



УДК 811

МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЫ ДАННЫХ В КОРПОРАТИВНЫХ БЕСПРОВОДНЫХ СЕТЯХ

Акыев Гуванч Аганьязович

преподаватель

Джемшидова Огулджерен Максадовна

студентка

Институт телекоммуникаций и информатики Туркменистана

г. Ашхабад, Туркменистан

Аннотация. Методы обеспечения информационной безопасности в корпоративных беспроводных сетях являются критически важным элементом современной ИТ-инфраструктуры, защищающим бизнес-процессы от внешних и внутренних угроз. В условиях массового перехода на концепцию мобильных рабочих мест беспроводной сегмент сети становится наиболее уязвимым вектором для потенциальных кибератак. Эффективная защита требует комплексного подхода, сочетающего в себе передовые технологии шифрования, строгие механизмы идентификации пользователей и средства непрерывного мониторинга радиоэфира.

Ключевые слова: информационная безопасность, корпоративные сети, беспроводная связь, шифрование данных, аутентификация, протокол WPA3, защита от вторжений.

METHODS OF ENSURING INFORMATION SECURITY AND DATA PROTECTION IN CORPORATE WIRELESS NETWORKS

Akyyev Gucanch Aganyyazovich

Lecturer

Jemshidova Oguljeren Maksadovna

Student

Turkmen Institute of Telecommunications and Informatics

Ashgabat, Turkmenistan

Abstract. Methods of ensuring information security in corporate wireless networks are a critically important element of modern IT infrastructure, protecting business processes from external and internal threats. With the massive shift towards mobile workspaces, the wireless segment of the network has become the most vulnerable vector for potential cyberattacks. Effective protection

requires a comprehensive approach that combines advanced encryption technologies, rigorous user identification mechanisms, and continuous monitoring of the radio environment.

Keywords: Information security, corporate networks, wireless communication, data encryption, authentication, WPA3 protocol, intrusion prevention.

Введение

Основой защиты корпоративного Wi-Fi является использование самого актуального стандарта безопасности WPA3-Enterprise, который обеспечивает усиленное шифрование данных на физическом уровне. В отличие от предыдущих версий, WPA3 предлагает 192-битный режим безопасности, соответствующий самым строгим отраслевым стандартам защиты государственной и финансовой информации. Этот протокол значительно усложняет проведение атак методом перебора паролей и защищает пользователей от перехвата трафика даже в случае компрометации отдельных ключей. Внедрение WPA3 является обязательным шагом для любой современной организации, стремящейся к надежной защите своих цифровых активов.

Аутентификация пользователей в корпоративных сетях должна строиться на базе протокола 802.1X с использованием RADIUS-сервера для централизованного управления учетными данными. Этот метод позволяет отказаться от общих паролей (PSK) в пользу индивидуальных сертификатов или уникальных пар логин-пароль для каждого сотрудника. Система 802.1X обеспечивает возможность гибкого управления доступом: при увольнении сотрудника его доступ аннулируется мгновенно на уровне сервера без необходимости смены пароля на всех точках доступа. Интеграция с каталогом Active Directory позволяет автоматизировать этот процесс и поддерживать актуальность прав доступа в реальном времени.

Протоколы шифрования и аутентификации

Основой защиты любой Wi-Fi сети является выбор правильного стандарта безопасности.

WPA3-Enterprise

На сегодняшний день это наиболее защищенный стандарт. В отличие от WPA2, он предлагает:

- **192-битное шифрование:** Соответствует стандартам CNSA (Commercial National Security Algorithm), что необходимо для государственных и финансовых организаций.
- **Защита от подбора пароля:** Использование протокола SAE (Simultaneous Authentication of Equals) делает невозможным офлайн-атаку по словарю.
- **Улучшенная защита конфиденциальности:** Шифрование индивидуальных сессий даже в открытых сетях (Enhanced Open).

802.1X и RADIUS-сервер

Для корпоративных сетей использование общего пароля (PSK) недопустимо. Вместо этого применяется аутентификация на базе портов 802.1X.

- **Принцип работы:** Пользователь или устройство предоставляет учетные данные (логин/пароль или сертификат). Точка доступа пересылает их на **RADIUS-сервер** (например, FreeRADIUS или Cisco ISE), который проверяет их в базе данных (Active Directory/LDAP).
- **Преимущество:** Возможность отозвать доступ конкретному сотруднику без смены пароля для всей компании.

Сегментация сети (VLAN и SSID)

Разделение трафика позволяет изолировать критически важные ресурсы от потенциально опасных зон.

- **Корпоративная сеть (Staff):** Полный доступ к внутренним ресурсам, строгая аутентификация по сертификатам.
- **Гостевая сеть (Guest):** Полная изоляция от внутренней сети. Доступ только в интернет через Captive Portal (страницу авторизации).
- **Сеть для IoT-устройств:** Принтеры, умные датчики и камеры часто имеют уязвимости в прошивках, поэтому их следует выносить в отдельный защищенный сегмент без доступа к серверам с данными.

Сегментация сети является эффективным методом локализации угроз и предотвращения несанкционированного перемещения злоумышленников внутри корпоративного периметра. Путем создания нескольких виртуальных сетей (VLAN) можно изолировать критически важные серверы от гостевого доступа и мобильных устройств сотрудников. Например, гостевой Wi-Fi должен иметь доступ только в интернет и быть физически или логически отделен от внутренней базы данных компании. Такая архитектура гарантирует, что даже в случае взлома одного сегмента, остальные части ИТ-инфраструктуры останутся в безопасности.

Системы обнаружения и предотвращения вторжений в беспроводных сетях (WIPS) предназначены для постоянного сканирования радиоэфира на предмет подозрительной активности. WIPS способны автоматически выявлять «чужие» точки доступа (Rogue AP), которые злоумышленники могут установить для имитации корпоративной сети и кражи учетных данных.

Заключение

В заключение следует подчеркнуть, что информационная безопасность корпоративных беспроводных сетей — это не разовое мероприятие, а непрерывный процесс адаптации к новым вызовам. Сочетание строгих технических стандартов, грамотной архитектуры и высокого уровня осведомленности сотрудников создает надежный щит для бизнеса. Развитие технологий



искусственного интеллекта в системах защиты данных открывает новые горизонты для автоматического обнаружения и нейтрализации угроз. Только комплексный и системный подход гарантирует защиту интеллектуальной собственности и репутации компании в цифровую эпоху.

Список литературы:

1. Анисимов, В. В. (2021). Безопасность беспроводных сетей: методы и средства защиты. Техносфера.
2. Петренко, С. А. (2019). Кибербезопасность и защита данных в корпоративных сетях. Эко-Трендз.
3. Таненбаум, Э., Уэзеролл, Д. (2012). Компьютерные сети. Питер.
4. Gast, M. S. (2017). 802.11 Wireless Networks: The Definitive Guide. O'Reilly Media.