

УДК 614.849

***ТЕХНОЛОГИИ ПРОТИВОПОЖАРНОЙ ЗАЩИТЫ ДАТА-ЦЕНТРОВ:
ГАЗОВОЕ ТУШЕНИЕ И СИСТЕМЫ РАННЕГО ОБНАРУЖЕНИЯ ДЫМА***

Аксенов С.Г.

*д-р э.н., профессор,
ФГБОУ ВО Уфимский университет науки и технологий,
РФ, г. Уфа*

Садыков М.И.

*студент,
ФГБОУ ВО Уфимский университет науки и технологий,
РФ, г. Уфа*

Аннотация:

В статье рассматриваются принципы работы систем раннего обнаружения пожара, включая аспирационные технологии и интеллектуальные методы анализа, а также механизмы газового пожаротушения на основе экологически безопасных агентов. Особое внимание уделяется интеграции этих систем в общую архитектуру дата-центра, вопросам герметизации, профилактики и роли человеческого фактора. На примере недавнего инцидента в южнокорейском дата-центре NIRS демонстрируется критическая важность многоуровневой стратегии пожарной безопасности, способной не только локализовать возгорание, но и предотвратить его задолго до появления пламени.

Ключевые слова: дата-центр, пожарная безопасность, газовое пожаротушение, раннее обнаружение пожара.

***DATA CENTER FIRE PROTECTION TECHNOLOGIES: GASEOUS FIRE
EXTINGUISHING AND EARLY SMOKE DETECTION SYSTEMS***

Aksyonov S.G.

*Doctor of Economics, Professor,
Ufa University of Science and Technology,
Ufa, Russian Federation*

Sadykov M.I.

Student,

Ufa University of Science and Technology,

Ufa, Russian Federation

Annotation:

The article discusses the principles of early fire detection systems, including aspiration technologies and intelligent analysis methods, as well as gas fire extinguishing mechanisms based on environmentally friendly agents. Special attention is paid to the integration of these systems into the overall architecture of the data center, issues of sealing, prevention and the role of the human factor. The recent incident at the South Korean NIRS data center demonstrates the critical importance of a multi-level fire safety strategy that can not only contain a fire, but also prevent it long before the flame appears.

Keywords: data center, fire safety, gas fire extinguishing, early detection of fire.

26 сентября 2025 года в государственном дата-центре National Information Resources Service (NIRS) в городе Тэджон (Южная Корея) вспыхнул пожар. За несколько часов огонь уничтожил серверы облачного хранилища, где чиновникам выделялось по 30 ГБ для хранения различных документов, которые запрещено было хранить на офисных компьютерах. Этим сервисом пользовалось 17 % всех федеральных чиновников в Корее — около 125 тысяч человек. Но не только: в том же дата-центре размещались данные ещё 163 онлайн-сервисов южнокорейского правительства, включая системы здравоохранения, социального обеспечения и электронного документооборота. Последствия катастрофы вышли далеко за рамки технического сбоя: произошёл масштабный коллапс государственных услуг, были утеряны не подлежащие восстановлению данные, а доверие граждан к цифровой инфраструктуре государства серьёзно пошатнулось. Этот инцидент — не единичный случай. По всему миру дата-центры становятся всё более критичной частью национальной и корпоративной инфраструктуры. Любое нарушение их функционирования, особенно вызванное пожаром, может повлечь за собой экономические, социальные и даже политические последствия. В отличие от традиционных зданий, серверные помещения требуют особых подходов к противопожарной защите: вода, пена или порошок

могут нанести не меньший ущерб, чем сам огонь. Поэтому современные дата-центры всё чаще полагаются на газовое пожаротушение и системы раннего обнаружения, способные предотвратить катастрофу на стадии возникновения возгорания [1,2].

Для понимания необходимости специализированных систем защиты важно осознать специфику пожарной опасности в дата-центрах. Основные источники риска связаны с высокой плотностью оборудования: серверные стойки, коммутационные шкафы и системы охлаждения создают плотную среду с множеством горючих материалов — пластик, изоляция кабелей, печатные платы. Серверы работают круглосуточно, что приводит к постоянному тепловыделению и повышенному риску перегрева. При этом доступ к оборудованию часто ограничен, а стоимость простоев исчисляется миллионами в час. В таких условиях даже небольшое количество воды или химического порошка может вывести из строя дорогостоящее оборудование и привести к безвозвратной потере данных. Пожар в дата-центре развивается стремительно: из-за конвекции и воздушных потоков от систем охлаждения пламя может распространиться по всему залу за считанные минуты. Поэтому ключевым становится время реакции — чем раньше обнаружен очаг возгорания, тем выше шансы на локализацию без масштабных последствий [3].

Системы раннего обнаружения пожара, представляют собой первый и самый важный рубеж обороны. В отличие от традиционных дымовых извещателей, такие системы способны фиксировать частицы дыма на стадии пиролиза — то есть до появления открытого пламени. Принцип её работы заключается в том, что через сеть трубок воздух постоянно отбирается из контролируемой зоны и направляется в лазерную камеру, где анализируется концентрация дымовых частиц. При превышении пороговых значений система выдаёт предупреждение на нескольких уровнях: от простого «Alert» до подтверждённого «Fire 2». VESDA способна обнаружить дым за 30–60 минут до возникновения открытого пламени, что даёт достаточно времени для диагностики и принятия мер без активации системы пожаротушения. Помимо аспирационных систем, всё большее распространение получают термовизионные камеры, газоанализаторы и даже ИИ-аналитика, использующая машинное обучение для выявления аномалий в работе оборудования. Комбинированный подход — использование нескольких типов

датчиков с централизованным управлением — обеспечивает максимальную надёжность и минимизирует ложные срабатывания [4].

Особое внимание при проектировании систем раннего обнаружения уделяется расположению точек забора воздуха. В крупных дата-центрах с высокой плотностью размещения оборудования (high-density racks) недостаточно просто установить датчики под потолком — дым может задерживаться в горячих коридорах между стойками или быть быстро унесён системами вентиляции. Поэтому современные решения предусматривают многоуровневый забор: на уровне пола (для обнаружения возгорания в кабельных каналах), на уровне серверных стоек и под потолком. Некоторые передовые системы даже интегрируются непосредственно в серверные шасси, отслеживая температуру и состав воздуха внутри корпуса. Такой подход позволяет локализовать источник угрозы с точностью до конкретного сервера или блока питания, что критически важно для предотвращения каскадных отказов [4].

Когда раннее обнаружение не спасает, в дело вступает система пожаротушения. В дата-центрах применяются чистые газовые агенты, не оставляющие остатков и не повреждающие электронику. Идеальный агент должен быть электрически непроводящим, не оставлять осадка или коррозии, быстро подавлять пламя, быть безопасным для людей при кратковременном пребывании в зоне и не разрушать озоновый слой. Среди наиболее распространённых решений — FM-200 (HFC-227ea), который действует за счёт прерывания цепной реакции горения и обеспечивает тушение менее чем за 10 секунд. Однако у него высокий потенциал глобального потепления, что приводит к постепенному отказу от его использования в Европе. Альтернативой служит Novec 1230 — экологически безопасный агент с почти нулевым GWP, который испаряется без следа, но требует больших объёмов и стоит дороже. Также применяются инертные газы, такие как Argonite или Inergen, снижающие концентрацию кислорода до уровня, при котором горение невозможно. Они полностью нейтральны с экологической точки зрения, но требуют герметичности помещения и занимают много места из-за больших баллонов. Углекислый газ, хоть и дешёв и эффективен, крайне опасен для людей и требует полной эвакуации перед срабатыванием. Выбор агента зависит от размера помещения, требований к экологии, бюджета и наличия персонала в зоне [5,6].

Современная газовая система — это не просто баллоны с клапанами. Это сложный, интеллектуальный комплекс, интегрированный в общую архитектуру управления дата-центром. Центральный контроллер постоянно получает данные от датчиков дыма, температуры, давления и герметичности. При переходе на уровень «Action» система может автоматически отключить питание в зоне риска, закрыть воздушные заслонки вентиляции, активировать аварийное освещение и отправить оповещение дежурному инженеру. Перед выпуском газа включается звуковая и световая сигнализация с задержкой от 10 до 60 секунд — этого достаточно для эвакуации персонала, но недостаточно для распространения огня. В крупных дата-центрах зоны тушения часто совпадают с так называемыми «горячими коридорами» — это позволяет минимизировать объём защищаемого пространства и снизить количество необходимого агента. Такой подход не только экономит средства, но и повышает скорость срабатывания.

Особую роль играет герметизация помещения. Газовое пожаротушение эффективно только при поддержании концентрации агента в течение определённого времени — обычно 10 минут. Если в помещении есть щели, открытые вентиляционные каналы или негерметичные двери, агент быстро выветрится, и огонь вспыхнет вновь. Поэтому при проектировании дата-центров заранее предусматриваются автоматические заслонки в системах вентиляции, герметичные двери с магнитными замками и даже уплотнения в кабельных вводах. Некоторые операторы проводят регулярные «тесты на утечку» с использованием дымогенераторов или гелия, чтобы убедиться в достаточной герметичности защищаемой зоны [6].

Важно понимать, что газовое пожаротушение — это не панацея, а часть многоуровневой стратегии безопасности. Оно должно работать в тесной связке с системами электропитания, охлаждения и мониторинга. Например, современные ИБП (источники бесперебойного питания) и системы резервного электроснабжения должны быть совместимы с газовыми агентами — некоторые компоненты могут выделять токсичные вещества при контакте с определёнными химическими составами. Аналогично, системы охлаждения должны автоматически отключаться при срабатывании пожаротушения, чтобы не рассеивать агент. Всё это требует тщательной координации на этапе проектирования и регулярного тестирования в эксплуатации.

Опыт крупных провайдеров облачных услуг показывает, что лучшая защита — это та, которая никогда не срабатывает. Именно поэтому всё больше

внимания уделяется профилактике. Это включает не только технические меры, но и организационные: регулярный аудит оборудования, замена устаревших компонентов, контроль за кабельной инфраструктурой, обучение персонала действиям в чрезвычайных ситуациях. Многие дата-центры внедряют программы предиктивного обслуживания, где данные с датчиков температуры, вибрации и энергопотребления анализируются в реальном времени для выявления «слабых звеньев» до того, как они превратятся в источник возгорания. В сочетании с системами раннего обнаружения это создаёт своего рода «иммунную систему» для дата-центра — способную не только реагировать на угрозы, но и предотвращать их.

Стоит также упомянуть о роли человеческого фактора. Несмотря на всю автоматизацию, именно персонал часто становится первым, кто замечает аномалии: запах гари, нехарактерный шум, мигающий индикатор. Поэтому культура безопасности — не просто формальность, а реальный элемент защиты. В лучших дата-центрах проводятся регулярные учения, включая симуляции пожаров с участием реальных систем оповещения и эвакуации. Это позволяет не только отработать действия, но и выявить слабые места в логике работы автоматики.

Технологии продолжают развиваться. Уже сегодня появляются гибридные системы, сочетающие газовое тушение с локальным водяным охлаждением на уровне отдельных стоек — в случае перегрева подаётся тонкий туман, который снижает температуру без ущерба для электроники. Другое перспективное направление — использование наночастиц в составе газовых агентов для повышения эффективности тушения при меньших концентрациях. Искусственный интеллект позволяет не просто обнаруживать дым, а предсказывать вероятность возгорания на основе исторических данных, погодных условий, нагрузки на сеть и даже графика технического обслуживания. В будущем дата-центры могут стать полностью автономными в плане пожарной безопасности — способными не только гасить огонь, но и «лечить» себя до того, как болезнь проявит себя.

Таким образом, пожар в дата-центре NIRS в Тэджоне стал жёстким напоминанием: цифровая инфраструктура так же уязвима, как и любая физическая. Однако, в отличие от заводов или складов, дата-центры не могут позволить себе «традиционные» методы борьбы с огнём. Их защита требует интеллектуальных, многоуровневых решений, где раннее обнаружение и газовое пожаротушение играют ключевую роль. Инвестиции в такие системы

— это не просто соблюдение норм, а стратегическая необходимость. Потеря данных или простои в работе критичных сервисов сегодня обходятся дороже, чем сама защита. Современные технологии позволяют не только минимизировать ущерб, но и предотвратить пожар до его возникновения. В эпоху, когда данные — это новая нефть, их защита от огня должна быть такой же надёжной, как и защита от кибератак. Будущее дата-центров — за интеллектуальной пожарной безопасностью, иисенсоры и экологичные газовые агенты работают в едином симбиозе, обеспечивая бесперебойную и безопасную работу цифрового мира.

Библиографический список

1. Аксенов С.Г., Сулейманова А.И., Харисова З.И. Об особенностях применения современных технических возможностей при расследовании пожаров // Государственная служба и кадры. 2022. № 2. С. 231-234.
2. Аксенов С.Г., Курочкина А.С., Губайдуллина И.Н. Анализ и оценка последствий чрезвычайных ситуаций, связанных с пожарами на промышленных предприятиях // Грузовик. – 2022, №9. - С. 41-43.
3. Савин М.В., Здор В.Л. Современные системы раннего обнаружения пожара // Пожаровзрывобезопасность. 2003. №6. – С. 70-73.
4. Кицак А. И., Лущик А. П., Есипович Д. Л., Кавальчук И. В. Повышение эффективности работы современных точечных оптических дымовых извещателей // CNBOR-PIB. 2014. №. 7. – С. 125-130.
5. Иванов Ю.С., Лущик А.П., Кицак А.И., Есипович Д.Л. Применение лазерных и оптоволоконных технологий для повышения эффективности работы современных оптических дымовых пожарных извещателей // Safety & Fire Technology 2018. №. 1. – С. 86-92.
6. Муцинский, В.А. Совершенствование технических параметров пожарных извещателей // Пожарная безопасность. - 2015. -№ 3. - С. 123-126.

Оригинальность 76%