**Висоцька О.О., Цевельов Є.О.**

*Національний авіаційний університет, Київ, Україна*

# Удосконалена система автентифікації в організації з використанням віддаленого доступу

**Вступ.** На сьогоднішній день, під час світової пандемії, велика кількість користувачів корпоративної системи працює з дому. Для зручного доступу користувачів використовується віддалений доступ до системи. Це сприяє зросту потенційних загроз для цих систем.

У зв'язку з цією ситуацією потрібно застосовувати методи захисту для корпоративних мереж з використання віддаленого доступу. Одним з надійних методів забезпечення захищеного віддаленого доступу до мережі є використання автентифікації. Такий метод дає можливість дати доступ лише конкретній особі, що володіє певними даними для доступу.

**Актуальність**. Сьогодні часто постає питання про безпеку інформації. Проблеми, які постали через ситуацію в світі, є критичними, а вдосконалення механізмів вирішення цих проблем є необхідним для забезпечення безпечного віддаленого доступу. Вирішення цієї проблеми – удосконалення системи автентифікації.

**Постановка задачі.** Якщо не встановлено безпечної системи автентифікації, є ризик, що зловмисник отримає доступ до інформації організацій. Тому потрібно розробити метод для мінімізації даних ризиків.

**Мета.** Аналіз систем автентифікації, які забезпечать захищений віддалений доступ до системи, за рахунок сучасних засобів автентифікації.

**Викладення матеріалу.** Так як, на сьогоднішній час виникла потреба в віддаленому доступі для робітників в організації, через пандемію, створюються системи автентифікації користувачів. Основним завданням таких систем є перевірка даних користувача для отримання доступу до інформації. Віддалена робота ґрунтується на обміні діловими даними або послугами за межами корпоративної інфраструктури, як правило, через Інтернет. Цього можна досягти за допомогою різноманітних клієнтських пристроїв, у тому числі багатьох, які

перебувають поза контролем організації. Віддалене середовище, в якому використовуються ці пристрої, також може становити небезпеку. Наприклад, проблеми безпеки можуть існувати навколо: відсутність засобів фізичного захисту – створює ризик втрати або крадіжки пристрою підслуховування – під час проходження інформації через загальнодоступний Інтернет несанкціонований доступ до систем або даних – можливо, з видом на екран моніторинг та маніпулювання даними – якщо хтось отримає доступ до пристрою Ви можете адаптувати більшість поширених заходів кібербезпеки для вирішення унікальних проблем безпеки віддаленого доступу.

Хоча автентифікація є лише одним аспектом кібербезпеки, це перша лінія захисту. Це процес визначення того, чи є користувач тим, за кого він себе видає. Існує багато технологій автентифікації, починаючи від паролів і закінчуючи відбитками пальців, для підтвердження ідентичності користувача перед наданням доступу. Це додає захисту та запобігає порушенням безпеки. Хоча часто поєднання різних типів автентифікації забезпечує надійне посилення системи від можливих загроз.

В інформаційних технологіях використовується такі види автентифікації:

1) однофакторна автентифікація;
2) технологія єдиного входу;
3) багатофакторна автентифікація.

Завдяки системі єдиного входу користувачам потрібно лише увійти в одну програму і, таким чином, отримати доступ до багатьох інших програм. Цей метод є більш зручним для користувачів, оскільки він знімає обов’язок зберігати кілька наборів облікових даних та створює більш безперебійний досвід під час оперативних сеансів.

Для того щоб забезпечити як великі, так і малі організації повним захистом їх даних при використанні віддаленого доступу, їм необхідно гарантувати, що корпоративні користувачі і стратегічні партнери були надійно ідентифіковані, їх доступ до мереж повинен бути безпечним, а використовувані інформаційні канали віддаленого доступу захищені належним чином.

Проаналізувавши сучасні засоби автентифікації, зрозуміло що вони мають певні недоліки. Також стало відомо, що проблеми забезпечення конфіденційності та цілісності інформації вирішуються за допомогою шифрування даних при відправці їх на сервер, але є можливість втрати ключа.

Керуючись інформацією, що наведено вище, можна визначити що для удосконалення системи автентифікації потрібно:

- аналіз вразливостей віддаленого доступу;
- дослідження принципів використання віддаленого доступу;
- проведення аналізу видів та способів автентифікації;
- аналіз вразливостей вибраного методу;
- розробка удосконаленої системи автентифікації з віддаленим доступом;
- наведення рекомендацій, що до використання системи автентифікації.

**Список використаної літератури.**


1. Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации. – М.: Яхтсмен, 1996. – 192 с.
2. Гайкович В.Ю., Ершов Д.В. Основы безопасности информационных технологий. М.: МИФИ, 1995. – 285с.
3. Самохвалов Ю.Я., Темпіков В.О., Хорошко В.О. Організаційно-технічне забезпечення захисту інформації: Навчальний посібник / За ред. проф. Хорошка В.О. – К.: НАУ, 2002. – С. 207
4. С.Н. Ардатский, О.С. Бартунов Управление доступом в сложных информационных системах. – Образовательные порталы России. Выпуск 1. - 2005.-187 с