З. Н. Афсахов, А. А. Оленников
Тюменский государственный университет, г. Тюмень
УДК 004.94:654.924.5

СТЕНД ДЛЯ ИМИТАЦИИ ШТАТНОЙ И АВАРИЙНОЙ РАБОТЫ СИСТЕМЫ ПОЖАРНОЙ СИГНАЛИЗАЦИИ ПРИ ВМЕШАТЕЛЬСТВЕ ЗЛОУМЫШЛЕННИКА

Аннотация. Данная статья описывает разработку стенда, позволяющего имитировать различные сценарии работы системы пожарной сигнализации при вмешательстве злоумышленника. Исследование включает разработку, тестирование и анализа стенда, также проектирование, выбор оборудования, создание моделей для имитации атак, тестирование сценариев, анализ результатов и выявление уязвимостей с последующей разработкой рекомендаций по повышение эффективности защиты объектов.

Ключевые слова: система пожарной сигнализации, проектирование, сетевая атака, монтаж, эксплуатация, злоумышленник, имитация, стенд, классификация, безопасность.

Введение. В современном мире безопасность объектов является одним из приоритетных вопросов, поскольку технологии продолжают внедрятся в любой отрасли экономики. В связи с этим возникает тесная связь с проблемой обеспечения пожарной безопасности, так как это неизбежно влечет за собой увеличение степени риска возникновения пожара [1]. Системы пожарной сигнализации играют важную роль в обеспечении безопасности, однако возможность вмешательства злоумышленников требует дополнительных мер защиты [2].

Системы пожарной сигнализации — это совокупность взаимодействующих технических средств, предназначены для обнаружения пожара, формирования, сбора, обработки, регистрации и выдачи в заданном виде сигналов о пожаре, режимах работы системы, другой информации и инициирующих сигналов на управление техническими средствами противопожарной защиты, технологическим, электротехническим и другим оборудованием. Системы пожарной сигнализации являются одним из наиболее эффективных средств защиты людей и сохранения материальных ценностей от пожара [3].

Данная тема в настоящее время требует особого внимания, поскольку безопасность человеческих жизней и имущества зависит от эффективности систем пожарной сигнализации. Они способны своевременно обнаружить возгорание и предупредить людей о возможной опасности [4]. Однако, в условиях постоянного развития информационных технологий, растет необходимость в более сложных и реалистичных системах пожарной сигнализации, которые могут обеспечить безопасность в зданиях различного назначения.

В современных условиях с ростом числа кибератак, системы пожарной сигнализации становятся уязвимыми для нежелательного вмешательства [5]. Чаще всего эти сети не являются отдельно выделенными, а скорее интегрированные с другими инженерными сетями и ЛВС организации. В итоге все это превращается в одну сложную инфраструктуру, которая увеличивает возможности для злоумышленников на предмет проникновения в эту сеть. Атакующие могут намеренно искажать данные, нарушать работу системы или вводить в заблуждение персонал, что может привести к серьезным последствиям [6]. В связи с этим на кафедре Информационной безопасности выделено отдельное научное направление посвященное защите информации в слаботочных сетях.

Проблема исследования. С учетом роста информационных угроз и интеграции сетей пожарной сигнализации с другими инженерными сетями, делает эти сети далеко небезопасными. Очень большая проблема состоит в том, что эти сети очень уязвимы и требуется их тотальная защита, а зачастую даже операторы иногда не понимают в каком состоянии находятся данные сети. Злоумышленники могут намеренно искажать данные или нарушать работу системы, что представляет угрозу для безопасности объектов [7].

Таким образом, целью данного исследования является разработка стенда, который позволит имитировать различные ситуации, связанные с вмешательством злоумышленников в работу системы пожарной сигнализации. Задачи исследования включают в себя изучение технологий работы систем пожарной сигнализации, их классификацию, разработать проектно-техническую документацию, разработать модуль генерации атак и создание специального стенда для проведения экспериментов.

Материалы и методы. Для исследования были выбраны три основных типа систем пожарных сигнализаций: адресный, неадресный и адресно-аналоговый. Решение о взятии в работу третьей топологии сети — комбинированной сети, включающей адресный и неадресный типы систем пожарных сигнализаций, было принято совместно с руководителем с целью придания универсальности данному стенду [8].

В рамках исследования рассмотрены три схемы сопряжения всех устройств в зависимости от методики выявления очага возгорания и подхода к трансляции данных для оповещения [9]:

1. Неадресная система: основана на лучевой системе, где контроль пульта осуществляется через сигнализационные кабели. Система имеет низкую стоимость и простоту монтажа, но недостаточно надежна и усложняет определение точного места возгорания.

2. Адресная пороговая пожарная сигнализация: взаимодействует с датчиками через контрольную панель, отправляя запросы о функциональной полноценности извещателей. Система обладает преимуществами адресации на уровне блоков и более надежна в сравнении с неадресной системой.

3. Адресно-аналоговая система: работает надежно и стабильно, постоянно анализируя состояние датчиков. Возможность таких систем — настройка датчиков для обнаружения отдельных факторов и уведомления об изменении совокупности наблюдаемых параметров. Система обладает возможностью корректировки работы в зависимости от характеристик объекта и способна с точностью указать очаг возгорания.

Схемы базируются на различных функциональных блоках и могут функционировать как единая система или использоваться в качестве самостоятельных компонентов:

– Прибор Орион обеспечивает достоверную информацию о состоянии объекта. Управляющий модуль в комплекте позволяет обрабатывать сигналы с периферии, а каждый датчик имеет уникальный идентификатор адреса. Орион может работать вместе с извещателями других производителей, для этого предусмотрены модули согласования компонентов, транслирующие сигналы в необходимом формате, совместимом с системой Болид.

– Модуль GSM отправляет сигналы о критических ситуациях и позволяет удаленно управлять цепью устройств. Он осуществляет рассылку сообщений на мобильные телефоны сотрудников и пожарных станций, а также транслирует сигналы на центральную консоль.

Конфигурирование и управление системой осуществляются посредством передачи соответствующих инструкций.

– Система на базе радиоканалов работает с извещателями, использующими беспроводную технологию. Она эффективна в труднодоступных зонах и местах, где прокладка кабелей затруднена. Для помещений сигналы могут передаваться на расстояние до 60 м, а для открытых территорий — до 1,5 км.

Тем самым мы имеем дело с тремя уровнями инфраструктуры. На нижнем уровне располагаются датчики и различные исполнительные механизмы, обеспечивающие непосредственное взаимодействие с окружающей средой и обнаружение возможных пожаров. Этот уровень является основой системы и представляет собой физическую составляющую, на которой строится вся система пожарной сигнализации. Второй уровень — включает контроллеры и пульты управления, которые обрабатывают информацию от датчиков, принимают решения и инициируют соответствующие действия в случае обнаружения пожара или других аварийных ситуаций. На этом уровне происходит обработка данных и координация работы всей системы. Верхний уровень представляет собой системы диспетчеризации, такие как SCADA системы, которые обеспечивают мониторинг и управление системой пожарной сигнализации в целом. Этот уровень обеспечивает операторам возможность мониторинга состояния системы в реальном времени, принятия решений и координации действий в случае возникновения чрезвычайных ситуаций [10]. Каждый из этих уровней играет ключевую роль в обеспечении безопасности объекта и эффективной работы системы пожарной сигнализации.

Разработка проектно-технической документации включает в себя комплекс мероприятий, начиная с определения объекта установки оборудования и его конфигурации, а также учета особенностей окружающей среды [3]. После этого проводится детальная планировка оборудования, которая учитывает его функциональность и оптимальную расстановку для обеспечения максимально эффективной работы системы в целом. После этого формируется структурная электросхема, описывающая взаимосвязи и взаимодействия всех элементов в системе. Важным шагом является правильная конфигурация схемы, так как именно от нее зависит надежность и эффективность системы в целом. В процессе разработки технического решения осуществляется выбор наиболее подходящего оборудования с учетом требований безопасности, функциональных особенностей объекта и его функциональности. После этого проводятся необходимые расчеты, чтобы подобрать необходимое оборудование и его спецификации, обеспечивая соответствие всем стандартам и требованиям безопасности. Структура систем пожарной сигнализации представлена на рис. 1.

В данной системе реализовано тотальное программирование всех устройств, где каждому блоку присваивается адрес, и работа осуществляется через 485 интерфейсную адресную сеть, объединяющую все блоки. Все блоки соединены технологической сетью, после чего происходит их программирование, назначение адресов и логики работы, включая моменты тревожных и аварийных ситуаций. Настройка портов, сблокировка и снятие от тревог осуществляются через интерфейсы С2000-USB и С2000-Ethernet, предназначенные для программирования и управления сетью [3, 10].

Два телекоммуникационных шкафа играют ключевую роль в системе. В одном из них размещается сервер с SCADA-системой управления инфраструктурой, а в другом — сервер для генерации атак. На втором сервере поднято несколько виртуальных машин с разными операционными системами, есть возможность сопряжения с реальным телекоммуникационным оборудованием. Это позволяет организовывать атаки как из внутренней сети. Атаки из внешней сети осуществляются через выделенный канал провайдера проходящие через настраиваемый межсетевой экран, размещенный при физическом стенде. Модуль генерации атак включает определенные инструменты, которые используются для проведения различных видов атак на оборудование [11]. Рассмотрим алгоритмы некоторых атак и возможные последствия от них.

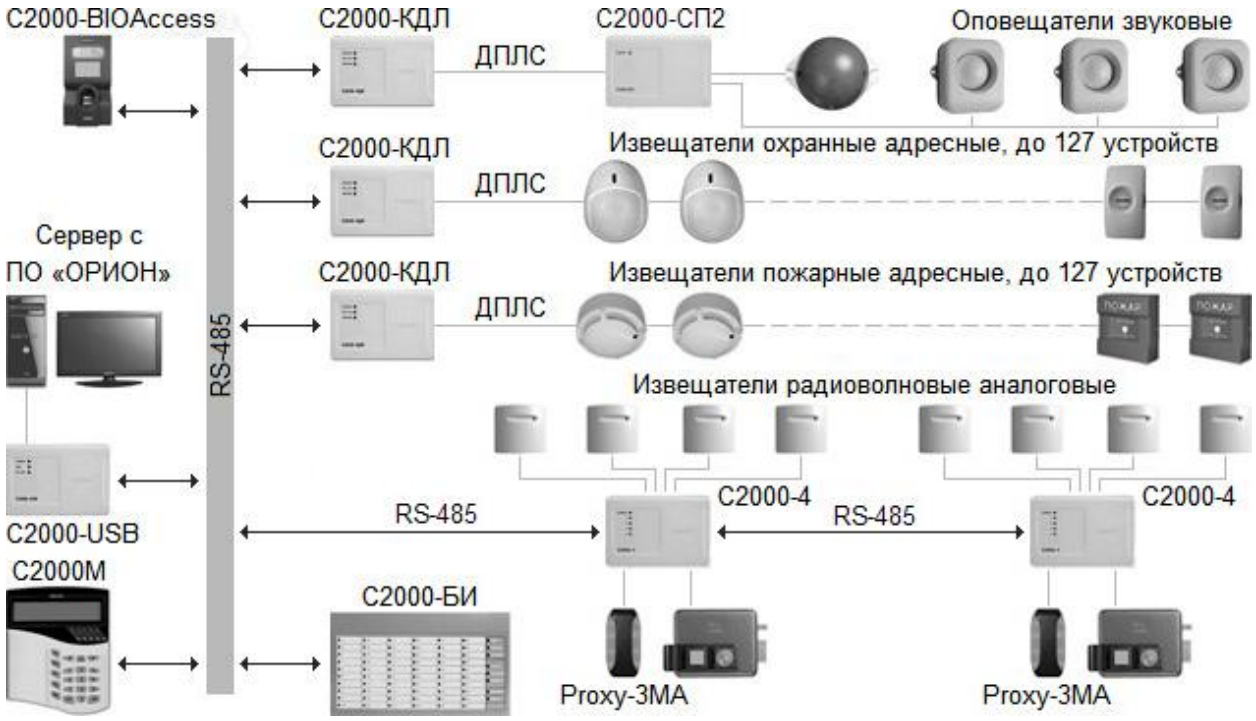

Рис. 1. Структура систем пожарной сигнализации

Атака № 1. В данном сценарии злоумышленник осуществляет атаку через блок С2000-Ethernet на приемно-контрольный прибор С2000-КДЛ, сопряженный с контрольно-пусковым блоком С2000-КПБ и реле УК-ВК. В результате коррекции параметров методом пульсации сигналов возможна активация режима ложной тревоги. Помимо активации ложного режима, активируется система оповещения, отключается общеобменная система вентиляции в здании и активируется противодымная система вентиляции. Также в процессе атаки злоумышленник может полностью блокировать Ethernet порт на блоке С2000-Ethernet, что приведет к разрыву связи с диспетчерской. Алгоритм атаки № 1 приведен на рис. 2.

Другой возможный сценарий предусматривает активацию тревожного режима при реальном пожаре, но при этом не активируются системы противодымной вентиляции. В результате такого воздействия возможны несчастные случаи от удушья посетителей здания продуктами горения.

Атака № 2, алгоритм которой показан на рис. 3, заключается в том, что злоумышленник воздействует через сеть на адресный тепловой датчик и корректирует его значения, изменяя данные о температуре срабатывания. Такая коррекция может привести к ложному срабатыванию системы пожарной сигнализации с активацией сигнала о тревоге, отключению общеобменной системы вентиляции и запуску противодымной системы. В результате такого воздействия активируется не только ложный сигнал о пожаре, но и нарушается воздухообмен в здании.

Рис. 2. Блок-схема «Атака № 1»

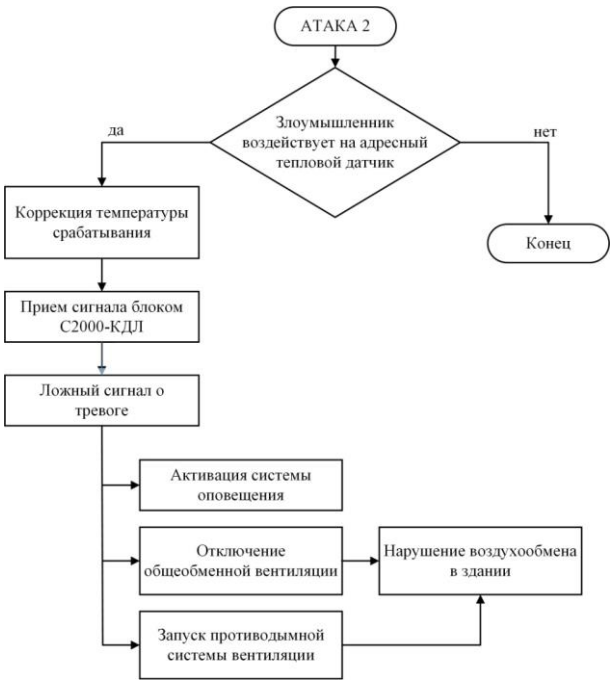

Рис. 3. Блок-схема «Атака № 2»

В результате на созданном стенде были проведены и другие атакующие воздействия, в ходе которых были зафиксированы временные зависимости в штатном режиме работы системы пожарной сигнализации и в аварийных режимах. Результаты представлены в табл. 1.

Атакующее воздействие проводилось с внутренней и внешней сети через основной коммутатор объединяющий сервер диспетчерской, блок С2000-Ethernet и оборудование генерирующее атаки из внутренней сети. В результате наблюдаются временные задержки при обмене данными. Все эти воздействия могут привести к серьезным последствиям, таким как неработающие электромагнитные замки на эвакуационных путях, отсутствие срабатывания дымовой вентиляции и системы автоматического пожаротушения, а также невозможность активации системы эвакуации с использованием звуковых и световых сигналов.

Даже небольшие задержки в 10-20 секунд могут иметь катастрофические последствия, такие как потеря человеческих жизней от удушья или попадание людей в огненные ловушки.

Таблица 1

Результаты предварительных испытаний

Оборудование	*Режим работы, t, с*		
	Штатный режим	*Аварийный*	
		внутреннее воздействие	*внешнее воздействие*
С2000-М	0,2с (RS-485)	0,9-12с (RS-485)	1,5-30с (RS-485)
С2000-БИ	0,2с (RS-485)	0,5-25с (RS-485)	1,4-58с (RS-485)
С2000-КДЛ	0,2с (RS-485)	0,8-53с (RS-485)	0,8-126с (RS-485)
С2000-КПБ	0,3с (RS-485)	6-120 с (RS-485)	9-140 с (RS-485)
Реле УК-ВК	0,2с (аналог.сигн.)	0,3-1,2 с (аналог.сигн.)	1,7-2,5 с (аналог.сигн.)
С2000-2	0,3с (RS-485)	0,8-83с (RS-485)	2,4-135с (RS-485)
С2000-Ethernet	0,4с (RS-485)	0,4-150с (RS-485) полный отказ	2,6-172с (RS-485) полный отказ
Технологический сервер (Scada)	0,8с (RS-485)	2,0-146с (RS-485) полный отказ восстановление 8с цикл отказ/восстановление, при 10 минутной атаке 3/3	2,8-187с (RS-485) полный отказ восстановление 8с цикл отказ/восстановление, при 10 минутной атаке 5/5

Результаты. В результате работы разработана проектно-техническая документация, создан физический испытательный стенд и реализована полноценная SCADA-систему для управления системой пожарной сигнализации. Разработан модуль генерации атак, развернутый на выделенном серверном кластере, проведены первые испытания. Разработанный стенд успешно имитирует различные сценарии вмешательства злоумышленника в работу системы пожарной сигнализации. Проведены некоторые мероприятия по обнаружению и предотвращению вмешательств в подобные системы, что способствует повышению безопасности сетей пожарных сигнализаций защищающих объекты различных назначений.

Заключение. Этот проект представляет собой комплексное решение, способное работать как самостоятельное законченное решение, так и с программно-аппаратной платформой Киберполигон развиваемый на кафедре Информационной безопасности ТюмГУ.

Дальнейшее совершенствование этого проекта позволит увеличить его функциональность и интегрировать его с другими инженерными системами, включающие системы видеонаблюдения, управления доступом, управление лифтовой автоматикой, а также систему автоматического пожаротушения. Это открывает новые перспективы для создания более надежных и интеллектуальных систем безопасности. Появляются возможности для проведения различных экспериментов и апробации систем разрабатываемых под конкретный объект. Эти системы могут быть реализованы на объектах разной сложности, таких как торговые центры, здания культурно-зрелищных учреждений и театры. Все это дает стенду еще больше возможностей для проведения исследований и испытаний, а также для обучения и подготовки специалистов в области безопасности зданий.

СПИСОК ЛИТЕРАТУРЫ

1. World Fire Statistics [Электронный ресурс]. — URL: https://www.ctif.org/world-fire-statistics (дата обращения: 15.03.2024).
2. Федеральный Закон № 69-ФЗ «О пожарной безопасности» от 21.12.1994 г. — URL: http://www.consultant.ru/document/cons_doc_LAW_5438/ (дата обращения: 15.03.2024).
3. ГОСТ Р 59638-2021 Системы пожарной сигнализации. Руководство по проектированию, монтажу, техническому обслуживанию и ремонту. Методы испытаний на работоспособность. Росстандарт от 24 августа 2021 г. // Официальное издание. — М.: Стандартинформ. — 2021. — 24 с.
4. Статистика пожаров и их последствий в Российской Федерации за 2018-2022 гг информ.-аналитич. сб. П 46. — Балашиха: ФГБУ ВНИИПО МЧС России. — 2023. — 80 с.
5. Исследование: более 4 000 устройств АСУ ТП уязвимы для удаленных атак. [Электронный ресурс]. — 2021. — URL: https://www.infowatch.ru/resources/blog/issledovanie-bolee-4-000-ustroystv-asu-tp-uyazvimy-dlya-udalennykh-atak (дата обращения: 16.04.2024).
6. Промышленные компании: векторы атак. [Электронный ресурс]. — 2018. — URL: https://www.ptsecurity.com/ru-ru/research/analytics/ics-attacks-2018/ (дата обращения: 12.04.2024).
7. О взаимодействии систем пожарной сигнализации с инженерными системами [Электронный ресурс]. — 2019. — URL: https://www.aktivsb.ru/statii/o_vzaimodeystvii_sistem_pozharnoy_signalizatsii_s_inzhenernymi_sistemami.html (дата обращения: 14.04.2024).
8. НВП «Болид». — URL: https://bolid.ru/ (дата обращения: 19.04.2024).
9. Методы и технологии обнаружения пожара: монография / В.В. Кутузов, Д.Ю. Минкин, С.Н. Терехин [и др.]. — СПб.: Астерион, Санкт-Петербургский университет ГПС МЧС России, 2015. — 220 с. ISBN 978-5-906152-08-4 — Текст: непосредственный.
10. Цифровые технологии и проблемы информационной безопасности / под ред. Е.В. Стельмашонок, И.Н. Васильевой. — СПб.: Изд-во СПбГЭУ, 2021. — 163 с. ISBN 978-5-7310-5243-6.
11. Назначение и задачи SCADA-систем [Электронный ресурс]. — 2020. — URL: https://www.tadviser.ru/index.php/Статья:SCADA_назначение_систем(дата обращения: 16.04.2024).