“Фан, таълим ва ишлаб чиқариш интеграциясида рақамли иқтисодиёт истиқболлари” республика илмий-техник анжуман, ЎзМУ Жиззах филиали, 5-6 май 2021 йил, Жиззах – 182-185 б.

4. Ахатов А.Р., Улугмуродов Ш.А., Умаров Х.А. Разработка методов и алгоритмов системы генерации речи по данным сенсорных устройств считывания с элементами искусственного интеллекта // «Zamonaviy tadqiqotlar, innovatsiyalarning dolzarb muammolari va rivojlanish tendensiyalari: yechimlar va istiqbollar» Respublika ilmiy-amaliy konferensiya to‘plami, O‘zMU Jizzax filiali, Jizzax - 2021-yil 29-30-oktabr – 56-60 б.

5. Ахатов А.Р., Улугмуродов Ш.А. Development of methods and algorithms for a speech generation system based on data from sensor reading devices with elements of artificial intelligence // «Zamonaviy tadqiqotlar, innovatsiyalarning dolzarb muammolari va rivojlanish tendensiyalari: yechimlar va istiqbollar» Respublika ilmiy-amaliy konferensiya to‘plami, O‘zMU Jizzax filiali, Jizzax - 2021-yil 29-30-oktabr – 60-65 б.

6. Akhatov A.R., Nazarov F. Rashidov A. Mechanisms of Information Reliability In big data and Blockchain Technologies. // International conference on information science and communications technologies: applications, trends and opportunities 4-6 November. ICISCT 2021(IEEE).

7. Ruzibaev O., Muhamediyeva D., Ismailov I. Selecting a Suitable Initial Approximation Of Multi-Component Cross-Diffusion Systems //2021 International Conference on Information Science and Communications Technologies (ICISCT). – IEEE, 2021. – С. 1-4.

8. D. Khasanov, M. Tojiyev and O. Primqulov, "Gradient descent in machine learning," 2021 International Conference on Information Science and Communications Technologies (ICISCT), 2021, pp. 1-3, doi: 10.1109/ICISCT52966.2021.9670169.

ИСПОЛЬЗОВАНИЕ ОДНОРАЗОВЫХ ПАРОЛЕЙ ДЛЯ ОДНОГО СЕАНСА АУТЕНТИФИКАЦИИ

*Арзиева Жамила Тилеубаевна - PhD., доцент
Каракалтакский государственный университет им. Бердаха, г. Нукус
(кафедра «Прикладная математика и информатика»)*

Аннотация: В работе рассматривается преимущество одноразового пароля по сравнению со статическим, что пароль невозможно использовать повторно. Защищает от атак, основанных на активном вмешательстве в канал связи, используемый для аутентификации.

Ключевые слова: Одноразовый пароль, атака, технология, алгоритмы OTP ([англ. one time password, OTP](#)), математический алгоритм, злоумышленник.

Одноразовый пароль ([англ. one time password, OTP](#)) — это пароль, действительный только для одного сеанса [аутентификации](#). Действие одноразового пароля также может быть ограничено определённым промежутком времени. Преимущество одноразового пароля по сравнению со статическим состоит в том, что пароль невозможно использовать повторно. Таким образом, злоумышленник, перехвативший данные из успешной сессии аутентификации, не может использовать скопированный пароль для получения доступа к защищаемой информационной системе. Использование одноразовых паролей само по себе не защищает от атак, основанных на активном вмешательстве в канал связи, используемый для аутентификации (например, от атак типа [«человек посередине»](#)) [1]. Человек не в состоянии запомнить одноразовые пароли. Поэтому требуются дополнительные технологии для их корректной работы.

Алгоритмы создания OTP обычно используют случайные числа. Это необходимо, потому что иначе было бы легко предсказать последующие пароли на основе знания

предыдущих. Конкретные алгоритмы ОТР сильно различаются в деталях. Различные подходы к созданию одноразовых паролей перечислены ниже.

- Использующие математические алгоритмы для создания нового пароля на основе предыдущих (пароли фактически составляют цепочку, и должны быть использованы в определённом порядке).
- Основанные на временной синхронизации между сервером и клиентом, обеспечивающей пароль (пароли действительны в течение короткого периода времени)
- Использующие математический алгоритм, где новый пароль основан на запросе (например, случайное число, выбираемое сервером или части входящего сообщения) и/или счётчике [1,2].

Также существуют различные способы, чтобы сообщить пользователю следующий пароль. Некоторые системы используют специальные электронные токены, которые пользователь носит с собой, создающие одноразовые пароли и выводящие их на маленьком экране. Другие системы состоят из программ, которые пользователь запускает с мобильного телефона. Ещё другие системы генерируют одноразовые пароли на сервере и затем отправляют их пользователю, используя сторонние каналы, такие, как SMS-сообщения. Наконец, в некоторых системах одноразовые пароли напечатаны на листе бумаги или на скретч-карте, которые пользователю необходимо иметь с собой. Один подход, разработанный Лесли Лэмпортом ([англ. Leslie Lamport](#); - американский учёный в области информатики, первый лауреат [премии Дейкстры](#). Разработчик [LaTeX](#) - популярного набора макрорасширений системы компьютерной вёрстки [TeX](#), исследователь теории [распределённых систем](#) и вопросов синхронизации процессов во взаимодействующих системах. Лауреат [Премии Тьюринга](#) 2013 года), использует одностороннюю функцию (назовём её f). Система одноразовых паролей начинает работать от начального числа s , затем генерирует пароли

$$f(s), f(f(s)), f(f(f(s))), \dots$$

столько раз, сколько необходимо. Если ищется бесконечная серия паролей, новое начальное число может быть выбрано после того, как ряд для s оказывается исчерпанным. Каждый пароль распределяется в обратном порядке, начиная с $f(f(\dots f(s)\dots))$, заканчивая $f(s)$ [3]. Если злоумышленнику удаётся получить одноразовый пароль, он может получить доступ только на один период времени или одно соединение, но это становится бесполезным, когда этот период закончится. Чтобы получить следующий пароль в цепочке из предыдущих, необходимо найти способ вычисления обратной функции f^{-1} . Так как f была выбрано односторонней, то сделать это невозможно. Если f -криптографическая хеш-функция, которая обычно используется, то, насколько известно, это будет вычислительно неосуществимая задача [1,3].

ЛИТЕРАТУРА

1. Karimov, M.M, Khudoykulov, Z.T, Arzieva, J.T A Method of Efficient OTP Generation Using Pseudorandom Number Generators International Conference on Information Science and Communications Technologies: Applications, Trends and Opportunities, ICISCT 2019 this link is disabled, 2019, 9011825
2. Tashev, K.A, Khudoykulov, Z.T, Arzieva, J.T Improvement of a security enhanced one-time mutual authentication and key agreement scheme International Journal of Innovative Technology and Exploring Engineering this link is disabled, 2019, 8(12), стр. 5031–5036
3. *Oded Goldreich*. Volume 1, Basic Tools // [Foundations of Cryptography](#). - [Cambridge University Press](#), 2001. — [ISBN 0-521-79172-3](#).