УДК 621.313

ОБЗОР И АНАЛИЗ МИРОВЫХ ТЕНДЕНЦИЙ ПОСТРОЕНИЯ СИСТЕМ ЗАЩИТЫ МЕСТ ПРОКЛАДКИ КАБЕЛЕЙ СВЯЗИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Е.А. МАСЕЙЧИК, А.А.ПИЛЮШКО

Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь

Поступила в редакцию 02 апреля 2026

Аннотация. Статья посвящена анализу мировых тенденций построения систем защиты мест прокладки кабелей связи от несанкционированного доступа с учетом современных вызовов, касающихся безопасности телекоммуникационной инфраструктуры Республики Беларусь. Актуальность данной тематики обусловлена ростом уязвимости линейно-кабельных сооружений к физическим воздействиям и несанкционированному доступу, способным нарушить функционирование объектов критической инфраструктуры.

Рассмотрены шесть направлений развития систем защиты: инженерные барьерные средства, видеонаблюдение, вибрационные и акустические датчики, распределенные волоконно-оптические системы, интеграция с IoT и применение методов искусственного интеллекта.

Установлено, что большинство решений ориентированы на фиксацию уже произошедшего воздействия, что ограничивает возможности раннего предупреждения инцидентов. Наиболее перспективным направлением признано развитие распределенных волоконно-оптических систем мониторинга с интеллектуальной обработкой сигналов. Обоснована целесообразность перехода к интегрированным системам мониторинга протяженных объектов связи с элементами прогнозной аналитики.

Ключевые слова: методы и системы защиты мест прокладки кабелей связи от несанкционированного доступа, волоконно-оптические распределительные системы мониторинга.

Введение

Анализ современной научно-технической литературы [1–14], посвященной анализу мировых тенденций построения систем защиты (охраны, оповещения и т. п.) как отдельных (компактных) объектов, так и обширных территорий, в том числе мест прокладки кабелей связи (линейно-кабельных сооружений) от природно-техногенных причин и несанкционированного доступа показывает, что в условиях резко изменяющейся климатической, а также внутри- и внешнеполитической обстановки в Республике Беларусь в последние 5-6 лет актуальность разработки и внедрения таких систем многократно возросла.

При этом существующие решения, как правило, ориентированы на фиксацию уже совершенного воздействия, что снижает эффективность предотвращения инцидентов. В этих условиях особое значение приобретает разработка и внедрение систем раннего обнаружения вторжений на протяженных объектах связи. Цель статьи – провести классификацию и сравнительный анализ современных направлений развития методов и систем защиты кабельной инфраструктуры и определить наиболее перспективное решение для дальнейшего совершенствования.

Обзор и анализ мировых тенденций построения систем защиты мест прокладки кабелей связи

Современные подходы к защите мест прокладки кабелей связи формируются под влиянием требований обеспечения устойчивости телекоммуникационной инфраструктуры, а также необходимости минимизации рисков физического воздействия и несанкционированного

доступа. Международная практика демонстрирует переход от изолированных инженерных решений к многоуровневым системам мониторинга и реагирования, интегрирующим физические, технические и информационные средства защиты [9, 10]. На основе анализа научных публикаций и отраслевых отчетов выделяются шесть ключевых технологий развития систем защиты протяженных объектов связи.

Физическая инженерная защита (барьерные и пассивные средства)

Физическая инженерная защита представляет собой традиционный и наиболее распространенный способ обеспечения сохранности линейно-кабельных сооружений. Она включает прокладку кабелей в кабельной канализации, использование бронированных оболочек, металлических и железобетонных коробов, запираемых люков, антивандальных шкафов, а также создание охранных зон. Данные меры направлены на ограничение прямого физического доступа к кабелю и снижение вероятности его механического повреждения.

Практика проектирования систем охраны периметра показывает, что инженерные барьерные средства обладают высокой надежностью при условии соблюдения нормативных требований и регулярного технического обслуживания [7]. Их достоинствами являются автономность функционирования, отсутствие зависимости от электропитания и сетевой инфраструктуры, а также сравнительно низкие эксплуатационные расходы. Такие решения устойчивы к отказам и не требуют сложной калибровки.

Вместе с тем физическая защита не обеспечивает интеллектуального контроля состояния объекта. Она не позволяет выявить подготовительные действия нарушителя до момента фактического вскрытия или повреждения конструкции. Анализ принципов построения систем охраны периметра показывает, что барьерные средства носят пассивный характер и выполняют функцию сдерживания, а не раннего обнаружения угрозы [6]. При отсутствии средств мониторинга фиксируется лишь факт нарушения целостности защитного элемента, что затрудняет оперативное реагирование.

Дополнительным ограничением является невозможность масштабного контроля протяженных участков без значительных капитальных затрат. В условиях увеличения длин трасс и пространственной распределенности их инфраструктуры эффективность исключительно инженерных решений снижается. Таким образом, физическая защита остается базовым элементом такой системы безопасности, но не обеспечивает раннего детектирования вторжения.

Системы видеонаблюдения и периметрального контроля

Системы видеонаблюдения (CCTV), тепловизионные комплексы и интеллектуальная видеоаналитика широко применяются для охраны узлов связи, распределительных шкафов, кабельных колодцев и иных точек повышенного риска. Они позволяют осуществлять визуальный контроль территории, фиксировать попытки проникновения и проводить постфактум анализ событий.

Оценка эффективности периметральных систем демонстрирует, что визуальная верификация существенно повышает достоверность выявления инцидентов и снижает вероятность ложных тревог [8]. Интеграция с аналитическими алгоритмами обеспечивает автоматическое распознавание движения, пересечения заданных зон и подозрительных действий. Зарубежный опыт применения систем тревожного оповещения подтверждает рост их роли в обеспечении территориальной безопасности объектов критической инфраструктуры [4].

Однако видеонаблюдение имеет ряд существенных ограничений. Его эффективность зависит от погодных условий, освещенности и отсутствия физических препятствий. Наличие «слепых зон» снижает полноту контроля, особенно на протяженных трассах вне населенных пунктов. Кроме того, большинство видеоаналитических систем фиксирует уже происходящее событие, не обеспечивая прогнозирования или раннего предупреждения о потенциальной угрозе [6].

Для протяженных линейных объектов организация сплошного видеоконтроля экономически и технически затруднительна. Это ограничивает применение данной технологии преимущественно узловыми участками инфраструктуры.

Датчики вибрации и акустического контроля

Системы на основе вибрационных и акустических датчиков предназначены для регистрации механических воздействий на ограждения, грунт или конструкции, вблизи которых проложен кабель. Принципы их работы основаны на фиксации колебаний, возникающих при попытке подкопа, вскрытия люков или разрушения защитных элементов.

Тактико-технический анализ физических принципов обнаружения нарушителя показывает, что данные средства способны выявлять ранние стадии вторжения при корректной настройке чувствительности датчиков [6]. Применение распределенных сенсорных модулей позволяет организовать контроль протяженных участков с формированием сигнала тревоги при превышении пороговых значений [3].

К преимуществам систем, построенных по данной технологии, относятся их относительно высокая чувствительность, возможность автономной работы и адаптация к различным типам ограждений и грунтов. Вместе с тем характерной проблемой является значительное количество ложных срабатываний, вызванных воздействием ветра, транспорта, животных или климатических факторов. Для снижения числа ошибочных тревог требуется сложная фильтрация сигналов и настройка параметров, что повышает требования к квалификации обслуживающего персонала [5].

Таким образом, вибрационные и акустические датчики обеспечивают более раннее обнаружение по сравнению с пассивными средствами, однако их эффективность существенно зависит от корректности алгоритмов обработки данных и условий эксплуатации.

Волоконно-оптические распределенные системы мониторинга

Одним из наиболее динамично развивающихся направлений является использование распределенных волоконно-оптических систем мониторинга (DAS, DTS, DSS), в которых само оптическое волокно выполняет функцию чувствительного элемента. Принцип работы таких систем основан на анализе изменений параметров отраженного сигнала при механическом, температурном или акустическом воздействии на кабель.

Распределенные системы акустического мониторинга обеспечивают непрерывный контроль протяженных участков с высокой точностью локализации события [11]. Технологии DAS позволяют фиксировать вибрации вдоль всей длины кабеля с определением координаты воздействия, что особенно актуально для магистральных линий связи. Международные рекомендации по защите подводных кабелей подчеркивают необходимость применения мониторинговых решений для предупреждения преднамеренных и непреднамеренных повреждений [12].

К достоинствам данной тенденции относятся:

– непрерывный контроль на десятках километров без установки множества отдельных датчиков;

– высокая чувствительность к различным типам воздействий;

– возможность интеграции с аналитическими системами обработки сигналов.

Основными ограничениями являются высокая стоимость внедрения, сложность калибровки и необходимость применения специализированных алгоритмов интерпретации данных. Дополнительно отмечается потребность в защите информационных потоков системы мониторинга в соответствии с требованиями безопасности телекоммуникационной инфраструктуры [9, 14].

Несмотря на указанные сложности, распределенные волоконно-оптические системы демонстрируют потенциал обеспечения раннего выявления механических воздействий еще до фактического повреждения кабеля.

Интеграция с IoT и системами кибербезопасности

Современные системы защиты все чаще строятся по принципу интеграции датчиков различного типа в единую информационную платформу с передачей данных в централизованные центры мониторинга. Использование IoT-технологий позволяет организовать удаленный контроль состояния объектов, формировать события в реальном времени и осуществлять корреляцию сигналов от различных источников.

Аналитические материалы в области защиты телекоммуникационной инфраструктуры указывают на необходимость комплексного учета физических и киберугроз при построении систем безопасности [10, 14]. Интеграция с системами управления доступом, видеонаблюдением и распределенными датчиками создает основу для построения многоуровневой архитектуры защиты.

Преимуществами данной тенденции являются масштабируемость, централизованный контроль, автоматизация обработки событий и возможность накопления статистических данных для анализа рисков. Вместе с тем возрастает зависимость от сетевой инфраструктуры и устойчивости каналов передачи данных. Возникают дополнительные киберриски, связанные с возможностью вмешательства в систему мониторинга или подмены данных [9].

Таким образом, интеграция IoT расширяет функциональные возможности систем защиты, но требует соблюдения требований информационной безопасности и резервирования каналов связи.

Использование искусственного интеллекта и машинного обучения для раннего обнаружения

Развитие распределенных сенсорных систем и накопление больших массивов данных о состоянии протяженных объектов обусловили формирование отдельной тенденции – применение методов искусственного интеллекта и машинного обучения для обработки сигналов и раннего выявления угроз. В отличие от традиционных пороговых алгоритмов, интеллектуальные модели способны учитывать совокупность признаков, анализировать временные зависимости и выявлять аномальные паттерны поведения.

В распределенных волоконно-оптических системах мониторинга применение алгоритмов классификации и глубинного обучения позволяет дифференцировать типы воздействий: движение транспорта, шаги человека, работы строительной техники, попытки подкопа или вскрытия защитных конструкций [11]. Это снижает уровень ложных тревог и повышает точность идентификации события. Аналогичные подходы реализуются при обработке сигналов вибрационных датчиков и систем видеонаблюдения, где используются алгоритмы распознавания образов и поведенческого анализа.

Интеллектуальная обработка данных позволяет перейти от фиксации факта воздействия к прогнозированию вероятности развития инцидента. При накоплении статистики возможна реализация предиктивной аналитики, основанной на выявлении повторяющихся сценариев и корреляции сигналов от различных подсистем. В контексте обеспечения безопасности телекоммуникационной инфраструктуры такие решения соответствуют международным требованиям комплексного подхода к защите критических сервисов [9, 10].

К достоинствам данной тенденции относятся:

– снижение количества ложных срабатываний за счет адаптивной фильтрации сигналов;

– повышение точности локализации и классификации событий;

– возможность раннего выявления аномалий, предшествующих фактическому повреждению кабеля;

– интеграция в централизованные системы мониторинга.

Основными ограничениями являются необходимость формирования обучающих выборок, зависимость качества работы алгоритмов от полноты и репрезентативности данных, а также потребность в вычислительных ресурсах и квалифицированном сопровождении. Дополнительным фактором риска выступает уязвимость интеллектуальных систем к кибервоздействиям и попыткам подмены входных данных, что требует соблюдения требований информационной безопасности [14].

Таким образом, использование методов искусственного интеллекта формирует основу для построения систем раннего обнаружения вторжений, однако требует технологической зрелости инфраструктуры и интеграции с распределенными сенсорными платформами.

Заключение

Проведенный анализ шести основных направлений развития систем защиты протяженных объектов связи показывает, что каждое из них решает определенный класс задач, однако их эффективность существенно различается в части обеспечения раннего выявления угроз.

Физическая инженерная защита обеспечивает базовый уровень устойчивости инфраструктуры и снижает вероятность случайного повреждения, но не формирует механизмов оперативного мониторинга [6, 7]. Она носит преимущественно сдерживающий характер и не позволяет фиксировать подготовительные действия нарушителя.

Системы видеонаблюдения и периметрального контроля повышают достоверность выявления инцидентов за счет визуальной верификации, однако остаются зависимыми от внешних условий и не обеспечивают непрерывного контроля протяженных трасс [4, 8]. Их реактивный характер проявляется в фиксации уже происходящего события, без возможности анализа скрытых воздействий на грунт или подземные коммуникации.

Вибрационные и акустические датчики обеспечивают более раннее реагирование на механические воздействия по сравнению с пассивными средствами. Тем не менее высокая чувствительность к внешним факторам приводит к значительному количеству ложных тревог, что требует применения сложных алгоритмов фильтрации [5, 6]. Без интеллектуальной обработки их эффективность ограничена.

Распределенные волоконно-оптические системы мониторинга обладают принципиально иными характеристиками. Они обеспечивают непрерывный контроль всей длины кабеля, точную локализацию воздействия и возможность интеграции с аналитическими модулями [11]. Международные рекомендации по защите кабельной инфраструктуры подчеркивают необходимость применения мониторинговых решений для предупреждения инцидентов, а не только их фиксации [12]. При этом высокая стоимость и сложность внедрения ограничивают масштаб их применения без дополнительного экономического обоснования.

Интеграция систем защиты с IoT-платформами и средствами кибербезопасности позволяет объединить разнородные источники данных в единую архитектуру мониторинга [9, 10, 14]. Однако при отсутствии интеллектуальной аналитики такая интеграция не обеспечивает качественного перехода к раннему детектированию, а лишь повышает управляемость существующих средств.

Использование искусственного интеллекта и машинного обучения формирует условия для перехода от реактивной к проактивной модели защиты. Интеллектуальная корреляция сигналов различных датчиков позволяет выявлять аномалии до момента физического повреждения кабеля. В совокупности с распределенными сенсорными технологиями данный подход обеспечивает наибольший потенциал раннего обнаружения вторжения.

Обобщенный сравнительный анализ показывает, что большинство традиционных систем ориентированы на фиксацию уже произошедшего воздействия. Их общий недостаток заключается в отсутствии гарантированного механизма раннего предупреждения о готовящемся или начавшемся вторжении на территорию объекта либо на конкретный участок периметра. Наиболее перспективным направлением является интеграция распределенных волоконно-оптических систем мониторинга с интеллектуальной аналитикой, обеспечивающая непрерывный контроль, точную локализацию и снижение количества ложных тревог при соблюдении требований информационной безопасности [9, 11]. Поэтому основные усилия целесообразно сосредоточить на разработке именно таких систем с применением методов искусственного интеллекта и машинного обучения. Данный подход позволит обеспечить непрерывный контроль протяженных участков, точную локализацию воздействия и возможность дифференциации типов событий [11].

Интеграция распределенных сенсорных технологий с интеллектуальной аналитикой позволит позволяет реализовать переход от реактивной модели реагирования к проактивной, ориентированной на раннее выявление аномалий и предупреждение инцидентов. Такая архитектура соответствует международным требованиям комплексной защиты телекоммуникационной инфраструктуры и учета физических и киберугроз [9, 10, 14]. Дополнительным преимуществом является возможность централизованного мониторинга и накопления статистических данных для совершенствования алгоритмов обнаружения.

REVIEW AND ANALYSIS OF GLOBAL TRENDS IN BUILDING SYSTEMS TO PROTECT COMMUNICATION CABLE INSTALLATION SITES FROM UNAUTHORIZED ACCESS

E.A. MASEYCHIK, A.A. PILYUSHKO

Abstract. The article is devoted to the analysis of global trends in the construction of systems for protecting communication cable installations from unauthorized access, taking into account modern challenges related to the security of the telecommunications infrastructure of the Republic of Belarus. The relevance of this topic is due to the increasing vulnerability of linear cable structures to physical impacts and unauthorized access that can disrupt the functioning of critical infrastructure facilities.

Six areas of protection systems development are considered: engineering barriers, video surveillance, vibration and acoustic sensors, distributed fiber-optic systems, integration with IoT and the use of artificial intelligence methods.critical infrastructure.

It has been established that most solutions are focused on fixing the impact that has already occurred, which limits the possibilities of early warning of incidents. The development of distributed fiber-optic monitoring systems with intelligent signal processing is recognized as the most promising direction. The expediency of switching to integrated monitoring systems for extended communication facilities with elements of predictive analytics is substantiated.

Keywords: methods and systems for protecting communication cable installation sites from unauthorized access, fiber-optic distribution monitoring systems.

Список литературы

1. Берсенев, В. П. Комплекс охраны периметров «Мурена-КС» как средство защиты объектов / В. П. Берсенев // Охранные системы и технологии. – 2021. – URL: https://cyberleninka.ru/article/n/kompleks-ohrany-perimetrov-murena-ks/pdf

2. Здоровцов, А. Г. Способы применения дистанционно управляемых средств охранной сигнализации для обнаружения проникновений / А. Г. Здоровцов // Безопасность и связь. – 2022. – № 12. – С. 92–96. – URL: https://cyberleninka.ru/article/n/sposoby-primeneniya-distantsionno-upravlyaemyh-sredstv-ohrannoy-signalizatsii-dlya-obnaruzheniya-proniknoveniy-na-ohranyaemye/pdf).

3. Костюк, А. И. Мониторинг перемещения охранных модулей в системе охраны периметра / А. И. Костюк // Автоматизация и безопасность. – 2022. – URL: https://cyberleninka.ru/article/n/monitoring-peremescheniya-ohrannyh-moduley-v-sisteme-ohrany-perimetra

4. Курбанбаев, Д. Ж. Зарубежный опыт современного состояния применения систем тревожного оповещения в обеспечении территориальной безопасности / Д. Ж. Курбанбаев // Информационные технологии и безопасность. – 2023. – URL: https://cyberleninka.ru/article/n/zarubezhnyy-opyt-sovremennogo-sostoyaniya-primeneniya-sistem-trevozhnogo-opovescheniya-v-sfere-obespecheniya-territorialnoy/pdf.

5. Магомедов, Ш. Г. Построение моделей описания рисков охранных действий по защите внешних периметров организаций / Ш. Г. Магомедов // Информационная безопасность и риски. – 2017. – URL: https://cyberleninka.ru/article/n/postroenie-modeley-opisaniya-riskov-ohrannyh-deystviy-po-zaschite-vneshnih-perimetrov-organizatsii

6. Николаев, В. А. Тактико-технический анализ физических принципов обнаружения нарушителя в системах охраны периметра / В. А. Николаев // Системы безопасности. – 2017. – URL: https://cyberleninka.ru/article/n/taktiko-tehnicheskiy-analiz-fizicheskih-printsipov-obnaruzheniya-narushitelya/pdf

7. Селищев, В. А., Чечуга, О. В. Выбор системы охраны периметра / В. А. Селищев, О. В. Чечуга // Известия Тульского государственного университета. Технические науки. – 2010. – URL: https://cyberleninka.ru/article/n/vybor-sistemy-ohrany-perimetra

8. Щербакова, И. В. Анализ эффективности систем охраны периметра объектов / И. В. Щербакова // Информационные технологии безопасности. – 2016. – URL: https://cyberleninka.ru/article/n/analiz-effektivnosti-sistem-ohrany-perimetra-obektov

9. CIP Association. Legal and Regulatory Aspects Relating to the Physical Security of the Telecommunications Infrastructure Used for Critical Communication Services : report. – CIP Association, 2025. – URL: https://www.cip-association.org/legal-and-regulatory-aspects-relating-to-the-physical-security-of-the-telecommunications-infrastructure-used-for-critical-communication-services/

10. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape for 5G Networks : report. – Athens : ENISA, 2023. – URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks.

11. Hartog, A. H. A distributed optical fibre sensor for the detection and classification of disturbances along a fibre link / A. H. Hartog // Journal of Lightwave Technology. – 2020. – Vol. 38 (16), P. 4424–4436. – URL: https://ieeexplore.ieee.org/document/9098927
12. International Cable Protection Committee (ICPC). Recommendations for the Protection of Submarine Cables : report. – London : ICPC, 2024. – URL: https://www.iscpc.org/publications/recommendations
13. Kwon, Y. Distributed Fiber-Optic Sensing Technologies for Structural Health Monitoring / Y. Kwon // Photonics. – 2021. – Vol. 8 (1), P. 15. – URL: https://www.mdpi.com/2304-6732/8/1/15
14. National Institute of Standards and Technology (NIST). Security and Privacy Controls for Information Systems and Organizations (SP 800-53 Rev. 5) : report. – Gaithersburg : NIST, 2020. – URL: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final