Лекция 04.10.23

1. Чем отличается процедура идентификации от аутентификации?

Идентификация – процедура присвоения идент-ра (ID) и в дальнейшем процедура распознавания этого идент-ра из заданного перечня идент-ров. Аутентификация – процедура проверки подлинности носителя названного идент-тора.

2. Что такое авторизация?

Авторизация – предоставление доступа к какому-либо ресурсу (напр., к электр. почте).

3. Кем была построена теория аутентификации?

3. Кем была построена теория аутентификации?

Теория аутентификации была построена Густавусом Джеймсом Симмонсом в 1985 году.

4. Как влияет на избыток инф-ции усиление аутентификации?

При усилении аутентификации увеличивается количество избыточной информации, которую должен представить пользователь.

5. Как влияет на избыток информации усиление конфиденциальности?

Аналогично: при усилении конфиденциальности увеличивается избыток информации.

6. Кто первым догадался, что при аутентификации на входе в систему не обязательно хранить пароли пользователей?

Первыми догадались Майк Гай и Роджер Нидхем в 1967 г.

пользователей?

Первыми догадались Майк Гай и Роджер Нидхем в 1967 г.

7. Что такое привязка к паролю?

Привязка к паролю (salt) – случайная строка, которая конкатенируется с паролями перед их обработкой односторонней функцией.

8. Какой атаке противостоит протокол аутентификации на входе с использованием открытого ключа?

Данный протокол противостоит атаке „человек посередине": когда Алиса посылает свой пароль Хэшу, пароль может прочесть любой, у кого есть доступ к маршруту прохождения данных, т.е. Ева может узнать пароль до его хэширования Хэшем.