- репрезентативна – функція, яка визначає мовної акт в його відношенні до референту або предмету думки;

- метаязикова – функція тлумачення мовних фактів;

- естетична – функція естетичного впливу, проявляється в тому, що кажуть починають помічати сам текст, його звукову та словесну фактуру.

Чіткі синтаксичні, століттями відпрацьовані, відшліфовані структури накладаються на аморфну думка, і це надає їй чіткість, виникає можливість для сприйняття цієї думки іншими людьми; так досягається розуміння як співвідношення слів і мовних структур із зразками, що зберігаються в мовної пам'яті слухача [3].

На основі усього вищевикладеного можна зробити висновок, що мовна сторона комунікації має складну багатоярусну структуру і виступає в різних стилістичних різновидах: різні стилі і жанри, розмовний і літературний мова, діалекти і соціолекти тощо. Всі мовні характеристики та інші компоненти комунікативного акту сприяють його успішній або неуспішній реалізації. Говорячи з іншими, з великого поля можливих засобів мовної комунікації вибираються ті кошти, які здаються найбільш підходящими для вираження думок в дані ситуації. Це – соціально значущий вибір. Процес цей і нескінченний, і нескінченно різноманітний. При цьому основною одиницею мови є мікротекст (складне синтаксичне ціле), який має свій особливий лінгвістичний статус.

Список використаних джерел:

1. Андріанов М.С. Невербальна комунікація. М.: Ін-т загальногуманітаних досліджень, 2007. 256 с.

2. Атватер И. Я вас слушаю. – М.: Изд-во «Экономика»,1988. – 111 с.

3. Василик М.А. Основи теорії комунікації: підручник. М.: Гардарики, 2003. С. 600-605.

4. Клюєв Є.В. Мовна комунікація. М.: Рипол Класик, 2002. 320 с.

5. Садохин А.П. Введення в теорію міжкультурної комунікації М.: Вища. шк., 2005. С. 125-127.

6. Якупов П.В. Комунікація: визначення поняття, види комунікації та її бар'єри. Вісник університету. 2016. № 10. С. 261-266.

Шульженко К.С.

студентка;

Артемчук Л.М.

кандидат педагогічних наук, доцент,

Національний університет біоресурсів і природокористування України

ЗАХИСТ ІНФОРМАЦІЇ В СОЦІАЛЬНИХ МЕРЕЖАХ

На сьогодні більшість людей не можуть уявити своє життя без соціальних мереж. Сотні мільйонів користувачів кожного дня приділяють чимало часу для мереж на зразок Однокласники, Вконтакте, Instagram, Facebook чи YouTube.

Користувачі спілкуються між собою, обмінюються повідомленнями, фотографіями, аудіо- та відеоматеріалами, діляться своїми враженнями, дізнаються багато нового та слідкують за новинами. Але, частіше всього, саме в соціальних мережах ми можемо стати жертвою шахраїв. Адже для того щоб зареєструватися користувач має надати досить широку інформацію про себе і навіть своїх друзів та родичів. Але багато хто навіть не задумується про необхідність забезпечення собі та своїм рідним просту конфіденційність. Тому в цій статті розглянемо, яким чином захистити свою інформацію та убезпечити себе від її витоку, користуючись соціальними мережами.

Одним з найголовніших кроків є створення надійного пароля. Адже існує безліч способів як захопити аккаунт. Наприклад, через підбір пароля. Тому що дуже часто при реєстрації користувачі вводять дуже прості паролі які складаються, з власного ім’я і дати народження. Знаючи такі дані і використавши спеціальні програми підібрати пароль зовсім не важко,потрібно лиш трохи часу. Тому щоб максимально убезпечити себе від такої ситуації потрібно використовувати безпечні паролі які мають не менше ніж 8 символів і складаються з великих і маленьких літер, цифр і символів на зразок – #, %, $, @. У багатьох мережах можна відновити пароль відповівши на секретне питання. Наприклад, таке як дівоче прізвище матері чи бабусі. Такою інформацією може володіти багато ваших знайомих, тому потрібно ставити таке секретне питання, відповідь на яке знатимете тільки ви.

Також дуже важливо захистити всій комп’ютер, ноутбук, планшет чи телефон від вірусів. Програми які працюють на комп'ютері користувача можуть отримати доступ до різних даних, в тому числі і до паролів, файлів cookie. Тому якщо в такі програми проникне вірус вони можуть збирати інформацію та відправляти її через інтернет-зловмисникам. Захист у даному випадку звичайно встановити антивірус,бажано ліцензійний і вчасно його оновлювати. Також віруси можуть розсилати електронною поштою у вигляді вкладень і можна заразити свій комп'ютер перейшовши по посиланню в інтернеті. Тому ніколи не відкривайте повідомлення надіслане з невідомої вам адреси та одразу видаляйте їх. Деякі якісні віруси залишаються непоміченими антивірусами протягом багатьох місяців. Головне як тільки вірус дасть про себе знати необхідно одразу його знешкодити. Так що головний захист – обережність користувача.

Дуже важливо налаштувати конфіденційність. Адже багато користувачів не знають, що можуть змінити параметри конфіденційності і, якщо не зроблять цього, то їхні особисті дані будуть відкритими для суспільства. Більшість соціальних мереж дозволяють вибирати інформацію, якою ви хочете поділитися і хто може її бачити. Тобто що ви можете обмежити доступ до своєї біографії, фотографій, відео, повідомлень для певних людей або групи, ваших друзів і знайомих. Тоді ваша інформація не буде доступна для незнайомців та неприємних вам людей. Пам'ятайте, що налаштування конфіденційності можуть змінитися. Іноді вони можуть ставати більш надійними і детальними, а іноді – навпаки. Особливо звертайте увагу на ці зміни – раптом інформація,

яка була конфіденційною, раптово стала відкритою для всіх, або нові додаткові налаштування дозволять краще контролювати рівень вашої конфіденційності.

Також не можна розміщувати на сторінках день народження та ваш номер телефону. Можливо, ви ніколи не могли навіть подумати, що така проста інформація може вам зашкодити. Однак це може допомогти викрадачам захопити ідентифікаційні дані і тому не рекомендується показувати повну дату народження у вашому профілі а тільки місяць і день або взагалі нічого не вказувати. Ви можете змінити цю інформацію у Вашому профілі. Всім нам звичайно приємно коли на сторінках публікують привітання, але справжні друзі і так знають ваш День народження.

Отже, є дуже багато загроз інформаційній безпеці в соціальних мережах але це не означає, що треба боятися ними користуватися або одразу видаляти сторінку. Для безпечного користування слід думати яку інформацію про себе розміщати в соціальних мережах, не вказувати ні в якому разі особисті дані, інформацію, що стосується близьких людей, родичів, використовувати антивірусне програмне забезпечення на ПК,встановити безпечний пароль, який знаєте тільки ви. І головне пам’ятати що тільки від вас залежить безпека ваших даних.

Список використаних джерел:

1. Голубенко О.Л. Соціальні мережі як загроза безпеки [Електронний ресурс] / О.Л. Голубенко, А.С. Петров, А.О. Петров. – 2011. – Режим доступу до ресурсу: http://www.nbuv.gov.ua/old_jrn/Soc_Gum/VSUNU/2011_7/title/1.pdf.

2. Деркаченко А.Я. Соціальні мережі, як середовище для технологій маніпулятивного впливу [Електронний ресурс] / А.Я. Деркаченко. – 2016. – Режим доступу до ресурсу: http://journals.dut.edu.ua/index.php/dataprotect/article/view/531/493.

3. Карманний Є.В. Підходи до захисту інформації при користуванні соціальними мережами [Електронний ресурс] / Є.В. Карманний, С.О. Ковжога. – 2015. – Режим доступу до ресурсу: http://dspace.nlu.edu.ua/bitstream/123456789/8420/1/Karmannuy_Kovgoa.pdf.

4. Зайченко Ю.П. Комп'ютерні мережі: Навчальний посібник. – К.: Слово, 2003. – 286 с.