

Методы и средства обеспечения информационной безопасности

Обзорная статья
DOI 10.66424/2071-8217-2026-3-3
УДК 004.056.5

ОБЗОР ПРОТОКОЛОВ ОРГАНИЗАЦИИ ЗАЩИЩЕННОГО УДАЛЕННОГО ДОСТУПА К КОМПЬЮТЕРНЫМ СИСТЕМАМ

А. М. Сиотанов*, А. С. Макаров

Санкт-Петербургский политехнический университет Петра Великого, Санкт-Петербург, Россия

✉ *siotanol.am@edu.spbstu.ru

ДЛЯ ЦИТИРОВАНИЯ

Сиотанов А. М., Макаров А. С.
Обзор протоколов организации
защищенного удаленного доступа
к компьютерным системам // Проблемы информационной безопасности. Компьютерные системы. 2026. № 3. С. 49–59.
DOI: 10.66424/2071-8217-2026-3-3

ПОСТУПИЛА 09.04.2026

ПРИНЯТА 15.07.2026

ОПУБЛИКОВАНА 13.10.2026

© Сиотанов А. М., Макаров А. С.
Издатель: Санкт-Петербургский
политехнический университет
Петра Великого

АННОТАЦИЯ

Рассматривается проблема обеспечения информационной безопасности при удаленном доступе к информационным ресурсам. Актуальность обусловлена ростом распределенных компьютерных систем и высокими рисками перехвата данных при передаче учетных данных. Выполнен анализ функций сервера удаленного доступа и базового протокола канального уровня Point-to-Point Protocol. Основное внимание уделено классификации и сравнению протоколов аутентификации: прямой (PAP, CHAP, S/Key) и не прямой (централизованной) схемы (RADIUS, Kerberos). Подробно разобраны алгоритмы работы каждого протокола. В результате исследования обоснована необходимость комбинированного подхода к выбору протоколов аутентификации в зависимости от архитектуры сети, а также сформулированы требования к современным системам удаленного доступа.

КЛЮЧЕВЫЕ СЛОВА

Защита информации, удаленный доступ, протокол, аутентификация, компьютерные системы

Review article
DOI 10.66424/2071-8217-2026-3-3

REVIEW OF PROTOCOLS FOR SECURE REMOTE ACCESS TO COMPUTER SYSTEMS

A. M. Siotanov*, A. S. Makarov

Peter the Great St. Petersburg Polytechnic University, St. Petersburg, Russia

✉ *siotanol.am@edu.spbstu.ru

FOR CITATION

Siotanov A. M., Makarov A. S. Review of protocols for secure remote access to computer systems. *Problems of information security. Computer systems*. 2026. No. 3, pp. 49–59.
DOI: 10.66424/2071-8217-2026-3-3
(In Russian)

RECEIVED 09.04.2026

ACCEPTED 15.07.2026

PUBLICATION 13.10.2026

ABSTRACT

The article discusses the problem of ensuring information security with remote access to information resources. The relevance of the work is due to the growth of distributed computer systems and the high risks of data interception during the transfer of credentials. The functions of the remote access server and the basic Point-to-Point Protocol link layer are analyzed. The main focus is on the classification and comparison of authentication protocols: direct scheme (PAP, CHAP, S/Key) and indirect (centralized) scheme (RADIUS, Kerberos). The article describes in detail the algorithms of each protocol. As a result of the research, the necessity of a combined approach to the choice of authentication protocols depending on the network architecture is substantiated, as well as the requirements for modern remote access systems are formulated.

KEYWORDS

Information security, remote access, protocol, authentication, computer systems

1. ВВЕДЕНИЕ

В современных распределенных компьютерных системах значимость удаленного доступа к информационным ресурсам возросла настолько, что он сравнялся по важности с доступом в режиме прямого соединения. При этом доступ к корпоративной сети извне идет через внешнюю, по сути небезопасную среду – через сеть Интернет. Таким образом появляется риск перехвата данных по средствам атаки Man-in-the-Middle, вследствие чего появляется необходимость проверки подлинности пользователя и сетевого узла. Для обеспечения безопасного сетевого взаимодействия при удаленном подключении должны использоваться специальные протоколы.

2. МЕТОДЫ

Ключевым элементом инфраструктуры, обеспечивающим контролируемый доступ удаленных клиентов к внутренним ресурсам, является «Сервер удаленного доступа», который выполняет установку связи с удаленными узлами, аутентификацию удаленного узла, передачу данных между узлами (посредник). Существует три схемы аутентификации, позволяющие

удаленно получить доступ к ресурсам компьютерной системы: прямая, непрямая и автономная.

Перед рассмотрением протоколов удаленной аутентификации необходимо рассмотреть среду их функционирования. Исторически сложилось, что большинство протоколов удаленной аутентификации создавались для работы в составе протокола канального уровня эталонной модели взаимодействия открытых систем, известного как протокол «точка – точка» или Point-to-Point Protocol (PPP). Point-to-Point Protocol создан для установления прямого соединения между двумя узлами по установленному каналу, используя пакеты сетевого уровня эталонной модели взаимодействия открытых систем. Алгоритм установления соединения PPP представлен на рис. 1.

Протокол PPP обеспечивает работу протоколов сетевого уровня по средствам инкапсуляции сетевых пакетов через канал удаленной связи. Он поддерживает следующие функции: аутентификацию пользователя и сервера; сжатие и шифрование при обмене данными; обнаружение ошибок и петлевых соединений; контроль целостности данных; настройку параметров сетевого уровня.

Прямая схема аутентификации (протоколы аутентификации удаленных пользователей). В схеме прямой аутенти-

фикации в роли точки обслуживания выступает один сервер либо каждая точка обслуживания функционирует сама по себе, т.е. проверяет пользователей самостоятельно и ведет собственную базу учетных записей (рис. 2).

Аутентификация – это процедура проверки подлинности субъекта доступа, которая является первым и важным этапом удаленного подключения. В протоколе PPP изначально заложены механизмы для удаленной проверки подлинности.

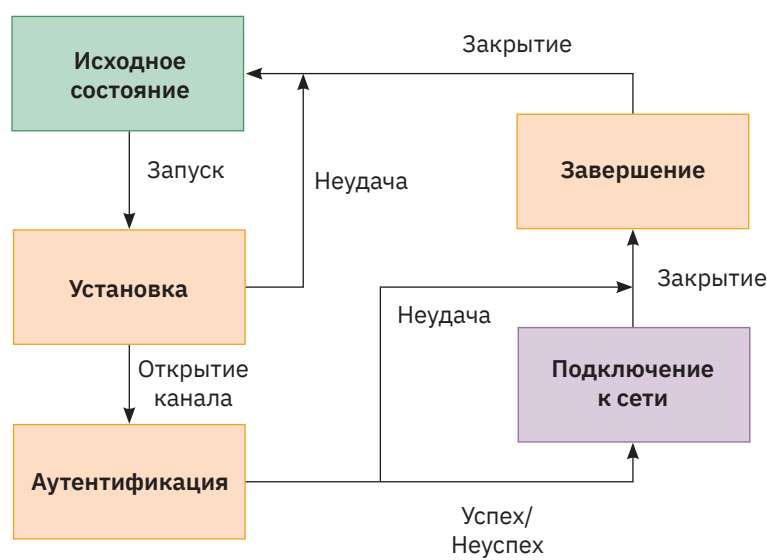


Рис. 1 | Алгоритм установления соединения PPP

Fig. 1 | Point-to-Point Protocol connection establishment algorithm

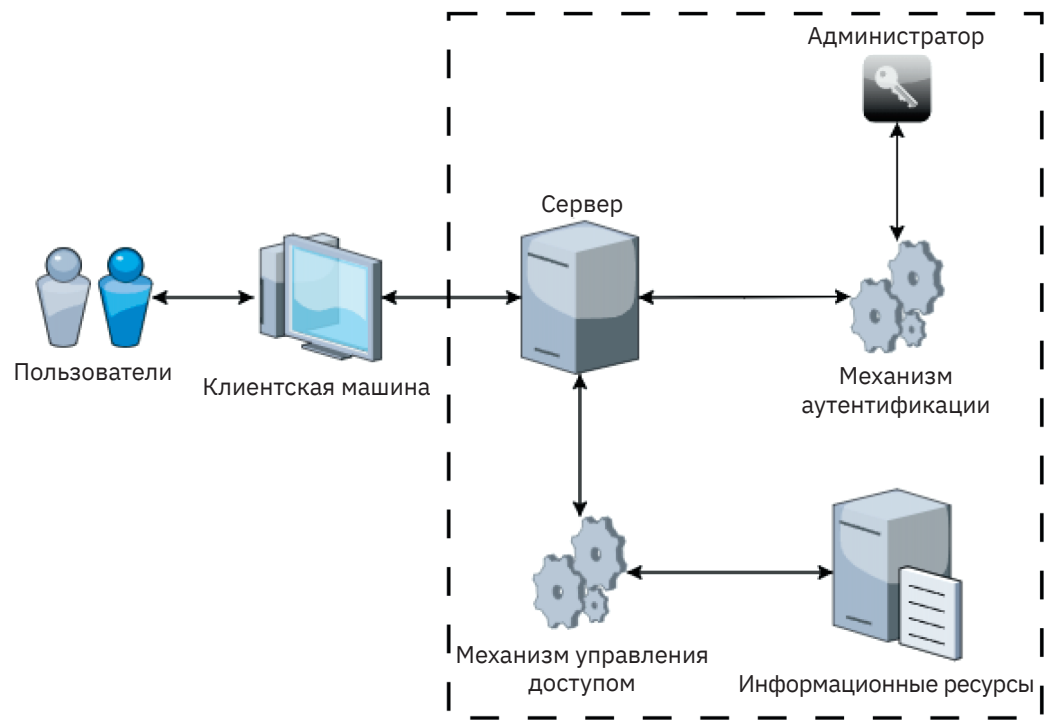


Рис. 2 | Схема прямой аутентификации

Fig. 2 | Direct authentication scheme

Стандарт RFC1334 описывает два таких протокола: Password Authentication Protocol (PAP) – протокол аутентификации по паролю; Challenge Handshake Authentication Protocol (CHAP) – протокол аутентификации по рукопожатию.

Наличие указанных протоколов говорит о том, что каждая из взаимодействующих сторон может самостоятельно предложить использование одного из стандартных (встроенных) протоколов.

Многие организации разрабатывают собственные протоколы удаленной аутентификации под PPP – стандартных средств из RFC 1334 им бывает недостаточно. На деле такие фирменные протоколы почти всегда базируются на PAP и CHAP, т.е. являются их модификациями. Обычно меняют форматы пакетов, добавляют новые коды сообщений или вводят дополнительные раунды обмена. Встречаются также варианты с усиленным хешированием вместо штатного.

Протокол PAP. Аутентификация в протоколе PAP подразумевает участие двух субъектов – клиент и сервер. В процессе аутентификации клиент передает свой идентификатор и аутентификатор серверу в незащищенном виде. Получив данные клиента, сервер проводит сравнение с записями. Данные записи берутся из внутренней регистрационной базы легитимных пользователей. При успешном сравнении данных аутентификация счи-

тается разрешенной и процесс завершается. В противном случае клиент получает запрет доступа к серверу.

Подобный подход является неприемлемым из-за высоких рисков перехвата учетных данных. Следовательно, протокол PAP целесообразно использовать только совместно с протоколами, основанными на одноразовых паролях, такими как S/Key.

Протокол CHAP является более защищенным, поскольку передает пароль клиента серверу в хешированном виде. Ключевая особенность заключается в том, что при формировании хеш-значения используется случайное число, сгенерированное сервером. Поскольку алгоритм хеширования является необратимым, риск перехвата данных существенно снижается. В стандарте RFC1334 для подсчета хеш-значений определен алгоритм Message Digest Algorithm версии 5, которая преобразует входные данные любого размера в данные фиксированного размера 128-битную (32-символьную шестнадцатеричную) строку.

Спецификация CHAP описывает четыре разновидности пакетов: challenge (пакет-запрос, он же «вызов»); response (пакет-ответ, он же «отклик»); success (пакет-подтверждение успешной аутентификации); failure (пакет-отказ в аутентификации).

На рис. 3 представлен процесс аутентификации по протоколу CHAP.

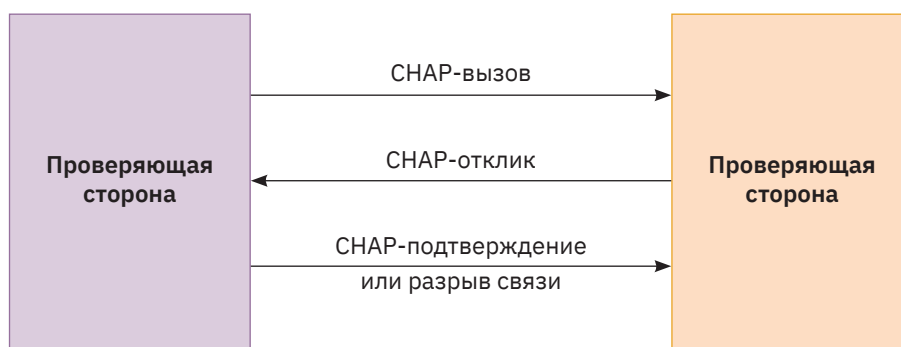


Рис. 3 | Аутентификация по протоколу CHAP

Fig. 3 | Authentication using the CHAP protocol

При описании процедуры удаленной аутентификации по CHAP используются следующие обозначения: сервер аутентификации – AS ; клиент – C ; пользователь – U ; пароль – P ; случайное число – N ; идентификатор пользователя/сервера – IDU/IDS ; хеш-значения (отклик) – R :

- 1) AS : генерация N .
- 2) $AS \rightarrow C$: IDS , N и его длину в байтах.
- 3) $U \rightarrow C$: P .
- 4) C : вычисление $R = H(IDS, N, P)$.
- 5) $C \rightarrow AS$: IDU, R .
- 6) AS : извлечение из регистрационной базы соответствующие IDU и P , вычисление собственного $H(IDS, N, P)$ и сравнение его с R .
- 7) $AS \rightarrow C$: в случае совпадения значения – авторизация U , иначе отказ в доступе и разрыв соединения.

Таким образом, пакет вызова производится на шаге 2, отклик на шаге 5, подтверждение или отказ на шаге 7.

К случайному числу N предъявляются два требования – уникальность (отсутствие повторов) и непредсказуемость. Если уникальность нарушена, например, из-за использования генератора псевдослучайных чисел с коротким периодом, то злоумышленник может перехватить пакет с откликом. Затем он дожидается, когда сервер снова отправит вызов с тем же N , и подставляет перехваченный отклик. Так реализуется несанкционированный доступ к серверным ресурсам. Если же N предсказуемо (например, генерируется по системному таймеру), атакующий способен сам сформировать корректный пакет-вызов и отправить его клиенту, имитируя сервер.

На практике значение N формируется как некоторая битовая последовательность, полученная объединением двух составляющих: метки текущего времени (дата и время с точностью до секунд) в момент генерации; случайного числа, выдаваемого программным либо аппаратным генератором псевдослучайных чисел. Такое комбинирование обеспечивает N нужные свойства уникальности (за счет временной метки) и непредсказуемости (за счет псевдослучайной компоненты).

В 1997 г. компания Microsoft разработала «фирменную» версию протокола CHAP под названием MS-CHAP. Затем MS-CHAP был модернизирован, и получена версия 2. Эта версия несет в себе эффективный механизм аутентификации, где соединение не считается установленным до тех пор, пока клиент не удостовериться в подлинности сервера удаленного доступа.

Протокол S/Key. Модель протокола S/Key основана на применении одноразовых паролей. Требование формирования одноразовых паролей строго регламентируется последовательностью применений необратимых функций алгоритма Message Digest Algorithm версии 4. Первым этапом работы протокола является генерация списка одноразовых паролей, вторым – непосредственно аутентификация.

Алгоритм работы протокола S/Key:

- 1) $AS \rightarrow C$: запрос IDU .
- 2) $C \rightarrow AS$: IDU .
- 3) AS : генерация случайного числа N .
- 4) $AS \rightarrow C$: запрос числа одноразовых паролей K .
- 5) $C \rightarrow AS$: K .
- 6) AS : по IDU извлекает из регистрационной базы значения P , вычисляет одноразовые пароли $w_1 = H(N, P)$, $w_2 = H(H(N, P))$, ..., $w_{K+1} = H(H(...(H(N, P))...))$, сохраняет значения в регистрационную базу.

При очередной аутентификации:

- 1) $C \rightarrow AS$: IDU .
- 2) $AS \rightarrow C$: K, N .
- 3) C : $w_1 = H(N, P)$, $w_2 = H(H(N, P))$, ..., $w_K = H(H(...(H(N, P))...))$.
- 4) $C \rightarrow AS$: w_k .
- 5) AS : $w_{k+1} = H(w_k)$, сравнивает полученное значение со значением в регистрационной базе. В случае совпадения, аутентификация считается успешной.

Непрямая схема аутентификации (централизованный контроль удаленного доступа). Непрямая аутентификация основана на использовании сложных протоколов (например, RADIUS, Kerberos). Их выполнение начинается после попытки аутентификации, поступающей с удаленного узла на любой сервер. Схема не прямой аутентификации представлена на рис. 4.

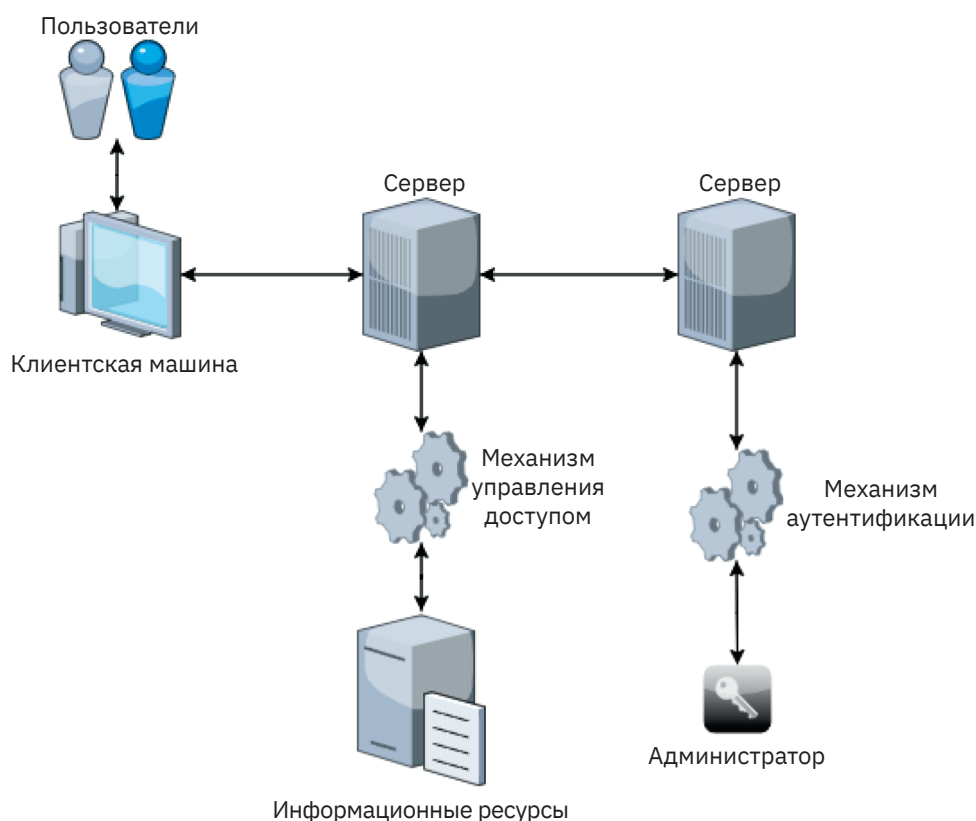


Рис. 4 | Схема не прямой аутентификации

Fig. 4 | Scheme of indirect authentication

Протокол Remote Authentication Dial in User Service (RADIUS) состоит из сервера доступа и собственных агентов. Агент – это посредник между клиентом и сервером. Сфера его задач заключается в передаче данных и инструкций. Сервер RADIUS взаимодействует исключительно с агентами, принимая от них данные и направляя инструкции.

В основе аутентификации между агентами и серверами RADIUS лежит использование разделяемого секретного ключа, который в рамках рассматриваемой схемы обозначим как KR (ключ RADIUS). Данный ключ заранее распределяется между взаимодействующими сторонами и никогда не передается по сети в открытом или зашифрованном виде – это позволяет исключить риск его компрометации при перехвате трафика. Весь обмен данными между агентами и сервером осуществляется исключительно в зашифрованном виде. Такой подход гарантирует конфиденци-

альность передаваемой информации, включая учетные данные пользователей. Схема централизованного управления удаленным доступом с использованием протокола RADIUS представлена на рис. 5.

Предлагается рассмотреть простой вариант работы протокола RADIUS, но перед этим введем дополнительные обозначения: сервер RADIUS – S ; агент RADIUS – A ; шифрование пароля – EP ; отклик – R ; аутентификатор – RA ; сеансовый ключ – K .

1) $S \rightarrow A: ID, P$.

2) A : генерация N , вычисление $K = H(KR, N)$, шифрование $EP = K \text{ XOR } P$.

3) $A \rightarrow S: N, ID, EP$.

4) S : вычисление $K = H(KR, N)$ расшифрованных $P = EP \text{ XOR } K$, извлечение из регистрационной базы пароля пользователя и его сравнение с получившимся после расшифровки P , генерация R – «доступ разрешен» или «отказ в доступе», вычисление $RA = H(R, N, KR)$.

5) $S \rightarrow A: R, RA$.

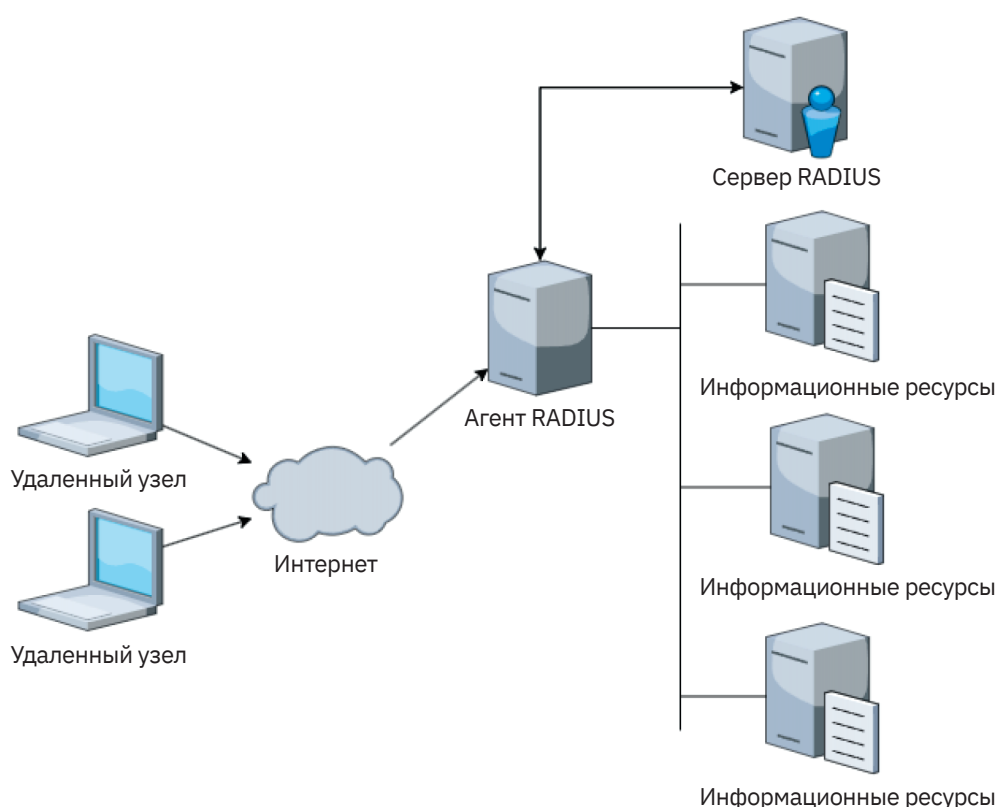


Рис. 5 | Схема централизованного контроля удаленного доступа по протоколу RADIUS

Fig. 5 | Scheme for centralized control of remote access via the RADIUS protocol

6) A : вычисление $H(R, N, KR)$ и сравнение с RA , при совпадении проверка R .

Случайное число N необходимо для сеансового ключа, который нужен для защищенной передачи пароля. Аутентификатор RA необходим для подтверждения ответа сервера и запроса агента.

Предлагается рассмотреть второй вариант реализации протокола RADIUS:

- 1) $C \rightarrow A: ID$.
- 2) $A \rightarrow S: ID$.
- 3) S : генерация случайного запроса X .
- 4) $S \rightarrow A: X$.
- 5) $A \rightarrow C: X$.
- 6) C : вычисление отклика $Y = F(X)$.
- 7) $C \rightarrow A: Y$.
- 8) A : генерация N .
- 9) $A \rightarrow S: ID, N, Y$.
- 10) S : вычисление $F(X)$ и его сравнение с Y , генерация R , вычисление $RA = H(R, N, KR)$.
- 11) $S \rightarrow A: R, RA$.

12) A : вычисление $H(R, N, RA)$ и его сравнение с RA , при совпадении проверка R .

Во второй версии RADIUS появился встроенный механизм «рукопожатия». Это обмен служебными пакетами до начала передачи учетных данных. Такая схема закрывает две основные угрозы – перехват пароля в канале и атаки повторра (replay). Механизм работает в момент, когда пароль передается от клиента к агенту, и использует временные метки или счетчики пакетов, чтобы старые перехваченные пакеты нельзя было использовать повторно.

Среди недостатков протокола RADIUS можно выделить, что любое взаимодействие клиента с агентом влечет за собой аутентификацию через сервер RADIUS. Как следствие, наблюдается рост сетевого трафика и возникают сложности при расширении инфраструктуры.

Протокол Kerberos работает по билетной схеме, где клиенту выдают билет (или

мандат) в момент, когда он аутентифицируется в сети. Далее этот билет используется для подтверждения его прав. Билеты допускают многократное применение на протяжении установленного при их создании периода действия. Сам билет является зашифрованной формой базового ключа. При этом один экземпляр ключа разделяют центр распределения ключей (KDC) и сервер, а другой – KDC и клиент.

Сервер Kerberos обычно делится на две части: сервер аутентификации (AS) и сервер выдачи билетов (TGS), которые могут быть в распределенном режиме или физически совмещены. Kerberos создает сеансовые ключи, которые выдаются двум узлам для защищенного общения. После завершения сеанса ключ уничтожается.

Предлагается рассмотреть основной алгоритм работы протокола Kerberos (рис. 6):

- 1) $C \rightarrow AS$: запрос билета для обращения к TGS.
- 2) $AS \rightarrow C$: выдача билета.
- 3) $C \rightarrow TGS$: запрос билета на получение доступа на информационный ресурс RS .

4) $TGS \rightarrow C$: выдача билета.

5) $C \rightarrow RS$: запрос на доступ, предоставление билета.

6) $RS \rightarrow C$: предоставление доступа.

3. РЕЗУЛЬТАТЫ И ОБСУЖДЕНИЕ

Для выбора оптимальной схемы удаленной аутентификации составлены критерии выбора: степень защищенности от возможных атак; простота реализации и администрирования; удобство масштабирования; оценка рисков при отказе работы системы удаленной аутентификации.

Углубленный разбор работы протоколов PAP, CHAP и S/Key подтвердил закономерность роста безопасности механизмов аутентификации. PAP признан устаревшим из-за незащищенной передачи пароля, CHAP с механизмом «рукопожатия» и хешированием пароля гарантирует защиту от прямого перехвата учетных данных, MS-CHAPv2 – более совершенный аналог для коммерческой

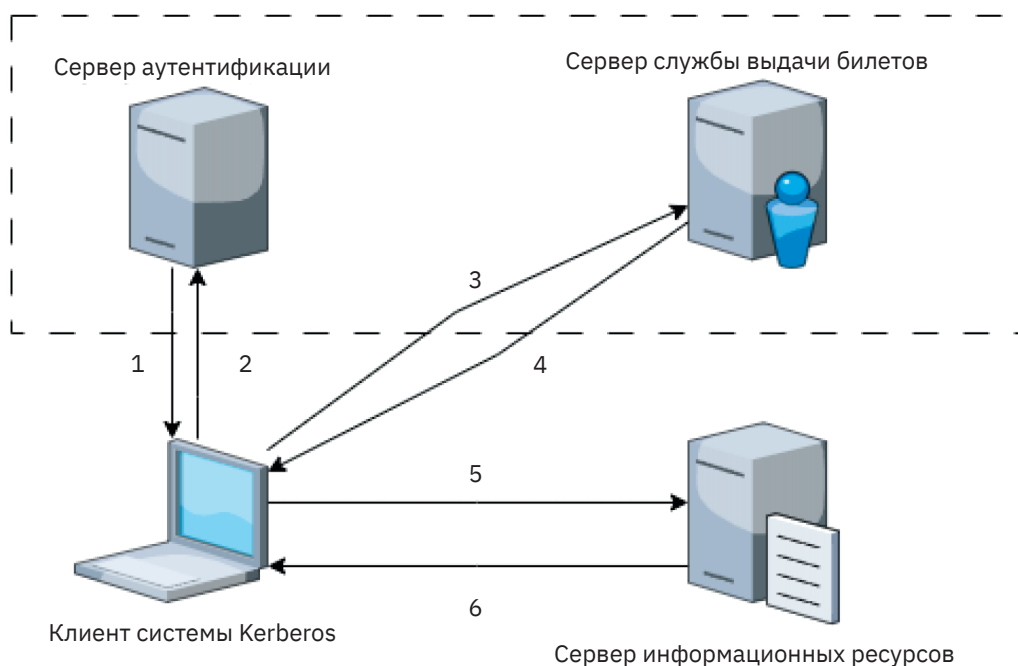


Рис. 6 | Схема удаленного доступа по протоколу Kerberos

Fig. 6 | Scheme of remote access using the Kerberos protocol.

среды. S/Key протокол обеспечивает высокий уровень защиты за счет одноразовых паролей, но требует дополнительной вычислительной мощности для генерации парольной последовательности.

Анализ протоколов не прямой аутентификации (RADIUS, Kerberos) показал, что при централизованном управлении доступом RADIUS подходит для простых решений, а Kerberos выигрывает в защищенности за счет шифрования и разделяемых ключей, но при этом увеличивает сетевой трафик из-за частых обращений к серверу. Механизм билетов и сеансовых ключей в Kerberos сокращает нагрузку на сервер при многократных запросах одного пользователя в пределах одной сессии, но требует синхронизации времени и сложно настраивается.

Практически оптимальным решением является смешанный сценарий, где используется CHAP для первоначального «точка – точка» подключения, а последующее централизованное управление доступом к распределенным ресурсам через Kerberos или RADIUS.

4. ЗАКЛЮЧЕНИЕ

По результатам исследования сформирован вывод, что выбор оптимального протокола удаленной аутентификации не может быть универсальным и должен производиться исходя из результатов анализа архитектуры сети, ее масштаба и требуемого уровня доверия к узлам.

Протокол PPP в своей основе отвечает за установку соединения и управление IP-адресами, но сам по себе не обеспечивает защиту данных с помощью шифрования. Поэтому для безопасности требуется добавление специальных протоколов.

Анализ не прямых схем аутентификации показал, что они хорошо работают для создания масштабируемых и централизованно управляемых сетей. Протокол RADIUS и Kerberos работают по схеме «агент – сервер» и помогают упростить процесс аутентификации, при этом обеспечить его безопасность.

Таким образом, для безопасного удаленного доступа в компьютерных системах нужен комплексный подход.

КОНФЛИКТ ИНТЕРЕСОВ / CONFLICT OF INTERESTS

Авторы заявляют об отсутствии конфликта интересов / The authors declare no conflict of interests.

СПИСОК ИСТОЧНИКОВ

1. Dalal N., Shah J., Hisaria K., Jinwala D. A Comparative Analysis of Tools for Verification of Security Protocols // International Journal of Communications, Network and System Sciences. 2010. Vol. 3. № 10. P. 779–787. DOI: 10.4236/ijcns.2010.310104.
2. Петров Н. В. Моделирование работы RADIUS-сервера с кэшированием данных // Перспективы развития информационных технологий. 2014. № 22. С. 83–89.
3. Васинёв Д. А., Петров Г. В. Реализация и тестирование взаимодействия узла коммутации организации и RADIUS-сервера // Вестник науки и творчества. 2020. № 5 (53). С. 45–49.
4. Евсеев С. П., Дорохов А. В., Король О. Г. Механизмы и протоколы защиты информации в компьютерных сетях и системах // VOJNOTEHNIČKI GLASNIK (MILITARY TECHNICAL COURIER). 2011. Т. LIX. № 4. С. 15–39.
5. Воробьев П. А., Зиятдинов Н. Р., Сенцова А. Ю. Практическое исследование протокола Kerberos: атаки, обнаружение и разработка правил детектирования // Инженерный вестник Дона. 2025. № 2 (122). С. 398–422.
6. Никешин А. В., Шнитман В. З. Обзор расширяемого протокола аутентификации и его методов // Труды Института системного программирования РАН. 2018. Т. 30. № 2. С. 113–148.

7. Бахарев В. В., Долгушина К., Шелейко В. А. Удаленная идентификация пользователей как управленческий и маркетинговый инструмент // Исследование проблем экономики и финансов. 2023. № 4. DOI: 10.31279/2782-6414-2023-4-8.
8. Береза Н. В., Михнова Е. Г. Информационные услуги удаленного доступа // Экономика и социум. 2015. № 1–2 (14). С. 445–447.
9. Довгаль В. А., Меретукова С. К., Шерedyко Д. И. Организация безопасного удаленного доступа сотрудника коммерческой компании, работающего вне офиса // Вестник Адыгейского государственного университета. Серия: Естественно-математические и технические науки. 2021. № 2 (281). С. 72–81.
10. Сидоренко Д. А., Федотов Е. А. Некоторые аспекты использования и программирования протокола PPP // Вестник науки. 2024. № 12 (81). С. 1643–1649.
11. Петров Н. В. Моделирование работы RADIUS-сервера в телекоммуникационной компании // Перспективы развития информационных технологий. 2013. № 14.
12. Омётов А. Я., Беззатеев С. В., Кучерявый У. А. Протокол аутентификации для передачи прав пользования электронными устройствами // Научно-технические ведомости СПбГПУ. Информатика. Телекоммуникации. Управление. 2017. Т. 10. № 4. С. 29–40. DOI: 10.18721/JCSTCS.10403.
13. Чекмарев Д. Ю., Борзенкова С. Ю., Баранова Е. М. Методы аутентификации и защиты информации на удаленных рабочих местах // Известия Тульского государственного университета. Технические науки. 2024. № 3. С. 111–113.
14. Балюк А. А., Финько О. А. Многоагентная аутентификация цифровых двойников в киберфизических системах // Вопросы кибербезопасности. 2022. № 5 (51). С. 100–113. DOI: 10.21681/2311-3456-2022-5-100-113.
15. Головняк П. А., Зайцев К. С., Пинчук А. М. Метод аутентификации на удаленном сервере для обеспечения непрерывности обработки данных в защищенных системах // International Journal of Open Information Technologies. 2022. Т. 10. № 8. С. 94–101.

REFERENCES

1. Dalal N., Shah J., Hisaria K., Jinwala D. A Comparative Analysis of Tools for Verification of Security Protocols. *International Journal of Communications, Network and System Sciences*. 2010. Vol. 3. No. 10, pp. 779–787. DOI: 10.4236/ijcns.2010.310104.
2. Petrov N. V. Modeling the operation of a RADIUS server with data caching. *Perspektivy razvitiya informacionnyh tehnologij*. 2014. No. 22, pp. 83–89. (In Russian)
3. Vasinyov D. A., Petrov G. V. Implementation and testing of the interaction between the organization's switching node and the RADIUS server. *Vestnik nauki i tvorchestva*. 2020. No. 5 (53), pp. 45–49. (In Russian)
4. Evseev S. P., Dorokhov A. V., Korol O. G. Mechanisms and Protocols for Information Security in Computer Networks and Systems. *VOJNOTEHNIČKI GLASNIK (MILITARY TECHNICAL COURIER)*. 2011. Vol. LIX. No. 4, pp. 15–39. (In Russian)
5. Vorobyov P. A., Ziyatdinov N. R., Sentsova A. Yu. Practical Study of the Kerberos Protocol: Attacks, Detection, and Development of Detection Rules. *Inzhenernyj vestnik Dona*. 2025. No. 2 (122), pp. 398–422. (In Russian)
6. Nikeshin A. V., Shnitman V. Z. The review of Extensible Authentication Protocol and its methods. *Proceedings of the Institute for System Programming of the RAS (Proceedings of ISP RAS)*. 2018. Vol. 30. No. 2, pp. 113–148. (In Russian)
7. Bakharev V. V., Dolgusina K., Sheleyko V. A. Remote Identification of Users as a Management and Marketing Tool. *Research in Economic and Financial Problems*. 2023. No. 4. DOI: 10.31279/2782-6414-2023-4-8. (In Russian)
8. Bereza N. V., Mikhnova E. G. Remote access information services. *Ehkonomika i socium*. 2015. No. 1–2 (14), pp. 445–447. (In Russian)
9. Dovgal V. A., Meretukova S. K., Sheredko D. I. Organization of secure remote access for an employee of a commercial company working outside the office. *Vestnik Adygejskogo gosudarstvennogo universiteta. Seriya: Est-*

- estvenno-matematicheskie i tehicheskie nauki*. 2021. No. 2 (281), pp. 72–81. (In Russian)
10. **Sidorenko D. A., Fedotov E. A.** Some aspects of the use and programming the PPP protocol. *Vestnik nauki*. 2024. No. 12 (81), pp. 1643–1649. (In Russian)
 11. **Petrov N. V.** Modeling the operation of a RADIUS server in a telecommunications company. *Perspektivy razvitiya informacionnyh tehnologij*. 2013. No. 14. (In Russian)
 12. **Ometov A. Ya., Bezzateev S. V., Koucheryavy Y. A.** Authenticating electronic devices for temporary use: access rights management protocol. *St. Petersburg State Polytechnical University Journal. Computer Science. Telecommunications and Control Systems*. 2017. Vol. 10. No. 4, pp. 29–40. DOI: 10.18721/JCSTCS.10403. (In Russian)
 13. **Chekmarev D. Yu. Borzenkova S. Yu., Baranova E. M.** Methods of authentication and information protection at remote workplaces. *Izvestiya Tul'skogo gosudarstvennogo universiteta. Tehnicheskie nauki*. 2024. No. 3, pp. 111–113. (In Russian)
 14. **Balyuk A., Finko O.** Information security of cyber-physical systems: authentication of digital twins. *Voprosy kiberbezopasnosti*. 2022. No. 5 (51), pp. 100–113. DOI: 10.21681/2311-3456-2022-5-100-113. (In Russian)
 15. **Golovnyak P. A., Zaytsev K. S., Pinchuk A. M.** Development of an authentication method for running apache spark tasks in the apache airflow. *International Journal of Open Information Technologies*. 2022. Vol. 10. No. 8, pp. 94–101. (In Russian)

СВЕДЕНИЯ ОБ АВТОРАХ / INFORMATION ABOUT AUTHORS

СИОТАНОВ Алексей Максимович – студент, Санкт-Петербургский политехнический университет Петра Великого, Россия, 195251, Санкт-Петербург, ул. Политехническая, д. 29
E-mail: siotanol.am@edu.spbstu.ru
ORCID: 0009-0009-2388-9467

SIOTANOV Alexey M. – Student, Peter the Great St. Petersburg Polytechnic University, Russia, 195251, St. Petersburg, Polytechnicheskaya str., 29

МАКАРОВ Александр Сергеевич – старший преподаватель, Санкт-Петербургский политехнический университет Петра Великого, Россия, 195251, Санкт-Петербург, ул. Политехническая, д. 29
E-mail: makarov_as@spbstu.ru
ORCID: 0009-0008-0063-9572

MAKAROV Alexander S. – Senior Lecturer, Peter the Great St. Petersburg Polytechnic University, Russia, 195251, St. Petersburg, Polytechnicheskaya str., 29