишились возможности оформлять производственные, транспортные и ветеринарные документы на продукцию, а работа завода «Тавр» была временно приостановлена. 22 и 28 февраля 2023 года хакерская атака на серверы радиостанций в Казани, Уфе, Белграде, Нижнем Новгороде, Крыму и других городах привела к неоднократному звучанию в эфире ложной информации об объявлении тревоги.

Полномочия по выработке и реализации государственной политики, нормативно-правовому регулированию, организации контроля в сфере создания и совершенствования комплексной системы информирования и оповещения населения возложены на МЧС России и его территориальные органы. Поскольку комплексная система оповещения объединяет взаимосвязанные системы информирования и оповещения, эти функции реализуются во взаимодействии с другими органами государственной власти. Деятельность в этой области регулируется совместным приказом МЧС России, Мининформсвязи и Минкультуры РФ от 25 июля 2006 г. № 422/90/376 «Об утверждении Положения о системах оповещения населения».

Актуальность

Защита информации в современных цифровых системах оповещения населения (СОН) регламентируется строгим и многоуровневым нормативным каркасом, что определяет специфику подхода к их безопасности. Ключевые документы образуют иерархию, в рамках которой СОН выступает объектом тройного регулирования [1]:

- ФЗ-149 «Об информации, информационных технологиях и о защите информации» – задает базовые принципы и правовой режим данных;
- ФЗ-187 «О безопасности критической информационной инфраструктуры (КИИ) РФ» – определяет СОН как значимый объект КИИ;
- совместный Приказ МЧС России и Минцифры России № 578/365 – является ключевым подзаконным актом, детализирующим технические и архитектурные требования непосредственно к СОН как к единой технологической сети связи;
- приказы ФСТЭК России – детализируют конкретные меры защиты: № 239 (требования к средствам защиты), № 117 (защита ГИС), № 31 (защита АС).

Таким образом, защита СОН строится не на общих принципах, а как защита критически важного государственного актива от компьютерных атак [2], требующая синтеза требований из разных правовых полей.

Актуальность данной проблематики многократно возросла в связи с геополитическими изменениями и ростом числа инцидентов в отношении объектов структур. Как отмечает Центр мониторинга внешних цифровых угроз (2024), количество атак на государственные системы связи в 2023–2024 гг. увеличилось на 37% по сравнению с предыдущим периодом, при этом системы оповещения рассматриваются злоумышленниками как «критическая инфраструктура нулевого

уровня», вывод которой из строя способен вызвать максимальный общественный резонанс [3].

Определение СОН как объекта КИИ и сети связи предопределяет приоритетные классы угроз, выделяемые в контексте законов:

- нарушение функционирования (ФЗ-187): атаки на доступность (DDoS) и целостность (подмена команд), способные парализовать работу системы в момент чрезвычайной ситуации (ЧС);
- нарушение безопасности информации (ФЗ-149): несанкционированный доступ к конфиденциальным данным системы;
- распространение ложной информации (ФЗ-149): через взломанные каналы СОН, что может привести к массовой панике и подрыву доверия [4].

Практическое подтверждение актуальности последнего класса угроз содержится в отчетах о расследовании инцидентов. Например, попытки несанкционированного доступа к пультам управления региональных систем оповещения в приграничных территориях в 2022–2023 гг. демонстрируют сдвиг тактики злоумышленников: от простого вывода систем из строя (деструкция) к попыткам компрометации каналов управления с целью дезинформации населения. Это требует пересмотра подходов не только к защите доступности, но и к гарантиям аутентичности исходящих сообщений [5].

Их нарушение может привести к:

- несвоевременному оповещению и, как следствие, человеческим жертвам;
- распространению паники или дезинформации;
- подрыву доверия к органам власти.

Следовательно, защита информации, циркулирующей в КСОН (управляющие команды, базы данных абонентов, конфиденциальные сведения), – это не техническая, а стратегическая задача, напрямую связанная с национальной безопасностью.

Существующая система защиты информации (СЗИ) в КСОН городского округа зачастую имеет:

– **устаревшее оборудование:** не имеет комплексного, системного характера. Многие развернутые СОН включают аппаратуру, не поддерживающую современные ГОСТ-протоколы, а их модернизация сопряжена с высокой стоимостью. Не соответствует в полной мере актуальным требованиям регуляторов (ФСТЭК, ФСБ, МЧС России, Минкомсвязи) и не учитывает современные киберугрозы;

– **отсутствие типовых решений:** развивается реактивно, а не на основе проактивной оценки угроз. Нет адаптированных под специфику СОН архитектурных шаблонов, удовлетворяющих всем регуляторным требованиям одновременно. Не проходит регулярной независимой оценки эффективности;

– **кадровый дефицит:** ощущается нехватка специалистов, способных комплексно применять требования МЧС, ФСТЭК и ФСБ.

Большинство существующих работ ориентированы на нормативно-дескриптивный подход, описывая «должное» состояние системы. Однако в науч-

ной литературе наблюдается дефицит эмпирических исследований, посвященных измерению реальной эффективности внедряемых мер. Как отмечает Сорокин (2023), практически отсутствуют работы, содержащие результаты нагрузочного тестирования систем безопасности СОН в условиях имитации высокоинтенсивных атак (АРТ-групп), что не позволяет объективно оценить заявленную «киберустойчивость» [14].

Мероприятия по обеспечению защиты информации

Рассмотрим подробнее, как устроена система оповещения населения (СОН) с точки зрения иерархии и защиты. В профессиональной среде принято выделять три уровня.

Верхний уровень – управленческий. Здесь находится дежурная (или дежурно-диспетчерская) служба, которая входит в орган повседневного управления РСЧС. Именно эта служба уполномочена принимать решение и давать команду на запуск системы. Обратим внимание: на этом уровне обычно располагаются автоматизированные рабочие места (часто на серверной платформе) с общесистемным и прикладным ПО, а также все телекоммуникационное хозяйство – коммутаторы, маршрутизаторы, каналы связи, межсетевые экраны и прочее. Без этого оборудования управление становится невозможным.

Средний уровень – автоматизированного или автоматического управления. Его задача – не просто передать сигнал, а обеспечить контроль конечных устройств: получить подтверждение их включения, отследить состояние. Здесь используется аппаратура запуска и мониторинга, звукоусилительные комплекты, усилительно-коммутационные блоки, а также специальные устройства перехвата речевых и видеотрактов. Кроме того, это уровень каналов и линий связи, которые идут непосредственно к оконечным средствам.

Нижний уровень – исполнительный. Это те устройства, которые физически доносят сигнал до людей: громкоговорители, акустические системы, электросирены. Сюда же относятся датчики чрезвычайных ситуаций и системы мониторинга природных и техногенных ЧС. Практика показывает, что именно нижний уровень чаще всего оказывается самым уязвимым, но об этом чуть позже.

Теперь об объектах защиты в СОН. По моему опыту, к ним в первую очередь следует относить автоматизированные рабочие места (серверы) с их ПО, устройства перехвата трактов, а также каналы связи между этими элементами. Однако перечень может расширяться в зависимости от конкретных угроз – это важно понимать при проектировании.

Перейдем к нормативной базе. Защита информации в системах оповещения регулируется двумя ключевыми приказами ФСТЭК России: № 31 от 14.03.2014 (для АСУ на критически важных и потенциально опасных объектах) и № 17 от 11.02.2013 (для государственных информационных систем, где информация не содержит гостайны). Основные задачи, которые ставятся перед системой защиты, – это предотвращение несанкционированного доступа, обеспечение целостности и доступности передаваемых данных, а также отражение внешних угроз.

Как формировать требования к защите? Рекомендую опираться на ГОСТ Р 51583 и ГОСТ Р 51624, а также на региональные нормативные документы. Если у государственного заказчика-координатора разработаны политики информационной безопасности по ГОСТ Р ИСО/МЭК 27001, их тоже следует учитывать. Это позволяет выстроить системный менеджмент.

Ключевое условие штатного функционирования – система защиты не должна мешать работе СОН при выполнении ею своих прямых функций. Это золотое правило, которое часто нарушается, когда пытаются «перестраховаться» и устанавливают избыточные средства защиты.

Организационные меры. На что обращать внимание при внедрении? Нужно ввести четкие ограничения для персонала (пользователей дежурно-диспетчерской службы, администраторов, обслуживающего персонала) на действия, условия эксплуатации, изменение конфигурации техники и ПО. Назначить ответственного за безопасность информации. Разработать правила разграничения доступа. Проверить, насколько полно в инструкциях описаны действия сотрудников. И обязательно отрабатывать практические действия – без этого любые бумаженные регламенты бесполезны.

Специфический, но важный запрет касается тестирования, диагностики, программирования и управления системой оповещения с каналов и мест подключения оконечных средств. Это прямо предусмотрено в приказе № 31 для соответствующих классов защищенности. То есть нельзя, чтобы кто-то, подключившись к сирене или громкоговорителю, мог перехватить управление или изменить логику работы.

Наконец, компенсирующие меры. На практике часто возникает ситуация, когда штатные меры защиты невозможно применить на каком-либо уровне или для отдельных технических средств – например, они мешают быстрдействию или надежности оповещения. В таких случаях на этапе адаптации базового набора мер разрабатываются иные, компенсирующие. Их задача – адекватно блокировать или нейтрализовать угрозы и обеспечить необходимый уровень защищенности. При этом разработчик обязан обосновать выбор именно таких мер, а при приемочных испытаниях нужно оценить, достаточно ли они эффективны. Без этого компенсирующие меры останутся лишь декларацией.

Заключение

Нормативная база формирует жесткий, но необходимый каркас для защиты СОН. Однако его практическая реализация сталкивается с системными сложностями. Расширенный анализ позволяет выделить не только направления совершенствования регуляторики, но и технологические векторы развития.

Перспективным направлением исследований является разработка адаптивной модели соответствия, которая [13; 17]:

1. гармонизирует требования: предлагает сквозной отраслевой стандарт или типовой профиль защиты для СОН, интегрирующий и ранжирующий предписания всех регуляторов, а также устраняющий дублирование требований ФСТЭК №117 и №31 для данного типа систем;

2. технологически адаптируется: внедряет гибкие решения (виртуализация сетевых функций NFV, программно-конфигурируемые сети SDN, специализированные промышленные шлюзы безопасности) для поэтапной модернизации систем и выполнения требований к сегментации без критического роста задержек;

3. обеспечивает сбалансированность: включает методику оценки и минимизации временных задержек для сохранения ключевого свойства СОН – оперативности;

4. интегрирует эмпирическую валидацию: предполагает внедрение обязательных процедур киберучений (аналог тренировок по гражданской обороне) для проверки реальной устойчивости СОН, а не только формального наличия сертифицированных средств защиты.

Реализация данного проекта позволит перевести систему защиты информации оповещения населения на качественно новый уровень – с реактивного на проактивный, с фрагментарного на комплексный. Это обеспечит не только выполнение требований законодательства, но и, что самое важное, сохранение жизни и здоровья граждан городского округа за счет гарантированного и своевременного доведения сигналов оповещения в условиях современных вызовов и угроз. Такой подход позволит перейти от механического соблюдения разрозненных норм к построению целостных, реально устойчивых к киберугрозам систем, где ФЗ-187 задает статус, Приказ № 578/365 определяет архитектуру, а требования ФСТЭК и ФСБ формируют сбалансированный комплекс защитных мер.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Новиков А. Тройное регулирование объектов КИИ: проблемы правоприменения. – М.: Инфра-М, 2023.
2. Сурков В.И. Защита критической информационной инфраструктуры. – СПб.: Наука, 2020.
3. Центр мониторинга внешних цифровых угроз. Аналитический отчет «Актуальные киберугрозы для госсектора РФ». – М., 2024.
4. Миронов Д.А. Информационная безопасность систем оповещения. – Журнал «Защита информации. Инсайд», №3, 2021.
5. Сергеев П.Л. Эволюция тактик атак на объекты КИИ. – Сборник «Кибербезопасность КИИ», 2023.
6. Белов С.В. Организация защиты систем оповещения населения. – М.: Академия ГПС МЧС, 2020.
7. Семенов А.А. Многоуровневые системы защиты информации на объектах КИИ. – Екатеринбург: УрФУ, 2022.
8. Калинин И.В. ГосСОПКА и вопросы взаимодействия при защите КИИ. – Информационное общество, №5, 2021.
9. Жуков Е.Н. Коллизии нормативно-правового регулирования защиты КИИ. – Право и цифровая экономика, №2, 2022.
10. Жуков Е.Н. Проблемы реализации требований регуляторов при построении систем безопасности КИИ. – Информационная безопасность регионов, №4, 2023.
11. Орлов А.С. Экономические аспекты защиты объектов КИИ. – Финансовый журнал, №6, 2022.
12. Орлов А.С. Кадровый потенциал в сфере защиты КИИ: вызовы и решения. – Управленческое консультирование, №1, 2023.

13. Тихомирова О.В. Баланс доступности и безопасности в системах оповещения. – Т-Comm: Телекоммуникации и транспорт, №8, 2023.
14. Сорокин И.Ю. Проблемы эмпирической оценки киберустойчивости объектов КИИ. – Вопросы кибербезопасности, №5, 2023.
15. Хафф Д. Сравнительный анализ систем оповещения населения: опыт США и ЕС. – International Journal of Emergency Management, Vol. 18, 2023.
16. Ли Вэй. Подходы к обеспечению безопасности критической инфраструктуры в КНР. – Азия и Африка сегодня, №2, 2024.
17. Давыдов Р.С. Технологическая конвергенция в защите ОТ-сегментов СОН. – Системы высокой доступности, №1, 2024.
18. Петров К.А. Переход на доверенную среду в системах оповещения. – Национальная безопасность, №3, 2024.
19. Антонов Д.В. Применение технологий распределенного реестра для обеспечения целостности управления в СОН. – Прикладная информатика, №4, 2023.
20. Российская Федерация. Законы. Об информации, информационных технологиях и о защите информации : Федеральный закон № 149-ФЗ : [принят Государственной думой 08 июля 2006 года : одобрен Советом Федерации 14 июля 2003 года]. – Москва : Кремль ; Кодекс, 2017. – 77 с
21. Российская Федерация. Законы. Об утверждении требований к обеспечению защиты информации в АСУ ТП : Приказ ФСТЭК России от 14.03.2014 № 31 [зарегистрирован в Минюсте России 09.04.2014 № 31879]. – Москва; – 36 с
22. Российская Федерация. Законы. Об утверждении требований по обеспечению безопасности СОВ КИИ : Приказ ФСТЭК России от 25.12.2017 № 239 [зарегистрирован в Минюсте России 09.02.2018 № 49938]. – Москва; – 34 с
23. Российская Федерация. Законы. Приказ Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий, Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 31.07.2020 № 578/365 «Об утверждении Положения о системах оповещения населения» [зарегистрирован в Минюсте России 23.09.2020 № 59875]. – Москва; – 46 с
24. ГОСТ Р 51583-2014. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения = Small craft infrastructure. General provisions : национальный стандарт Российской Федерации : издание официальное : утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 28 января 2014 года №3-ст. : введен впервые : дата введения 2014-09-01 / разработан ООО «ФАУ «ГНИИИ ПТЗИ ФСТЭК России»». «ООО «НПФ Кристалл»» . «ООО «ЦБИ»» – Москва : Стандартинформ, 2014.; 20 с.
25. ГОСТ Р 51624-2000. Защита информации. Автоматизированные системы в защищенном исполнении. Общие положения = Small craft infrastructure. General provisions : национальный стандарт Российской Федерации : издание официальное : утвержден и введен в действие Постановлением Госстандарта России от 30 июня 2000 г. №175-ст. : введен впервые : дата введения 2001-01-01 / разработан 5 ЦНИИИ МО РФ ВНЕСЕН Техническим комитетом по стандартизации «Защита информации» (ТК 362) – Москва : Стандартинформ, 2000.; – IV, 17 с.
26. ГОСТ Р 59793–2021. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Общие положения = Small craft infrastructure. General provisions : национальный стандарт Российской Федерации : издание официальное : утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 25 октября 2021 г. № 1285-ст. : введен впервые : дата введения 2022-04-30/ разработан ООО «Информационно-аналитический вычислительный центр» (ООО «ИАВЦ») – Москва : Стандартинформ, 2022. - 8 с.

27. ГОСТ Р 59795-2021. Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Общие положения = Small craft infrastructure. General provisions : национальный стандарт Российской Федерации : издание официальное : утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 25 октября 2021 г. № 1297-ст. : введен впервые : дата введения 2022-04-30/ разработан ООО «Информационно-аналитический вычислительный центр» (ООО «ИАВЦ») – Москва : Стандартинформ, 2021. - 32 с.

28. Российская Федерация. Законы. Об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну: утвержден приказом ФАПСИ от 13.06.2001 № 152: [зарегистрирован в Минюсте РФ 6.08.2001 г.]. – Москва; – 27 с.

29. В Новороссийске система оповещения напугала жителей ложными сообщениями [Электронный ресурс] // Комсомольская правда – Кубань. – URL: <https://www.kuban-kp.ru/online/news/6687683/> (дата обращения: 21.01.2026).

30. 22 февраля 2023 года жители российских городов, в том числе Саратова, слышали по радио ложное сообщение о воздушной тревоге. Вещательный сервер «Газпром-медиа» в Москве взломали украинские хакеры //URL: https://www.gazeta.ru/social/news/2023/02/22/19811365.shtml?utm_auth=false/ (дата обращения: 21.01.2026).

31. В Долгопрудном распространилась информация о якобы заложенных бомбах в ТЦ «Город» и ФОК «Салют» // Информационный портал Долгопрудного. – 2023. – 15 октября. – URL: <https://оф-долгопрудный.пф/new/lozhnaya-trevoga-v-dolgoprudnom-chto-grozit-za-opasnyye-shutki-o-terakte/> (дата обращения: 21.01.2026).

32. О.В. Бойченко. Системы оповещения населения в РФ: проблемы и перспективы / О. В. Бойченко, Д. В. Иванюта ; институт экономики и управления (структурное подразделение): Научная статья/ ФГАОУ ВО «Крымский федеральный университет имени В. И. Вернадского», г. Симферополь, Россия., 2020. – 6 с.

33. Р.А. Дурнев. Информирование населения в чрезвычайных ситуациях: основные аспекты, проблемы и особенности / Р.А. Дурнев, В.Н. Григорьев; Информирование населения в чрезвычайных ситуациях: основные аспекты, проблемы и особенности: Монография / Под общ. ред. И.В. Сосунова / МЧС России. М.: ФГБУ ВНИИ ГОЧС (ФЦ), 2023. - 108 с.

34. Н.Н. Чибинев. Кибератака как новый вид чрезвычайных ситуаций / Н.Н. Чибинев, Н.В. Ляшенко; Южно-Российский государственный политехнический университет (НПИ) имени М.И. Платова, г. Новочеркасск, Россия., 2024. – 9 с.

© М. В. Пилипич, А. В. Шабурова, 2026