УДК 004.056.5

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПРОТОКОЛОВ БЕЗОПАСНОСТИ ДЛЯ ЗАЩИЩЕННЫХ БЕСПРОВОДНЫХ КОРПОРАТИВНЫХ СЕТЕЙ

МАРЦИНКЕВИЧ ВЛАДИСЛАВ АНТОНОВИЧ,
БЕГЛЯК ЕКАТЕРИНА ВАЛЕРЬЕВНА,
магистранты
РОМАНЮК МАКСИМ ВАЛЕРЬЕВИЧ,
ассистент кафедры «Информатики»
ШАРОНОВА ЕЛЕНА ИВАНОВНА
ассистент кафедры «Вычислительных методов и программирования»
Белорусский Государственный Университет Информатики и Радиоэлектроники

Аннотация: В статье представлен анализ протоколов безопасности, таких как WEP, WPA, WPA2 и WPA3, используемых в беспроводных сетях. Особое внимание уделено уязвимостям данных протоколов и их последствиям. Подробное сравнение проводилось на основе критериев: устойчивость к атакам, уровень шифрования, производительность, удобство использования и совместимость. Анализ показывает, что каждый протокол имеет свои сильные и слабые стороны, и выбор наиболее подходящего протокола зависит от конкретных требований и условий эксплуатации.

Статья нацелена на исследователей и инженеров по кибербезопасности и предлагает детальный обзор протоколов безопасности, а также рекомендации по выбору эффективных решений для защиты корпоративных Wi-Fi сетей.

Ключевые слова: беспроводные сети, уязвимость, протоколы безопасности, шифрование данных, аутентификация, Wired Equivalent Privacy, Wi-Fi Protected Access, TKIP (Temporal key Integrity Protocol), CCMP (Counter mode with Cipher block Chaining Message Authentication Code), SAE (Simultaneous Authentication of Equals), AES (Advanced Encryption Standard), WEP, WPA, WPA2, WPA3

COMPARATIVE ANALYSIS OF SECURITY PROTOCOLS FOR SECURE WIRELESS ENTERPRISE NETWORKS

Martsinkevich Uladzislau Antonovich,
Begliak Ekaterina Vale'evna,
Romanuk Maksim Vale'evich,
Sharonova Elena Ivanovna

Abstract: The article presents an analysis of security protocols such as WEP, WPA, WPA2 and WPA 3 used in wireless networks. Special attention is paid to the vulnerabilities of these protocols and their consequences. A detailed comparison was conducted based on the following criteria: attack resistance, encryption level, performance, usability, and compatibility. The analysis shows that each protocol has its own strengths and weaknesses, and the choice of the most appropriate protocol depends on the specific requirements and operating conditions. The article is aimed at cybersecurity researchers and engineers and offers a detailed overview of security protocols, as well as recommendations on choosing effective solutions for protecting corporate Wi-Fi

networks.
Keywords: wireless networks, vulnerability, security protocols, data encryption, authentication, Wired Equivalent Privacy, Wi-Fi Protected Access, TKIP (Temporal key Integrity Protocol), CCMP (Counter mode with Cipher block Chaining Message Authentication Code), SAE (Simultaneous Authentication of Equals), AES (Advanced Encryption Standard), WEP, WPA, WPA2, WPA3

С развитием технологий беспроводные сети (WLAN) стали неотъемлемой частью корпоративной инфраструктуры, предоставляя удобство, гибкость и мобильность, постоянно расширяясь как для общественного, так и для личного использования, и Wi-Fi стал неотъемлемой частью повседневной жизни.

Безопасность беспроводных сетей является актуальной темой для исследователей и специалистов в области информационной безопасности. Эти сети подвержены дополнительным рискам, таким как перехват данных, атаки типа "человек посередине" (MITM) и отказ в обслуживании (DoS, DDoS).

Для защиты корпоративных беспроводных сетей требуются надежные механизмы, обеспечивающие безопасную аутентификацию, контроль доступа и шифрование данных. Рассмотрим основные протоколы безопасности, применяемые в Wi-Fi-сетях.

WEP (Wired Equivalent Privacy) – первый стандарт безопасности для беспроводных сетей, представленный в 1997 году. Он использует алгоритм шифрования Rivest Cipher 4 (RC4) с 40- или 104-битным ключом, имеет совместимость со старыми устройствами, простая реализация и поддержка. Однако WEP имеет крайне низкий уровень безопасности из-за уязвимостей в алгоритме RC4 – ключи шифрования статичны и могут быть взломаны в течение короткого времени с помощью инструментов вроде Aircrack-ng, уязвим для атак типа Initialization Vector Reuse (IV). Исследователи из UC Berkeley обнаружили, что для успешной атаки на WEP достаточно проанализировать около одного дня сетевого трафика [1]. Еще одной уязвимостью WEP является его способность транслировать поддельные пакеты данных из-за аутентификации с общим ключом, что позволяет злоумышленнику легко подделать сообщение аутентификации. Повторное использование вектора инициализации также делает WEP слабым, когда различные методы криптоанализа могут расшифровать данные. WEP признан небезопасным и не рекомендуется к использованию [2, с. 105].

WPA (Wi-Fi Protected Access) был разработан в 2003 году как временное решение до внедрения полноценного стандарта WPA2. WPA использует улучшенный алгоритм TKIP (Temporal Key Integrity Protocol) для шифрования, где RC4 применяется для генерации других ключей. Протокол безопасности WPA использует динамическое управление ключами, при котором для каждого пакета генерируется 128-битный ключ. Это предотвращает атаки на основе повторного использования ключей. WPA поддерживает аутентификацию через серверы RADIUS, обеспечивая безопасное подключение к сети, а также использует Pre-Shared Key (PSK) — статический ключ для инициации связи между двумя сторонами. Контроль целостности данных осуществляется через механизм Message Integrity Check (MIC), который предотвращает изменение данных в передаваемых пакетах [3, с. 186]. Для обеспечения управления ключами используется механизм 4-стороннего квитирования (рукопожатия). Основная уязвимость в WPA заключается в использовании RC4, где вычисление ключей с одним и тем же вектором инициализации позволяет злоумышленнику легко вычислить временный ключ. Другая уязвимость заключается в том, что при слабом пароле он уязвим для атак методом подбора, если пароль состоит менее чем из 20 символов.

В 2004 году появился WPA2, который обеспечил значительное улучшение по сравнению с предыдущими протоколами безопасности. Основное отличие заключается в его методе шифрования. WPA2 использует алгоритм AES (Advanced Encryption Standard), который значительно сложнее для взлома по сравнению с TKIP, применяемым в WPA. WPA2 использует режим счетчика с протоколом кода аутентификации сообщений цепочки блоков шифра (CCMP), который шифрует данные с помощью AES. Генерация ключа в WPA2 требует 4-стороннего рукопожатия для переходного парного ключа (PTK) и группового временного ключа (GTK), а также рукопожатия группового ключа.

В WPA2 предусмотрено два режима работы: режим Pre-Shared Key (PSK) для персональных сетей и корпоративный режим (Enterprise) для крупных сетей. В WPA2-PSK точка доступа аутентифицирует клиента на основе заранее предоставленного пароля, тогда как аутентификация в корпоративном режиме выполняется с помощью расширяемого протокола аутентификации (EAP) в архитектуре 802.1X [2, с. 112].

Несмотря на высокий уровень защиты, WPA2 не является абсолютно неприступным. Одной из слабостей WPA2 является возможность злоумышленника получить доступ к сети и определенные ключи для атаки на другие устройства, подключенные к сети. Выполнение такого действия может занять от 2 до 14 часов, что представляет собой проблему безопасности, которую необходимо решить. Кроме того, WPA2 допускает повторную инициализацию ключей, что приводит к атакам, называемым KRACK. Эта атака использует 4-стороннее рукопожатие, которое протоколы беспроводной безопасности используют для аутентификации пользователей при подключении к сети. После сброса счетчиков злоумышленник может повторно воспроизвести и расшифровать сообщения.

Стандарт безопасности WPA3 был представлен в 2018 году и является наиболее безопасным стандартом на текущий момент. Как и его предшественник, он имеет два режима работы: WPA3-Personal и WPA3-Enterprise.

WPA3-Personal использует протокол аутентификации с обменом ключами (SAE), который представляет собой защищенный протокол обмена ключами между одноранговыми узлами, разработанный для целей аутентификации. SAE заменяет Pre-Shared Key (PSK), используемый в WPA2, и обеспечивает более безопасное установление соединения, предотвращая атаки методом перебора паролей. Аутентификация происходит при каждом подключении устройства, что усложняет процесс взлома. Высокоэнтропийный парный главный ключ (PMK), создаваемый при аутентификации WPA3-SAE, используется в качестве входных данных для 4-стороннего рукопожатия, создающего парный переходный ключ (PTK). Защита кадров управления (MFP) в WPA3-SAE предотвращает атаки де-аутентификации, когда злоумышленники заставляют пользователей отключаться от точки доступа (AP).

Не все текущее сетевое оборудование Wi-Fi способно поддерживать MFP или SAE, и поэтому сертификат WPA3 имеет переходный режим, который поддерживает WPA2 и WPA3 одновременно. В этом режиме точка доступа WPA2 будет подключаться с использованием 4-стороннего рукопожатия без MFP, а точка доступа WPA3 будет подключаться с использованием рукопожатия SAE с MFP [4].

WPA3-Enterprise принципиально не отличается от версии WPA2, но вместо этого сосредоточен на добавлении улучшений и повышении устойчивости к неправомерному использованию. На уровне протокола WPA3 предлагает дополнительный 192-битный режим безопасности, который использует 256-битный протокол режима Галуа/счетчика (Galois/Counter Mode Protocol) (GCMP), широко известный как GCMP-256, для обеспечения аутентифицированного шифрования.

WPA3 является рекомендованным стандартом для корпоративных сетей, обеспечивая максимальную защиту.

Для выбора наиболее надежного протокола защиты беспроводной корпоративной сети необходимо сравнить существующие решения по ключевым критериям: устойчивость к атакам, уровень шифрования, производительность, удобство использования и совместимость (табл. 1).

Таблица 1

Сравнительная таблица характеристик протоколов безопасности

Протокол	WEP	WPA	WPA2	WPA3
Шифрование	RC4 (40/104 бит)	TKIP	AES-CCMP	AES-GCMP (128/192 бит)
Аутентификация	PSK (статический ключ)	PSK/802.1X	PSK/802.1X	SAE/802.1X
Устойчивость к атакам	Очень низкая (легко взламывается)	Уязвим к атакам (слабый TKIP)	Подвержен атаке KRACK	Высокая (защита от словарных атак и MITM)
Производительность	Высокая (низкая нагрузка)	Средняя	Средняя/ высокая	Средняя
Совместимость	Старые устройства	Широкая	Большинство устройств	Современные устройства

Использование WEP или WPA категорически не рекомендуется, они не обеспечивают надежной защиты и не должны использоваться в корпоративных сетях.

WPA2 остается допустимым вариантом для корпоративных сетей, но необходимо использовать длинные сложные пароли и обновленные версии прошивок для защиты от KRACK.

WPA3 является самым безопасным протоколом для новых корпоративных сетей благодаря защите от современных атак.

Список источников

1. Security of the WEP algorithm [Электронный ресурс]. – Режим доступа: URL: http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html (24.02.2025)
2. Технология современных беспроводных сетей Wi-Fi / Е.В. Смирнова [и др.]. – Москва : МГТУ им.Баумана, 2017. – 446 с.
3. Бирюков, А.А. Информационная безопасность: защита и нападение / А.А. Бирюков. – Москва : ДМК Пресс, 2023. – 440 с.
4. Wireless Security Protocols WPA3: A Systematic Literature Review [Электронный ресурс]. – Режим доступа: URL: https://ieeexplore.ieee.org/document/10274082 (24.02.2025)