Дудин В.Д. Общеканальная система сигнализации объекта информатизации как элемент защиты информационно-телекоммуникационной сети // Международный журнал информационных технологий и энергоэффективности. – 2026. – Т. 11 № 1(63) с.152–156

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056.53

ОБЩЕКАНАЛЬНАЯ СИСТЕМА СИГНАЛИЗАЦИИ ОБЪЕКТА ИНФОРМАТИЗАЦИИ КАК ЭЛЕМЕНТ ЗАЩИТЫ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ

Дудин В.Д.
ФГБОУ ВО «САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М. А. БОНЧ-БРУЕВИЧА», Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: slava_4944@mail.ru

В работе обоснована актуальность развития общеканальных систем сигнализации. Рассмотрены теоретические основы построения систем с общим каналом сигнализации, включающие архитектурные принципы, механизмы функционирования и особенности применения единого защищённого канала передачи сигналов. Представлена типовая модель, описывающая процессы сбора, обработки и доставки сигнальных сообщений. Проанализированы преимущества предлагаемого подхода по сравнению с традиционными. Показана роль общеканальных систем сигнализации как элемента комплексной защиты информационно-телекоммуникационных сетей и приведены направления дальнейшего совершенствования механизмов корреляции и обработки сигнального трафика.

Ключевые слова: информационная безопасность, объект информатизации, система сигнализации, общеканальная архитектура, мониторинг, несанкционированное воздействие, корреляция событий.

CHANNEL-WIDE ALARM SYSTEM FOR AN INFORMATION FACILITY AS AN ELEMENT OF INFORMATION AND TELECOMMUNICATION NETWORK PROTECTION

Dudin V.D.
SAINT PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROF. M.A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: slava_4944@mail.ru

This paper substantiates the relevance of developing common-channel signaling systems. It examines the theoretical foundations of building systems with a common signaling channel, including architectural principles, operational mechanisms, and the specifics of using a single secure signaling channel. A standard model describing the processes of collecting, processing, and delivering signaling messages is presented. The advantages of the proposed approach compared to traditional approaches are analyzed. The role of common-channel signaling systems as an element of comprehensive protection for information and telecommunications networks is demonstrated, and directions for further improvement of signaling traffic correlation and processing mechanisms are outlined.

Keywords: information security, information technology object, alarm system, common-channel architecture, monitoring, unauthorized impact, event correlation.

Введение

Информационно-телекоммуникационные сети являются основой функционирования большинства современных объектов информатизации, включая критически важные. Усложнение сетевой инфраструктуры, распределённый характер вычислительных ресурсов и рост количества взаимодействующих элементов способствуют формированию новых угроз, в

том числе внутренних, направленных на нарушение штатной работы и компрометацию информации.

Для своевременного выявления подобных воздействий необходимы системы, обеспечивающие оперативное получение сведений о событиях безопасности. Применяемые на практике раздельные каналы сигнализации создают избыточность инфраструктуры и приводят к разрыву информационных потоков, что затрудняет анализ событий и замедляет реагирование.

В этих условиях целесообразно применение общеканальной системы сигнализации (далее - ОСС), объединяющей передачу всех типов сигналов в едином защищённом коммуникационном контуре.

Целью работы является определение принципов построения ОСС и анализ её роли в обеспечении защищённости информационно-телекоммуникационных сетей от несанкционированных воздействий.

Понятие и назначение общеканальной системы сигнализации

Общеканальная система сигнализации представляет собой совокупность аппаратных и программных средств, обеспечивающих централизованный приём, обработку и передачу сообщений о событиях безопасности по защищённому каналу связи. [4, с. 30]

Основные функции ОСС включают сбор сведений о состоянии подсистем и компонентов сети, обеспечение своевременной и достоверной доставки сообщений, интеграцию данных различной природы — физических, сетевых и логических, а также автоматизированное оповещение операторов и подсистем реагирования.

ОСС является элементом комплексной системы защиты информации и выполняет задачи мониторинга, первичной аналитики и корреляции событий.

Концепция общего канала.

Общеканальный подход в контексте системы сигнализации предусматривает передачу всех сигналов по единому защищенному каналу, в отличие от традиционных решений, которые, в свою очередь, используют выделенные каналы для каждой из подсистем.

Предложенный подход упрощает инфраструктуру и исключает возможное дублирование информации, что повышает согласованность данных. Подход основан на идее переноса принципов общеканальной сигнализации из области телекоммуникаций на сферу обеспечения безопасности информационно-телекоммуникационных сетей общего назначения. [3, с. 115]

Архитектурные принципы построения ОСС

Предлагаемая архитектура общеканальной системы сигнализации включает в себя следующие положения:

- **единый коммуникационный контур**, передающий все типы сигналов по защищённому каналу;
- **модульное построение**, включающее блоки сбора сообщений, маршрутизации, обработки и визуализации;
- **централизованное управление**, позволяющее выполнять анализ и принятие решений на выделенном сервере сигнализации;

• **криптографическая защита коммуникаций**, предусматривающая защищённые протоколы передачи данных, взаимную аутентификацию и контроль целостности;

• **интеграция с существующими подсистемами** — вышеупомянутая модульность позволяет интегрировать другие средства защиты систем.

Подобная модель построения общеканальной системы сигнализации обеспечивает согласованность данных, повышение надежности защищаемой инфокоммуникационной системы и снижение времени реакции при инцидентах безопасности. ОСС становится центральным элементом инфраструктуры мониторинга, объединяющим разнородные подсистемы в единый защищённый канал обмена. [5, с. 20]

Роль общеканальной сигнализации при несанкционированных воздействиях

При нарушении штатной работы сети возможны угрозы, связанные с перехватом и модификацией управляющих сообщений, подменой сигналов, генерацией ложных уведомлений и блокировкой каналов передачи данных.

Общеканальная система сигнализации должна обеспечивать выявление аномалий в сигнальном трафике, резервирование маршрутов передачи данных, а также автоматическую корреляцию событий на различных уровнях информационно-телекоммуникационной сети, осуществляя защиту от подмены и перехвата сообщений. [4, с. 34] ОСС выступает как механизм раннего обнаружения нарушений, позволяющий свести к минимуму последствия несанкционированных воздействий на инфраструктуру.

Сравнение общеканального подхода с современно используемыми методами организации инфраструктуры сигнализации

Современные ИТ-инфраструктуры, как правило, используют раздельный подход к организации каналов сигнализации, при котором различные подсистемы безопасности функционируют изолированно. [1, с. 92]. Так, системы пожарной и охранной сигнализации, СКУД, IDS/IPS, средства мониторинга технического состояния оборудования и сетевые анализаторы передают данные по собственным каналам и применяют специализированные протоколы обмена. Этот подход исторически сформирован как следствие различий в функциональных требованиях, регламентах и стандартах отраслей.

Однако фрагментированная модель обладает рядом недостатков, особенно в условиях усложнения ИТКС и роста количества источников событий безопасности:

• **Отсутствие единой картины событий** — информация поступает в различные центры мониторинга и обрабатывается разными программными комплексами, что требует ручной корреляции и увеличивает время анализа инцидентов.

• **Разрозненность протоколов и инфраструктуры связи** приводит к избыточности каналов, усложняет сопровождение и повышает вероятность ошибок конфигурации.

• **Возможность обхода систем безопасности** за счёт того, что события на одном уровне (например, физическом) могут не учитываться подсистемами, работающими на логическом или сетевом уровнях.

• **Снижение оперативности реагирования** при одновременном возникновении событий в нескольких подсистемах, что характерно для мультивекторных атак.

Общеканальный подход, реализуемый в ОСС, принципиально отличается от традиционных архитектур.

Во-первых, описанный подход обеспечивает консолидацию всех потоков событий в едином защищённом канале, позволяя синхронно доставлять сообщения от различных подсистем, что упрощает инфраструктуру за счёт отказа от множества потоков сигнальных сообщений.

Во-вторых, такая модель позволяет реализовать более глубокую корреляцию физических, сетевых и логических событий, повышая качество аналитики и точность выявления источников угроз.

В-третьих, сокращается время реакции за счёт исключения промежуточных этапов обработки и передачи данных.

Дополнительным преимуществом является повышение уровня защищённости, поскольку единый коммуникационный канал проще контролировать и защищать, чем разнородный набор распределённых линий связи.

Заключение

Общеканальная система сигнализации выступает ключевым элементом архитектуры защиты информационно-телекоммуникационных сетей. В работе обоснованы принципы построения ОСС, разработана теоретическая модель её функционирования, а также выделены преимущества общеканального подхода по сравнению с традиционными решениями на основе раздельных каналов сигнализации. Перспективными направлениями дальнейших исследований являются создание математических моделей корреляции сигналов и оптимизация параметров передачи данных в распределённых защищённых сетях..

Список литературы

1. Бирих Э.В., Виткова Л.А., Левин М.В., Чмутов М.В. Развитие стандартов и руководств в сфере облачных технологий // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017). Сборник научных статей VI Международной научно-технической и научно-методической конференции. В 4-х томах. Под редакцией С.В. Бачевского. 2017. С. 26. URL: https://www.sut.ru/doci/nauka/6apino/programm2017apino.pdf
2. Ворона В.А. Комплексные (интегрированные) системы обеспечения безопасности / В.А. Ворона В.А., Тихонов В.А. // М:Горячая Линия–Телеком. 2013. С. 5-121. URL: https://www.techbook.ru/book.php?id_book=569
3. Езерская А. Б. Автоматизированная интегрированная система управления комплексной безопасностью научного центра // Научный альманах. 2017. №9-1(35). С. 34-35. URL: https://elib.pnzgu.ru/files/eb/TfB1FuoCi2G5.pdf
4. Махмутова Н.Ф., Бирих Э.В., Сахаров Д.В., Кривец А.С., Дегтярев М.А. Исследование способов повышения безопасности корпоративных сетей // Вестник Дагестанского гос. техн. ун-та. — 2024;51(3): `С. 110–116. URL: https://doi.org/10.21822/2073-6185-2024-51-3-110-116
5. Рыжова В.А. Проектирование и исследование комплексных систем безопасности // С: НИУ ИТМО. 2013. С. 8–149. URL: https://books.ifmo.ru/book/837/proektirovanie_i_issledovanie_kompleksnyh_sistem_bezopasnosti.htm.

References

1. Birikh E.V., Vitkova L.A., Levin M.V., Chmutov M.V. Development of standards and guidelines in the field of cloud technologies // In the collection: Actual problems of infotelecommunications in science and education (APINO 2017). Collection of scientific articles of the VI International scientific-technical and scientific-methodical conference. In 4 volumes. Edited by S.V. Bachevsky. 2017. P. 26. URL: https://www.sut.ru/doci/nauka/6apino/programm2017apino.pdf
2. Vorona V.A. Comprehensive (integrated) security systems / V.A. Vorona V.A., Tikhonov V.A. // M: Goryachaya Liniya-Telecom. 2013. P. 5-121. URL: https://www.techbook.ru/book.php?id_book=569
3. Ezerskaya A. B. Automated integrated management system for complex security of a scientific center // Scientific Almanac. 2017. No. 9-1 (35). P. 34-35. URL: https://elib.pnzgu.ru/files/eb/TfB1FuoCi2G5.pdf
4. Makhmutova N. F., Birikh E. V., Sakharov D. V., Krivets A. S., Degtyarev M. A. Study of ways to improve the security of corporate networks // Bulletin of the Dagestan State Technical University. - 2024; 51 (3): `P. URL: https://doi.org/10.21822/2073-6185-2024-51-3-110-116
5. Ryzhova V.A. Design and Research of Integrated Security Systems // NRU ITMO. 2013. pp. 8–149. URL: https://books.ifmo.ru/book/837/proektirovanie_i_issledovanie_kompleksnyh_sistem_bezopasnosti.htm.