Міністерство освіти і науки України

Сумський державний педагогічний університет ім. А. С. Макаренка

Фізико-математичний факультет

Кафедра інформатики

УДК 378.016:51]:004

Юшко Катерина Сергіївна

ОСОБЛИВОСТІ НАВЧАННЯ УЧНІВ СТАРШИХ КЛАСІВ КРИПТОГРАФІЧНИХ МЕТОДІВ ЗАХИСТУ ДАНИХ В УМОВАХ ГУРТКОВОЇ РОБОТИ

Спеціальність: 014. Середня освіта (Інформатика)

Галузь знань: 01. Освіта

Кваліфікаційна робота

на здобуття освітнього ступеню магістра

Науковий керівник

_____А.О.Юрченко,

кандидат педагогічних наук,
доцент кафедри інформатики

«___» _____ 20__ року

Виконавець

_____К.С.Юшко

«___» _____ 20__ року

Суми – 2020

СПИСОК УМОВНИХ ПОЗНАЧЕНЬ

КМ – криптографічні методи

ЗІ – захист інформації

КМЗІ – криптографічні методи захисту інформації

ЗНЗ – загальноосвітній навчальний заклад

ПО – позашкільна освіта

ВСТУП

Актуальність. На сьогоднішній день гостро представлена проблема ЗІ. Питанням ЗІ, на сьогоднішній день, приділяється велика увага, і це не випадково. Телекомунікаційні системи, що активно розвиваються останнім часом, є артеріями сучасних глобальних інформаційних систем. Інформація, що циркулює в таких системах, становить суттєву цінність і тому є вразливою до різного роду зловживань. Тому саме в останні десятиліття стала настільки актуальною проблема ЗІ.

КМ, що спрямовані на ЗІ, займають одне з передових місць в сфері ЗІ в цілому. Їх особливість полягає в незалежності від властивостей матеріальних носів інформації, а орудують лише її характеристиками.

Оскільки в сьогоденні комп'ютерні технології застосовуються в кожній сфері діяльності, без виключень, і приріст інформаційного оснащення зростає з кожним днем – стрімко зростає і попит на вивчення криптографії. На відміну від апаратних криптосистем, програмні засоби набули більшого застосування, адже немає потреби в великих фінансових витратах. Проблема реалізації КМ завжди залишатиметься актуальною, проте саме такі методи гарантують повний захист даних.

Середня освіта не є виключенням, щодо важливості змістової лінії «КМЗІ», проте оскільки навчальна програма не передбачає введення даного курсу, то приділяється увага позакласній діяльності, в даному випадку – гуртковій роботі. В період сучасної інформатизованої освіти, підвищення ефективності освіти завжди передбачає введення нових форм до процесу навчання учнів.

Об'єкт дослідження. Процес навчання інформатики учнів в старших класах.

Предмет дослідження. Особливості навчання учнів старших класів криптографічних методів захисту даних в умовах гурткової роботи

Мета: визначити особливості навчання учнів старших класів криптографічних методів захисту даних в умовах гурткової роботи.

Відповідно до мети були поставлені такі **завдання** дослідження:

1) Описати сутність криптографічних методів захисту даних;

2) Описати вимоги до підготовки учнів з уроків інформатики;

3) Охарактеризувати особливості навчання інформатики в умовах гурткової роботи;

4) Розробити план роботи гуртка з вивчення криптографічних методів захисту даних та його методичний супровід.

Практичне значення: результати роботи можуть бути використанні під час проведення гурткової роботи з курсу «Криптографічні методи захисту інформації», як додатковий матеріал для вчителя.

Кваліфікаційна робота складається зі вступу, трьох розділів, висновків, додатків та списку використаних джерел.

У вступі обґрунтовано вибір теми дослідження, актуальність, визначено об’єкт, предмет, мету та завдання.

У першому розділі «Криптографічні методи захисту інформації» розглянуто теоретичний аспект з теми КМЗІ, витяги з Законів Украни, щодо ЗІ, історія криптографії.

У другому розділі «Навчання інформатики в умовах гурткової роботи» описано вимоги до обох сторін навчального процесу(«учень-вчитель»), описано сучасні форми навчання, доцільність використання гурткової роботи для вивчення теми КМЗІ у старшокласників.

У третьому розділі «Опанування криптографічних методів захисту інформації учнями старших класів в умовах гурткової роботи» розписано план гурткової роботи, цілі його проведення; наведено приклад у вигляді конспекту урока.

Апробація роботи: Матеріали прийнято на V Міжнародна науково-практична конференція “Study of modern problems of civilization”, 19-23 Жовтня, Осло, Норвегія.; XI Міжнародна науково-практична конференція “Academic research in multidisciplinary innovation”, 30.10 – 03.11 2020 р., Амстердам, Нідерланди.

РОЗДІЛ 1. КРИПТОГРАФІЧНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ ТА ЇХ ПРАКТИЧНА РЕАЛІЗАЦІЯ

1.1. Захист інформації в умовах розвитку інформаційного суспільства

Для аналізу роботи, що стосується ЗІ, необхідно повністю орієнтуватися в поняттях, що стосуються вищезгаданої теми.

Звернувшись до основного закону, що регулює порядок поводження з персональними даними на території України, Закону України №2297 від 01.06.2010 р. «Про захист персональних даних», виділимо основні теоретичні аспекти.

Означення 1.1.1. Обробка персональних даних – будь–яка дія або їх сукупність, таких як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення персональних даних, у тому числі з використанням інформаційних (автоматизованих) систем [1].

Надалі, під персональними даними вважатимемо певні відомості, про ідентифіковану людину.

Аналізуючи той же документ, спостерігаємо, що будь–яка обробка персональних даних без згоди фізичної особи, крім випадків, які передбачені законом – пряме порушення Законодавства України, за що прописано в даному законі, адже персональні дані – інформація обмеженого доступу.

Розуміючи, що інформація – будь–які відомості чи повідомлення, знання чи вміння, перейдемо до розгляду наступних її характеристик.

Інформацію, відносно інформаційних систем, можна охарактеризувати за такими показниками, як:

1. Надійність. Характеризується поведінка системи як в нормальному, так і в позаштатному станах, відповідно до запланованої.

2. Точність. Характеризується повне виконання всіх необхідних команд системи.

3. Контроль доступу. Гарантія різного доступу для різних груп осіб, та постійного виконання таких обмежень.

4. Контрольованість. Гарантія можливості повної перевірки довільного компоненту систему в будь–який момент..

5. Контроль ідентифікації. Гарантія ідентифікації клієнта, що підключений до системи.

6. Стійкість до навмисних збоїв. Характеризується поведінка системи при навмисних правках (внесених помилках).

Порушення будь–якої з вищевказаних характеристик потребує коригування системи.

Відносно інформаційної безпеки, інформація має наступні властивості:

1. Конфіденційність. Властивість визначається тим, чи доступна інформація комусь, окрім того кола осіб, для яких вона призначалася. Порушення конфіденційності – «*розкрадання*».

2. Цілісність. Визначається гарантія початкового стану інформації, без сторонньої обробки – не було застосовано несанкціонованих змін. Порушення цілісності – *«фальсифікація повідомлення»*.

3. Автентичність. Гарантія авторства – чи є автором той, хто ним зазначений. Порушення автентичності – *«фальсифікація авторства».*

4. Неспростовність. Дана властивість майже ідентична попередній, відміна в тому, що при заміні, видачі чужої інформації за власну, сам автор відмовляється від авторства.

Означення 1.1.2. Загроза безпеки інформації – сукупність умов та факторів, що створюють потенціальну або реальну загрозу порушення безпеки інформації [2].

Залежно від того, як якого характеру відбувався вплив на інформацію, з подальшим її пошкодженням, класифікують штучні та природні загрози інформаційної безпеки (Рис.1.1.1.):

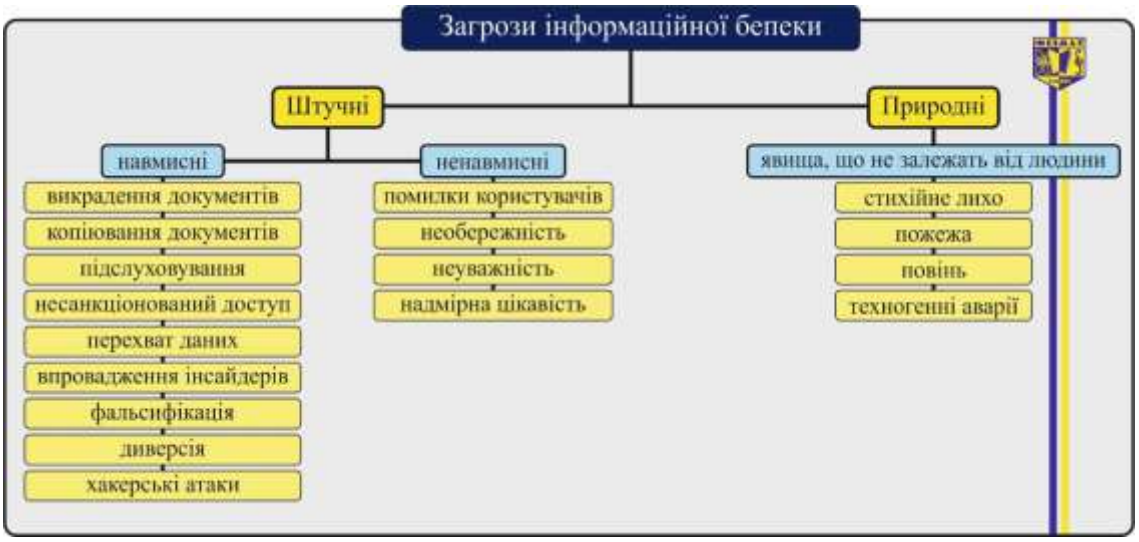

Рис.1.1.1. Класифікація загроз інформаційної безпеки

1. Штучні. Небезпека щодо інформаційної безпеки з боку стороннього користувача.

2. Природні. Загроза з боку явищ, що не залежать від людини.

На сьогоднішній день, спеціалісти області ЗІ, класифікуючи ряд методів для її захисту, виділяють наступні: організаційні, криптографічні, програмні та технічні (Рис.1.1.2.)[3,4].

Рис.1.1.2. Класифікація методів ЗІ

Організаційні методи ЗІ поділяються на чотири підгрупи:

1. Законодавчі. Направлені на застосування законодавчіх актів, що визначають, в свою чергу, права та обов’язки осіб, як фізичних так і

юридичних. Законодавчі методи ЗІ також регламентують права та обов'язки держави [5,6].

2. Адміністративні. Направлені на створення відповідної секретності, її режиму [7].

3. Морально–етичні. Підтримка моральної атмосфери, де негативно оцінюється порушення правил, а дотримання – сприяє ЗІ [8].

Криптографічні методи ЗІ націлені на використання шифрування або кодування інформації, за для уникнення несанкціоноваго доступу до неї сторонніми особами [9,10].

Технічні методи ЗІ застосовують електричні чи інші пристрої при функціонуванні [11].

В *програмних* методах ЗІ використовуються програмні засоби при розмежуванні доступу до потрібної інформації [5].

Всі вищезгадані методи націлені на зберігааня основних властивостей інформації: конфіденційність, цілісність, автентичність, неспростовність.

Як було зазначено, вирішенням проблеми ЗІ шляхом її перетворення займається криптографія.

Означення 1.1.3. Криптографія — наука, що займається вивченням всіх математичних методів забезпечення конфіденційності (неможливості прочитання інформації несанкціонованим) і автентичності (цілісності і дійсності авторства) інформації [12].

Варто зазначити зворотню науку до криптографії – криптоаналіз.

Означення 1.1.4. Криптоаналіз – наука, що займається вивченням методів дешифрування, без використання ключа [13].

Іншими словами, криптоаналіз – наука про взлом шифру, за для несанкціонованого доступу до потрібної інформації.

Криптографія та криптоаналіз вивчають одні й ті ж самі об'єкти (ЗІ), проте з різних сторін, якщо перша вичає його дотримання, то інша – всі шляхи несанкціонованого доступу до довільної зашифрованої інформації.

Криптографія та криптоаналіз є складовими науки, що вивчає всі методи захисту та взлому інформації – криптології.

В КМ захисту мета здійснюється за допомогую певного шифрування, тобто перетворення, що роблять вхідні дані важкозчитуваними без знання спеціальної інформації – ключа, пд яким розуміємо легкозмінну частину певної криптосистеми, що визначає яке саме перетворення, з усіх можливих, виконується в даний момент.

Забезпечення того, що ключ залишається таємним, має першорядне значення для забезпечення безпеки зашифрованої інформації, яка повинна залишатися прихованою. З появою комп'ютерної криптографії ключі тепер представляються у вигляді великих, майже випадкових рядків букв і цифр, таких як 2b7e151628aed2a6abf7158809cf4f3c (це число, як правило, буде набагато більше). Різні методи шифрування та дешифрування володіють різними властивості.

Означення 1.1.5. Криптосистема (система шифрування) – сукупність ірофамних та апаратних засобів та інструкцій, алгоритмів, призначених як для шифрування так і для зворотнього процесу – дешифрування, що дозволяють спочатку шифрувати, і внаслідок розшифровувати текст [14].

Криптосистема (алгоритм), в залежності від кількості наявних ключів, поділяється на симетричну та асиметричну.

1. Симетрична криптосистема. Вид кодування, в якому і для кодування, і для декодування використовується один блок інформації (ключ) та один алгоритм кодування.

В даному випадку ключ (K) – секретний, закритий. Ключ важливо регулярно змінювати, щоб уникнути несанкціонованого доступу до відправної інформації. Проте необхідно мати надійний спосіб (механізм) передачі ключа між відправником і отримувачем [15,16].

2. Асиметрична криптосистема. Спосіб кодування, де для шифрування даних використовується один ключ ($К_1$), а для дешифрування інший ($К_2$).

У випадку асиметричної криптосистеми, один з ключів ($К_1$), може бути відкритим, тобто доступним будь–якому користувачеві, проте інший ($К_2$) – засекречений. Перший ключ ($К_1$) шифрує відкриту інформацію, другий ($К_2$), відомий лише отримувачу, використовується ним для дешифрування [16].

Враховуючи наявність самого ключа, алгоритми поділяють на тайнопис та криптографію з ключем («with a key»).

1. Тайнопис. Всі перетворення над інформацією відомі лише відправнику та одержувачу. Алгоритм шифрування нікому сторонньому недоступний.

2. Криптографія «with a key». Алгоритм залежить від параметру – ключа, доступного відправнику та одержувачу, проте сам алгоритм доступний стороннім.

В залежності від того, які дії були проведені над текстом (характер впливу) алгоритми криптосистеми поділяються на перестановочні та символьні [15].

1. Перестановки. Всі структурні блоки інформації не змінюють зміст, але змінюють своє положення, порядок їх проходження. Внаслідок цього інформація недоступна сторонньому обличчю.

2. Символи. Блоки змінюються в залежності від законів певного криптоалгоритму.

В залежності від розміру оригінального блоку інформації, алгоритми криптосистеми розділяють на потокові та блокові.

1. Потокові. Одиницею кодування таких алгоритмів є біт. Представлена система застосовується в тому випадку, коли передача інформації може починатися та закінчуватись в довільний момент часу, випадково порушуватись, перериватись. Результат всього кодування не має залежності від вхідного потоку інформації.

2. Блокові шифри. Одиниця такого кодування – блок, що містить декілька байтів. Запропонована система застосовується у випадку пакетної передачі довільної інформації. Результат блокового кодування завжди залежить від всіх вихідних байтів [15,16].

Як підсумок, можна сказати, що всі схеми класифікації, засновані на окремих характеристиках чи властивостях, характерній групі ознак, тому, один й той же криптоалгоритм може відноситись (проходити) одночасно за декількома схемами класифікації, та опинятись в кожній класифікації, в будь–якій з підгруп. Враховуючи, вищеперераховані класифікації, створимо загальну класифікацію всіх криптографічних алгоритмів (Рис. 1.1.3).

Рис.1.1.3. Класифікація криптографічних алгоритмів

Досить часто трапляється ситуація, як у випадку асиметричних криптосистем, що ключ також потрібно змінити за певним алгоритмом, для цього існує хешування.

Означення 1.1.5. Хеші – це математичні функції або рівняння, які «зчитують» частину інформації (наприклад, файл) і видають набір цифр і букв, унікальних для введення [17].

Означення 1.1.6. Хешування – це процес перетворення заданого ключа в інший, який має інакше значення [17].

Хеш–функція використовується для генерації нового значення відповідно до математичного алгоритму. Результат хеш–функції відомий як хеш–значення або просто хеш (Рис.1.1.4).

Рис.1.1.4. Принцип роботи хеш–функції

Якісна хеш–функція використовує односторонній алгоритм хешування, або іншими словами, хеш не може бути перетворений назад у вихідний ключ (Рис.1.1.5.).

Рис.1.1.5.Якісний результат роботи хеш–функції

Існують випадки, коли два ключі можуть генерувати однаковий хеш. Це явище відоме як зіткнення (Рис.1.1.5).

Рис.1.1.6. Процес «зіткнення»

Хешування переважно використовується для реалізації хеш–таблиць. Хеш–таблиця зберігає пари «ключ/значення» у вигляді списку, де будь–який елемент можна отримати за допомогою його індексу [17].

Оскільки кількість пар «ключ/значення» не обмежена, ми можемо використовувати хеш–функцію, щоб зіставити ключі з розміром таблиці → хеш–значення стає індексом для даного елемента.

Подібно до шифрування, існують різні алгоритми хешування з унікальними характеристиками. Наприклад, використовуючи алгоритм хешування SHA–256, слово «університет» хешує до:

«de3923e3f14caa7a19259b80f1b980d126d668c2745ef7ac8e5f231f41861981»

Але при використанні одного і того ж алгоритму та введенні слова «університети» (зауважте, що різниця лише в одну букву), результат зовсім інший:

«4e35f62b9a0028f3a8f19bfe65d8547a67c1b4556a34c9a78ee5021684c6ab38»

У цьому полягає сенс хешів – виявлення змін. Файл будь–якого розміру може бути переданий через алгоритм хешування, навіть великі та складні комп'ютерні програми.

1.2. Ретроспективний аналіз криптографічних методів захисту інформації

Аналізуючи історію криптографії, спостерігаємо виділення трьох основних етапів її розвитку (Рис.1.2.1).

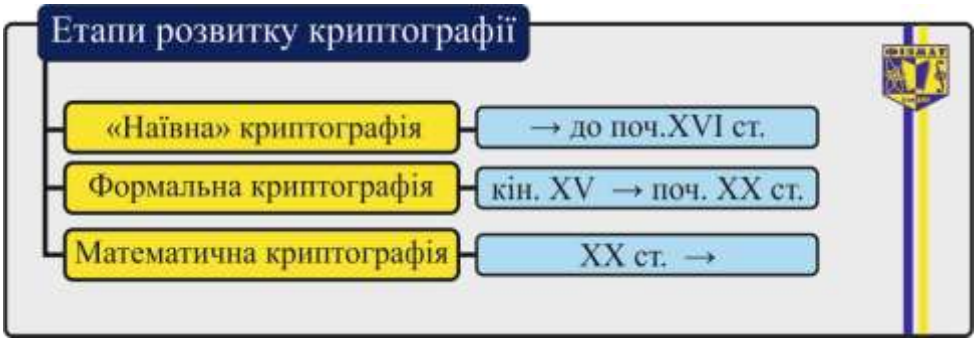

Рис.1.2.1. Етапи розвитку криптографії

1. «Наївна» криптографія. Ще в стародавні часи збереженню важливої інформації надавали великого значення, та зберігали її в таємниці від сторонніх

осіб. В часи, коли лише з’явилася писемність, з’явилася і необхідність захищати нову інформацію від небажаного прочитання. Оскільки йдеться про початок самої писемності, то будь–які написи вважалися криптографію в оригінальному вигляді, адже володіли майстернісю письма одиниці.

З часом, коли писемність почала набирати більшого оберту, почала формуватися в якості самостійної науки і криптографія. Ще в таких стародавніх цивілізаціях як Месопотамія, Індія та Єгипет були відомості про шифрування листів, їх систематизація[18].

Для періоду «наївної» криптографії було наявне широке застосування всіх відомих способів обману противника щодо змісту переданих повідомлень. На першому етапі для захисту довільного повідомлення чи інформації використовували методи кодування і стеганографії, які були дотичні, але не тотожні до криптографії. Шифрувальні системи зводилися до використання перестановки або заміни букв на різні символи (інші букви, знаки, малюнки, числа і т.п.). Одні і ті ж методи шифрування використовувалися повторно, ключі були короткими, використовувалися примітивні способи перетворення вихідної інформації в зашифроване повідомлення. Це дозволяло за єдиним встановленим алгоритмом шифрування, швидко розшифровувати інші повідомлення.

Точний час виникнення цих способів обміну таємною інформацією губиться в глибині століть, і встановити його неможливо. Історики вважають, що перші протокриптографічні прийоми з'явилися в Стародавньому Єгипті близько 4 тис. років тому. Писарі, що складали життєпис правителів, прагнули надати стандартним ієрогліфам незвичайний вид на пам'ятниках і гробницях (Рис.1.2.2), щоб надати написам менш звичайний і більш шанобливий стиль. Жерці користувалися цим же прийомом при переписуванні релігійних текстів, щоб ті виглядали для мирян загадковіше і солідніше. Такі «переклади» ставали все менш зрозумілими простому люду, який в результаті опинявся у все більшій залежності від жерців [19].

Рис.1.2.2. Фрагмент східної стіни гробниці Хнумхотепа II «Ловля птахів сіткою»

По мірі розвитку єгипетської цивілізації ширилося використання ієрогліфів. Зі збільшенням кількості написів, що висікали на стінах храмів, люди втрачали до них інтерес. Єгиптологи вважають, що писарі тоді стали ще більше видозмінювати деякі знаки в прагненні пробудити цікавість і привернути увагу населення. Ці модифікації жодним чином не були кодами або шифрами, але вони містили в собі два основних принципи криптології, а саме: зміну листа і приховування його сенсу. Безперечних доказів, що вказують на широке використання модифікацій ієрогліфів для приховування дипломатичних, торговельних або військових планів в Стародавньому Єгипті, немає.

Більш явні криптологічні приклади дійшли до нас від цивілізацій Месопотамії – від вавилонян, ассирійців, халдеїв, які використовували особливу систему письма – клинопис. У 1500 р. до н.е. на глиняній табличці був записаний рецепт глазурі для гончарних виробів, що ретельно охоронявся на той момент. Знаки, що визначають необхідні інгредієнти, були навмисно перемішані. Таким чином, ми маємо право стверджувати, що ця табличка є найбільш ранньою відомостю секретного запису.

Приблизно з 500 р. до н.е. в Індії також широко застосовувалися секретні записи, зокрема в донесеннях шпигунів і текстах, імовірно, що

використовувалися Буддою. Методи засекречення включали в себе фонетичну заміну, коли приголосні і голосні мінялися місцями, використання перевернутих букв і запис тексту під випадковими кутами. Різні індійські трактати, яскравим прикладом яких є «Артхашастра» (близько 321–300 рр. до н. е.), показують, що індійці були добре знайомі зі способами приховування інформації.

Найпершим прикладом шифрування, що був документально зафіксованим є шифр Цезаря, що полягає в заміні кожної літери потрібного вихідного тексту віддаленою на k кроків, де k – ключ.

Також, відомим шифром є «Квадрат Полібія», автором якого вважають грецького письменника та філософа Полібія. Даний шифр є елементарним шифром заміни. В квадраті прописувалися букви відповідного алфавіту (наприклад, для грецького алфавіту розмір такого квадрату становив 5x5). Кожна літера вихідного тексту замінювалося на пару цифр – номер рядка і стовпчика, на перетині їх – зашифрована буква.

VIII століття нашої ери характеризується розвитком криптографії переважно в арабських країнах. Халіль аль–Фараxіфі, арабський філолог, документально першим зазначив, що певний набір стандартних фраз, що містяться у відкритому тексті, можна використовувати для дешифрування. Наприклад, ним було висунуто припущення, що фраза «В ім'я Аллаха», з якої зазвичай починаються грецькі листи, дозволяє прочитати весь текст, що залишається. Даний метод він описав в своїй книзі «Кітаб аль–Муамма», що перекладається як «Книга таємної мови» [19].

Вже в 855 році, відомий арабський вчений того часу Абу Бакр Ахмед ібн Алі Ібн Вахшія ан–Набаті пише першу книгу з криптографії – «Книга великого прагнення людини знайти відповіді на запитання древньої писемності». В ній вчений описує декілька шифрів та застосовує не один алфавіт.

Також, до даного періоду часу – IX століття, можна віднести «Манускрипт про дешифрування криптографічних повідомлень» Аль–Кінді, де вперше згадується частотний криптоаналіз (Рис.1.2.3.).

Рис.1.2.3. Фрагмент першої сторінки «Манускрипт про дешифрування криптографічних повідомлень» Аль–Кінді

Чотирнадцятитомна енциклопедія «Субхі ал–Ааша», що була написана Шихабом ал–Калкашанді в 1412 році, містить розділ «Приховування в літерах таємних полвідомлень», де описується сім шифрів перестановок чи замін частотного криптоаналізу і таблиці, в яких спостерігалася частота появи певної арабської літери в Корані.

Саме арабський народ запровадив поняття «алгоритм» та «шифр» до сучасного словника криптології.

В стародавні часи широкого застосування знайшли різні найпростіші криптографічні пристрої.

Грецьким поетом Архілохом, що жив в VII столітті до н.е., згадується пристрій під назвою скитала (Рис.1.2.4). Достовірно відомо, що скитала використовувалася у війні Спарти проти Афін в кінці V століття до н. е. Даний пристрій являє собою циліндр і вузьку смужку пергаменту, що обмотують навколо нього по спіралі, на якій в свою чергу писалося повідомлення [20].

Рис.1.2.4. Скитала

Зашифроване повідомлення писали на пергаментній стрічці по всій довжині палички, і після того як остання виявлялася вичерпаною, її повертали і продовжували писати повідомлення далі, поки воно не закінчиться, або поки не списувалася вся пергаментна стрічка, в разі чого використовувався наступний шматок такої ж стрічки. Для дешифрування адресат використовував паличку аналогічного діаметру, на яку потрібно було намотувавати пергамент, до тих пір, поки повідомлення не було прочитано. Такі народи як античні греки чи спартанці, використовували цей шифр за допомогою скитали, для зв'язку під час військових дій. Проте, як виявилося, такий шифр було легко зламати. Наприклад, перший метод злому скитали був запропонований ще Арістотелем. Він полягає в використанні конуса, який мав регулюючий діаметр, і навіть не знаючи точного діаметру палички, що була використана при шифруванні, переміщаючи пергамент з повідомленням по його довжині текст почне читатися – таким чином знаходиться потрібний діаметр скитали.

Також, досить відомим пристроєм, що мав за основу криптографічний ЗІ, вважався «диск Енея» – інструмент, що був вигаданий Енеєм Тактиком, приблизно в IV столітті до нашої ери (Рис.1.2.5.). За такий пристрій слугував диск, з довільного матеріалу, що мав діаметр близько 13–15 см та товщину 1–2 см, в якому було пророблено отвори, кількість яких рівнялася до кількості літер в алфавіті того часу. Кожному отвору відповідала конкретна літера. У центрі такого диска знаходилася котушка, на яку була намотана нитка [20].

Рис.1.2.5. Диск Енея

Механізм такого шифрування був доволі простий і полягав в почерговому протягуванні вільного кінця нитки, що була на катушці, через отвори, що позначали літери вихідного повідомлення. Як висновок, сам диск, з протягнутою в його отвори ниткою, і слугував зашифрованим посланням. Одержувач повідомлення послідовно витягаючи нитку з кожного отвору отримував потрібну послідовність літер. Але ця послідовність була зворотньою по відношенню до вихідного повідомлення, тобто одержувач читав повідомлення в зворотньому порядку – з кінця. Таке зашифроване повідомлення було доступним до прочитання будь–кому, хто зміг заволодіти диском. Так як повідомлення могли змінювати звичайні гінці, а не воїни, Еней передбачив наскільки шкидко може бути знищена потрібна передана інформація. Еней стверджував, що необхідно і достатньо лише вийняти всю нитку за один кінець, або просто можна знищити диск, наприклад наступивши на нього. За думкою фахівців, «диск Енея» наврядчи можна назвати дієвим криптографічним інструментом, адже за даним способом шифрування прочитати зашифроване в такий спосіб повідомлення міг кожен, хто знав принцип роботи диску. Проте саме цей пристрій став прабатьком найпершого криптографічного інструменту даного типу, який теж винайшов Еней.

2. Формальна криптографія. Наступний етап – етап формальної криптографії, який був пов'язаний з появою формалізованих та відносно

стійких до ручного криптоаналізу шифрів. У європейських країнах етап формальної криптографії проходив в ті часи, коли розвиток науки та торгівлі викликав попит на надійні, будь–які способи що дадуть можливість захищати інформацію.

До кінця XIV ст. між італійськими містами–державами в листуванні вже застосовувалися «номенклатори».

Означення 1.2.1. Номенклатори – великі переліки, які включали в себе кодові заміни імен людей, країн, міст, видів зброї, провіанту і т.д. З метою підвищення захищеності інформації до переліків були додані шифроалфавіти для кодування слів, що не увійшли до переліку, а також правила їх використання, що базуються на різних КМ [21].

Симеоне де Крема був першим (1401 р.), хто використовував таблиці омофонів для приховування частоти появи голосних в тексті за допомогою більш ніж однієї шифрозаміни.

Батьком західній криптографії називають вченого епохи Відродження Леона Баттіста Альберті. Вивчивши методи дешифрування моноалфавітних шифрів (шифрів однозначної заміни), що використовувалися в Європі, він спробував створити шифр, який був би стійкий до частотного криптоаналізу. В праці «Трактат про шифри» був представлений в папську канцелярію в 1466 році і вважається першою науковою працею з криптографії. Альберті було запропоновано використання двох і більше секретних алфавітів замість єдиного як, наприклад, в моноалфавітних шифрах, та перемикатися між ними за певним правилом (поліалфавітні шифри).

Рис.1.2.6 Перша сторінка «Трактату про шифри»
Леона Баттіста Альберті

Згадуючи роботи, в яких наявне узагальнення та формулювання алгоритмів шифрування важливо зазначити працю «Поліграфія» німецького абата Трітемія (Рис.1.2.7), в якій вперше було помічено можливість шифрування двома літерами – біграмами.

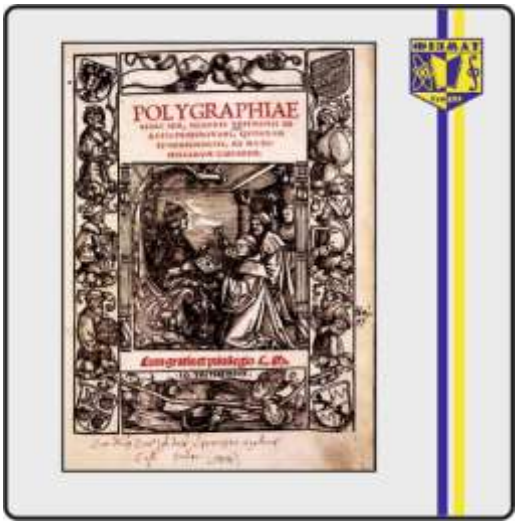

Рис.1.2.7. Перша сторінка «Поліграфії» Трітемія

Джіроламо Кардано, відомий італійський математик тих часів, в 1550 році, перебуваючи на той час на службі у Папи Римського, запропонував нову техніку шифрування – «Решітка Кардано» (Рис.1.2.8). Даний спосіб мав за

основу стеганографію – мистецтво прихованого письма, та саму криптографію. В даному методі було важко навіть побачити що текст містить зашифроване повідомлення, а розшифрувати його за відсутності ключа, в даному випадку решітки, в той час було майже неможливо. Метод «Решітка Кардано» вважається першим в своєму роді транспозиційним шифром, або геометричним шифром, що заснований на положенні букв в зашифрованому тексті.

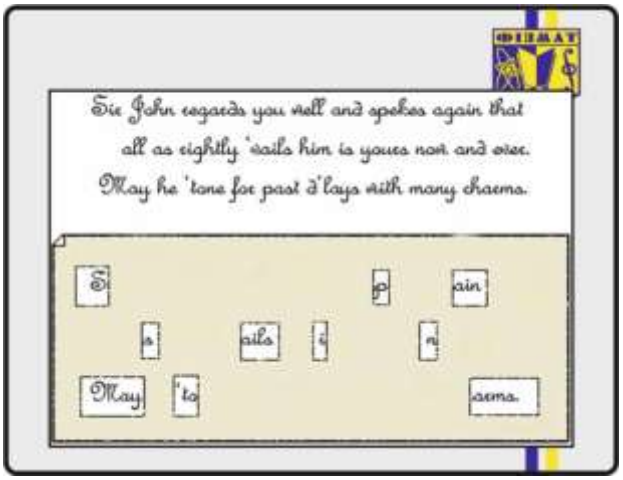

Рис.1.2.8. Принцип роботи «Решітки Кардано»

Важливим поштовхом в історії криптографії був період винаходу телеграфу. Проте, завдяки такому винаходу передача даних вже не була секретною, і оригінальним повідомленням, в теорії, міг заволодіти будь–який охочий. Навіть серед простого люду зростає інтерес до криптографії, в результаті чого багато спробували створити свої власні індивідуальні системи шифрування. Перевага телеграфу була очевидною також і на полі бою, де головнокомандувач мусив віддавати негайні накази на поле битви, а також отримувати інформацію з безпосередніх місць подій. Саме це і послужило поштовхом до розвитку польових шифрів на той час.

Відомий прусським криптограф, Фрідріх Казіскі, у 1863 році опублікував метод, який в подальшому названий його ім'ям – «метод Казіскі», що надавав швидке та ефективне розкриття майже кожного шифру того часу, в

тому числі і поліалфавітного. Метод Казіскі складався з двох частин, перша з яких полягає у визначенні періоду заданого шифру, і друга – в дешифруванні повідомлення за допомогою частотного криптоаналізу.

Огюст Керкгофс, відомий криптограф, що був уродженцем Голландії, в 1883 р, опублікував працю «Військова криптографія» (Рис.1.2.9), де детально описав шість вимог, яким повинна задовольняти захищена, на той час, система [21]:

1. Стійкий шифр не повинен бути зламним відносно фізичного чи математичного злому (впливу);
2. У випадку потрапляння до зловмисника, стійка система не вимагає секретності;
3. Ключ, для дешифрування системи, повинен бути максимально простим, щоб без труднощів зберігався в пам'яті без запису на сторонньому папері, а також легко змінним при бажанні;
4. Телеграф без проблем може передавати шифр такої системи;
5. Шифрувальний пристрій не важкий, легко переноситься, дає можливість працювати одній особі, не вимагаючи сторонньої допомоги;
6. Шифрувальний пристрій простий у використанні, не викликає труднощів та не вимагає великих розумових затрат чи слідування одразу багатьом правилам.

Рис.1.2.9. «Військова криптографія» Керкгофса

Огюстом Керкгофсом також був сформульований відомий «принцип Керкгофса» – правило розробки криптографічних систем, згідно з яким в засекреченому вигляді тримається лише певний набір параметрів алгоритму, званий ключем, а сам алгоритм для шифрування повинен бути у відкритому доступі. Іншими словами, при оцінці надійності шифрування необхідно припускати, що противник знає про систему, що застосовується при шифрування, проте йому невідомі застосовувані ключі.

Відомий американський криптограф Вільям Фрідман, у 1920 р. опублікував власну монографію «Індекс збігу і його застосування в криптографії» (Рис.1.2.10). Дана робота була опублікована у відкритій пресі, не зважаючи на те, що була виконана в рамках військового замовлення, що зазвичай суперечить розголошенню. Двома роками пізніше, в 1922 р. Вільям Фрідман також ввів до наукового обігу такі терміни як «криптологія» та «криптоаналіз», що використовуються до сих пір [22].

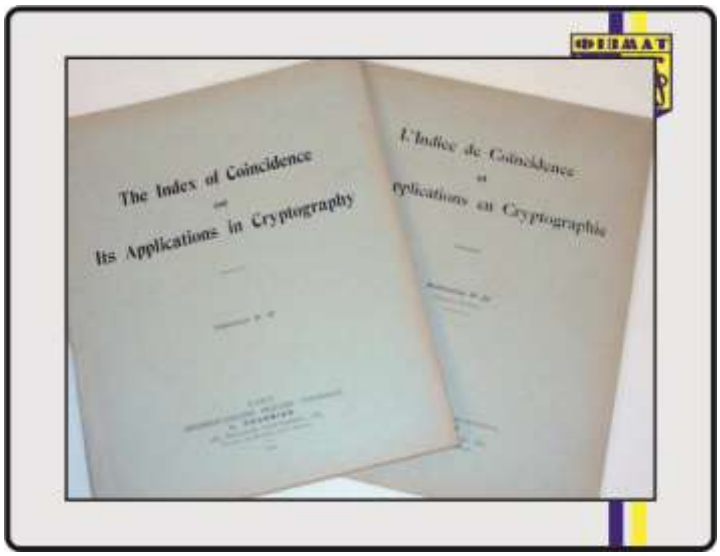

Рис.1.2.10. «Індекс збігу і його застосування в криптографії»

Значно вплинула криптографія і на літературну лінію. Давньогрецький історик Геродот, описуючи шифрування в контексті певних історичних подій, згадує криптографію, як окрему науку. Одною з перших літературних згадок, де зустрічається про криптографію, можна вважати роман французького

письменника, лікаря XVI століття Франсуа Рабле «Життя Гаргантюа та Пантагрюель», де в одній із глав автор описує спроби дешифрування зашифрованих повідомлень. Також, наука криптографія зустрічається в відомому історичному часописі «Генріх V» Шекспіра. Проте, вперше в якості центрального елементу художнього твору, криптографія, як наука, використовується в сюжеті оповідання «Золотий жук», що був написаний Едгаром Алланом По в 1843 р., в якому письменник не лише показує спосіб за яким відбувається розкриття заданого шифру, а й результат до якого може привести описана діяльність – процес знаходження захованого скарбу. Одним з кращих літературних прикладів, де зустрічається опис застосування криптографії, вважається твір Артура Конан Дойля, що був написаний в 1903 році – «Танцюючі чоловічки». В даному оповіданні, великий детектив Шерлок Холмс, що широко відомий і в сьогоденні, зустрічається з певним різновидом шифру, що приховує факт передачі повідомлення до сторонніх осіб, використовуючи дитячі картинки–символи, цим самим шифр також приховує сам зміст повідомлення. В оповіданні «Танцюючі чоловічки» Шерлок, для вирішення такої проблеми, застосовує частотний аналіз і припускає певну структуру відкритого повідомлення, що знадобиться для дешифрування.

Аналізуючи історичний аспект, важливо згадати початок Другої світової війни – в часи, коли передові світові держави мали в запасі технічні пристрої для шифрування повідомлень, результат роботи таких пристроїв вважався стійким до розкриття. На той час, ці пристрої ділилися лише на два типи – роторні машини та машини, що конструювалися на цівкових дисках. Головним прикладом першого типу є відомий апарат, який використовували німецькі війська – «Енігма», також відомим прикладом криптографічного пристрою є американська М–209, яку відносимо до другого типу. В Союзі Радянських Соціалістичних Республік (СРСР) виробляли як перший, так і другий тип таких захисних апаратів [22].

Усі можливі успішні криптоатаки, на подібного роду криптографічні апарати, стали можливі тільки з появою ЕОМ.

3. Математична криптографія. Після завершення минулого періоду – Першої світової війни, уряди передових держав приділили більше уваги конфіденційності практично всім роботам в області науки криптографії та всіх приладів для її реалізації. Вже на початку 30–х років, в сфері науки, було завершено узагальнення розділів математики, які стали базисом для майбутніх математично спрямованих наук: загальна алгебра, теорія чисел, теорія ймовірностей і математична статистика. Побудова перших машин, що відносилися до програмно–розрахункових, припала на кінець 1940-х років. В основі таких пристроїв були закладені базиси алгоритмічної теорії та науки кібернетики. В період після завершення Першої світової війни і практично до кінця 1940–х років, у відкритій пресі було видано мінімум робіт та монографій. Найбільшого прогресу в криптографії було досягнуто в сфері військових відомостей.

Ключовим етапом в розвитку науки криптографії вважається головна праця американського математика Клода Шеннона «Теорія зв'язку в секретних системах» – секретна доповідь, представлена ним в 1945 р., і опублікована в «Bell System Technical Journal» у 1949 р. У даній роботі, за думкою багатьох теперішніх науковців, що займаються криптографією, було вперше показано підхід до науки криптографії в цілому як до математичної [22].

Приблизно в 1960–х роках з'являються серед наукових робот та досліджень різноманітні блокові шифри, які були наділені більшою стійкістю до злому порівняно з більшістю роторних машин. Проте, навіть такі шифри передбачали необхідність використання електронних пристроїв – ручні або напівмеханічні методи шифрування інформації на той час вже не були актуальними.

У 1967 році опублікована книга американського історика та криптографа Девіда Кана «Зламщики кодів». Не зважаючи на те, що книга не містила нових результатів досліджень, вона більш конкретно описувала вже існуючі результати в області криптографії того часу, значний історичний матеріал, в якому містилися переважно вдалі випадки використання методів

злому шифрів – криптоаналізу, та дані, які уряд США до того моменту вважав за конфіденційний. Але головною перевагою було те, що дана книга мала значний комерційний успіх і ознайомила з наукою криптографії безліч людей з усіх куточків світу. З того часу почали з'являтися роботи і у вільному доступі [22].

Приблизно в цей же час відомий прусський вчений–криптограф Горст Фейстель перейшовши з військової служби США до праці в підрозділах американської корпорації IBM – однієї з найбільших постачальників програмного забезпечення та інформаційно–технологічних сервісів, починає займатися створенням нових методів шифрування та розробляє конструкцію Фейстеля, що є фундаментом до багатьох шифрів теперішніх часів, в тому числі відомого шифру Lucifer, що став прообразом відомого шифру DES – колишнього еталону шифрування США, найпершого державного стандарту на шифрування даних світового значення, що був у відкритому доступі. На основі конструкції Фейстеля створювалися різноманітні блокові шифри, такі як TEA (1994 р.), Twofish (1998 р.), IDEA (2000), а також колишній (ГОСТ 28147–89) і діючий (ГОСТ 34.12– 2015) – російські стандарти шифрування.

Уже в 1976 році була опублікована робота американських криптографів Вітфілда Діффі і Мартіна Хелмана «Нові направлення криптографії». В цій роботі описано нову область в криптографії, яку сьогодні називають «криптографія з відкритим ключем». Також криптографи в своїй роботі детально описали алгоритм Діффі–Хеллмана–Меркле, що дозволяв двом сторонам, між якими передавалося повідомлення, згенерувати загальний секретний ключ, при цьому використовуючи відкритий канал зв'язку.

Хоча робота Діффі–Хеллмана зробила значний теоретичний внесок до відкритої криптографії, першою дійсною криптосистемою з відкритим ключем вважають алгоритм RSA (названий по імені авторів – Рон Рівест, Аді Шамір і Леонард Адлеман). Опублікована в серпні 1977 р. робота дозволила сторонам обмінюватися секретною інформацією, при цьому не маючи заздалегідь схваленого прихованого ключа. Варто відзначити, що і алгоритм Діффі–

Хеллмана–Меркле, і RSA були вперше відкриті в англійських спецслужбах, але не були ні опубліковані, ні запатентовані через свою конфіденційність [22].

Створення асиметричних криптосистем підштовхнуло математиків і криптоаналітиків до вивчення способів факторизації, дискретного логарифмування, операцій над еліптичними кривими в кінцевому полі.

Одним з нових методівм є відносне шифрування, який запропонували Шафі Гольдвассер та Сільвіо Мікель. Шифрування названо «відносним» в зв'язку з тим, що один і той же вихідний текст для шифрування, з використанням одного і того ж ключа, може перетворюватися в абсолютно різні, не залежні один від одного, шифротексти. Відносне шифрування дозволяє на порядки збільшити складність такого виду атаки.

Чарльз Бенет і Жиль Брасард, спираючись на роботу Стівена Віснера, розробили теорію квантової криптографії, яка базується скоріше на квантовій фізиці, ніж на математиці. Процес відправлення та прийому інформації виконується за допомогою об'єктів квантової механіки (наприклад, за допомогою електронів в електричному струмі або фотонів в лініях волоконно–оптичного зв'язку). Заснована на принципах квантової механіки, ця система, на відміну від звичайної криптографії, теоретично дозволяє гарантовано захистити інформацію від зловмисника, навіть якщо той володіє найсучаснішою технологією і необмеженими обчислювальними потужностями. На даний момент, розробляються лише прототипи квантових криптосистем [22].

У той же час ефекти квантової фізики, можливо, зможуть використовуватися і для криптоаналізу. Якщо будуть побудовані квантові комп'ютери, то це поставить під сумнів існування сучасної криптографії.

Висновки до розділу 1

Підводячи підсумки до першого розділу, можна стверджувати, що на сьогоднішній день, у світі сучасної комерції, інформація – один з найважливіших елементів та як відомо, основна частина будь–якої важливої інформації обробляється в електронному вигляді. Найкращим способом перешкоджання несанкціонованого доступу до неї, навмисного чи випадкового втручання є надійні методи ЗІ. В майбутньому, оскільки комерція та будь–яка комунікація будуть тісніше пов’язані з комп’ютерною мережею – криптографія стане невід’ємною частиною нашого життя, а значення математичних основ криптографії матиме першорядне значення для всіх, хто бажає досягнень успіху в програмах комп'ютерних наук із зосередження на безпеці. Оскільки історія криптографії досить насичена то для подальшої роботи в даній області важливо знати всі аспекти її розвитку та вміти апелювати даними відомостями.

РОЗДІЛ 2. НАВЧАННЯ ІНФОРМАТИКИ В УМОВАХ ГУРТКОВОЇ РОБОТИ

2.1. Вимоги до підготовки учнів старшої школи з інформатики

На сьогоднішній день, заклади загальної середньої освіти вважаються головним соціальним інститутом. Такі заклади мають за мету адаптацію учнів до подальшого життя, індивідуально–особистісного зростання, інформованість учнів щодо різних сфер життєдіяльності.

Як відомо, активна участь при створенні задовільного та прогресивного освітнього середовища та введення до навчального плану тематичних курсів, які нададуть змогу сучасним школярам зробити усвідомлений вибір профілю свого навчання, при цьому враховувати подальший розвиток в своїй професії – ефективний та найбільш вагомий напрямок школи.

В основі модернізації сучасної освіти, що стосується старших класів, поставлене завдання забезпечення профільного навчання, «системи підготовки за спеціалізаціями, що має орієнтацію на індивідуалізоване навчання та соціалізацію кожного учня, з урахуванням потреб ринку праці».

У шкільному процесі навчання, інформатика вважається наймолодшою з усіх наук, проте саме вона вимагає більшої концентрації та розумових здібностей і саме інформатика є найбільш трудомісткою серед інших.

Всі задачі, що виконуються на уроках з інформатики, містять ряд сторонніх прикладних наук – математику, фізику та інші, саме тому інформатику вважають предметом, що містить міжпредметні зв’язки.

В зв’язку з тим, наскільки стрімко розвивається інформатика, підвищуються і вимоги як до вчителя, так і до учня.

На сьогоднішній день, інформатика має за мету не лише освітній розвиток, опанування новими знаннями й навичками, а й розвиток інтелектуального потенціалу учня – особистості.

В залежності від інформаційної насиченості, вимог та поставлених завдань, процес вивчення інформатики вивчається за двома рівнями: рівень стандарту та профільний. Головною, спільною метою для обох рівнів

вивчення курсу інформатики є формування в учнів інформативної компетентності та інформаційної культури, за для реалізації потенціалу та соціалізації, якої вони досягнуть завдяки вмінню ефективного використання всіх сучасних інформаційних технологій.

В старших класах, стандартний рівень навчання більш зосереджений на логічному продовженні курсу основної школи, в той час як профільний рівень має за основу більш розширені та доповнені завдання, що спрямовані на розвиток логічних здібностей. Також, профільний рівень навчання передбачає підготовку учнів до інтелектуальних змагань, професійної діяльності, пов'язаної з інформаційними технологіями.

Стандартний рівень навчання ставить перед собою наступні завдання, при вивченні інформатики в старших класах:

1. Готовність застосувати вивчений матеріал, інформаційні технології за для виконання будь–яких задач що до їх реалізації;
2. Формування знань, умінь і навичок, що будуть необхідні при використанні інформаційних технологій в навчальній діяльності та повсякденному житті;
3. Формування усвідомленості щодо важливості інформаційної культури, її розвиток; володіння знаннями правильної експлуатації засобів інформаційних технологій при виконанні робіт, де наявна їх необхідність;
4. Розвиток самостійності при опануванні та використанні програмних засобів, пошуку та систематизації, аналізу відомостей, використання електронних засобів обміну даними.

Аналізуючи навчальну програму для профільного рівня, спостерігаємо, що всі вищеперераховані завдання зустрічаються в більш розширеному вигляді. Головні завдання, які передбачає курс вивчення інформатики за профільним рівнем наступні [23]:

1. Формування в учнів відповідного теоретичного базису, щодо будь–яких процесів обробки інформації та систематизації даних;

2. Досягнення розуміння важливості інформаційних технологій та відповідних процесів;
3. Розвиток аналітичного та логічного мислення, індукції, дедукції, вміння аналізувати та систематизувати.
4. Розвиток здібностей до розв'язання різнорівневих задач, використовуючи диференційований підхід;
5. Використання творчого підходу при вивченні інформатики;
6. Розвиток навчальних здібностей до рівня участі в інтелектуальних конкурсах (олімпіади, турніри і т.д.);
7. Досягнути розуміння практичного значення здобутих знань та навичок у подальшому житті, новій професії;
8. Встановлення міжпредметних зв'язків;

Проте варто розуміти, що жодні, з вищеперерахованих завдань навчальних програм, не можуть бути виконані самостійно, без виконання інших, адже вони всі можуть досягатися лише паралельно та одночасно. Вважається, що без забезпечення загальної освіти в галузі інформатики унеможливлюється виконання виховної мети предмету.

Реалізація вмінь та навичок на персональному комп'ютері, що були здобуті на уроках інформатики, вимагають від учня великих розумових та вольових зусиль, розвиненої логічної уяви, повної концентрації уваги, зазвичай призводять до бажаного результату, під яким мається на увазі розвиток самостійності учня, його наполегливості, активності, відповідальності та цілеспрямованості, формування критичного мислення, поставленої дисципліни. Один з найважливіших компонентів для роботи з персональним комп'ютером – точність власного мислення, чіткість і лаконічна послідовність дій. Саме до цього компоненту курс інформатики в школі передбачає власний, особливий стандарт.

Основний курс інформатики, як правило, надає учням обізнаність про сферу майбутньої професії, яка буде пов'язана з персональним комп'ютером, інформатикою, або з професіями, що спираються на взаємодію з персональним

комп’ютером. Всі такі дії виконуються з метою повної обізнаності учнів про можливі сфери майбутньої діяльності, та з метою загальної профорієнтації. Підготовка учнів до практичного та грамотного використання персонального комп’ютера та будь–якої з комп’ютерних чи інформаційних технологій – основні практичні цілі курсу інформатики в школі.

Враховуючи, наскільки важлива та необхідна сучасна інформатизація в економіці, та те, що змінюється домінанта діяльності в сфері професійної діяльності, вважатимемо за необхідне підготовку учнів до основних видів діяльності, що пов’язані з обробкою інформації.

2.2. Сучасні форми навчання інформатики

В період сучасної комп’ютерної обізнаності та інформатизації, сучасному учню загальноосвітнього закладу надаються великі можливості безпосередньої взаємодії з персональний комп’ютером, навіть не враховуючи уроки інформатики, тобто поза шкільним процесом. В ролі таких можливостей переважно виступають заняття в гуртках, що спрямовані на більш вузькі напрямлення певної спеціалізації або безпосередня робота за персональним комп’ютером в домашніх обставинах. Проте, навіть така робота повинна базуватися на чіткій організації, в разі відсутності якої, у більшості учнів формується різний рівень психологічної підготовки та впевненості при роботі з персональним комп’ютером в одній віковій категорії. В освітній практиці, не рідко зустрічається ситуація, коли в учнів формується псевдо впевненість в тому, що вони володіють всіма потрібними знаннями та навичками з інформатики, хоча більшість з таких учнів не бачать різниці між поняттями «інформатика» та «ІКТ». Поряд з цими можливими проблемами, існує не менш важлива – нездатність тверезо оцінювати можливості використання знань та навичок, здобутих на уроках інформатики, поза навчальним процесом.

В період сучасних технологій, суспільство вимагає вільного володіння інформаційною культурою заради успішної адаптації в соціумі. Навчаючись в

школі, необхідно також самовдосконалюватися, якщо учень має за мету встигати за сучасним темпом розвитку інформаційних технологій.

В системі сучасного процесу навчання, головна мета вчителя інформатики та інформаційно–комунікаційних технологій (інша назва – ІКТ) – сприяти формуванню особистості учня, для здатності жити в сучасних умовах інформаційного суспільства.

Досягти такої поставленої головної мети, вчителю необхідно виконувати наступні завдання:

1. Створити оптимальні умови що максимально розкривають рівень обдарованості кожного учня:
2. Створення міжпредметних зв’язків на уроках інформатики чи інформаційно–комунікаційних технологій;
3. Створення умов для саморозвитку кожного учня, його самоосвіти;

Система сучасної освіти, з кожним новим навчальним роком, задовольняє нові потреби для індивідуалізації навчання, особистого направлення для кожного учня окремо. На уроках інформатики досягнуто всіх умов для проведення навчання за різноманітними формами навчання, застосовуючи все більше різноманітних методів.

Означення 2.2.1. Форма навчання – зовнішня сторона організації навчання [24].

Більшість сучасних фахівців поділяють усі наявні форми навчання на навчально–планові, позапланові та допоміжні [25].

1. Навчально–планові форми навчання. Представниками даних форм навчання є уроки, лекції, семінари та заняття з контролю знать (заліки, іспити).
2. Позапланові форми навчання. До даних форм відносять всі лабораторні заняття, що виконуються в групах, конференції, гурткові заняття, екскурсії та консультації.
3. Допоміжні форми навчання. Такі форми навчання передбачають проведення групових чи індивідуальних занять з інформатики.

Також існує класифікація форм навчання на загальні, зовнішні та внутрішні [26].

Варто відзначити, що наявність персонального комп'ютера також є важливо показником при класифікації форм навчання інформатики: комп'ютерні чи безкомп'ютерні.

В свою чергу, загальні форми навчання також мають свою класифікацію [27]:

1. Загально–колективні форми навчання.
2. Загально–фронтальні форми навчання.
3. Загально–групові форми навчання.
4. Загально–індивідуальні форми навчання.
5. Загальні форми навчання з динамічним складом навчальної групи чи класу.

Поділ таких загальних форм відбувається за урахуванням характеристик взаємодії між вчителем та класом (групою), внутрішніми відносинами.

1. Загально–фронтальна форма навчання. Навчання за такою формою впроваджується у випадку роботи всієї групи учнів над одним змістом навчального матеріалу, тобто передбачається взаємодію вчителя з кожним учнем за одним темпом навчання, досягненням одного й того ж завдання, мети. Фронтальна форма навчання на уроках інформатики вважається традиційною, та застосовується при реалізації всіх необхідних методів навчання: практичних, словесних та наочних.

За твердженням А. І. Бочкіна, спостерігати величину впливу комп'ютера на учня можна за можливістю точного відтворення ним діяльності, аналогічної до діяльності, що демонструється вчителем [28].

2. Загально–колективна форма навчання. В запропонованій формі навчання члени колективу, в даному випадку класу чи групи, позиціонуються в якості окремої ланки, з яскраво вираженими лідерами та набутими характеристиками.

3. Загально–групова форма навчання. При використанні представленої форми клас працює в групах, що створюються на основі різнопланових завдань. Переважно даний тип використовується при засвоєнні нових знань, знайомстві з новими технологіями, програмними засобами. При роботі за загально–груповою формою навчання відбувається інтенсивна робота в групах, навантажена обміном інформацією, саме тому така форма підходить для наявних різних рівнів підготовки учнів, різної навчальної мотивації. Дана форма навчання також передбачає роботу в парах, де відбувається взаємодія лише між парою учнів. При парному навчанні набуває розвитку взаємоконтроль та взаємодопомога, адже частим випадком є ситуація, коли учень краще сприймає інформацію від однокласника, ніж від вчителя. У представленій формі навчання мають місце такі взаємозв'язки спілкування як «учень–учень» та «вчитель–учень». На сьогоднішній день, розроблено ряд форм навчання, при яких пари учнів змінюються за певною послідовністю, що дозволяє інтегрувати парну форму навчання з колективною.

4. Загально–індивідуальна форма навчання. Представлена індивідуальна форма навчання передбачає взаємодію вчителя з учнем окремо від решти групи чи класу. Найбільш типові представники даної форми навчання – менторство та репетиторство. На уроках інформатики сформувався новий вид загально–індивідуальної форми навчання – «учень–комп'ютер». В даному випадку, учень працює індивідуально з навчальною програмою через посередника – комп'ютер, оволодіваючи необхідними знаннями та навичками у зручному для себе темпі. Комп'ютер, в якості ЕОМ, з роками відроджує масове індивідуальне навчання. Враховуючи насиченість інформації в мережі Інтернет, мультимедійних курсах, учні отримали можливість використання безлічі джерел інформації, можливості додаткових занять, самонавчання. В сучасній системі освіти однією з провідних задач кожного вчителя є формування в учнів самостійної діяльності з метою пізнання нової інформації.

Широко відомою ситуацією є випадок, коли інформатику починають вивчати лише в старших класах, при цьому учні вивчають базовий курс, що

міститься в програмі, затвердженій Міністерством освіти України, тоді як в переважній більшості шкіл наявне поглиблене вивчення інформатики, що містить курс програмування. Така різниця зумовлюється різністю профільного направлення класу чи школи в цілому.

Якщо для конкретного класу характерне гуманітарний профіль навчання, то на уроках інформатики вивчається базовий курс користувача персонального комп'ютеру та короткий екскурс за використанням деяких комп'ютерних технологій. Якщо клас навчається за фізико–математичним профілем – в курсі інформатики має місце вивчення курсу програмування, предметного курсу застосування в повсякденності комп'ютерних технологій, побудова та розв'язок алгоритмів до різних типів задач. Для класу фізико–математичного профілю постійно відбувається формування всіх необхідних навичок та знань щодо використання персонального комп'ютера, який вже розглядається як пристрій професійної діяльності, а значна частина курсу інформатики приділяється вивченню програм комп'ютерного моделювання, вивченню курсу програмування. Для учнів, що навчаються в класі гуманітарного профілю – в більшій мірі зменшується обсяг потрібних теоретичних знань, а переважна частина навчального матеріалу приділяється використанню деяких прикладних програм. Проте, якщо учень гуманітарного чи профільного класу бажає поглибити свої знання більш вузького направлення з інформатики – мають місце факультативи, елективні курси та різноманітна гурткова робота.

2.3. Гурткова робота в старших класах в галузі навчання інформатики

В системі сучасної освіти, кожний учень наділений широкими можливостями для індивідуального вибору та реалізації потреб стосовно професійного направлення. Для цієї мети реалізовується ефективна форма навчання в освітньому процесі – гурткова робота, яка розглядається в якості ефективного формування особистості, її творчого потенціалу, нових знань та

навичок. На сьогоднішній день, саме гурткова робота є важливою сферою для вияву активності, особистісного самовизначення, самореалізації.

Значною перевагою, що відноситься до гурткової роботи у сфері інформаційно–комунікаційних технологій можна зазначити різноманітність занять, яким можна надати ігровий характер, що більш приваблює учнів.

Аналізуючи статтю 5 Закону України «Про позашкільну освіту», розглянемо структуру самої позашкільної освіти, в якості процесу навчання [29]:

1. Заклади, спрямовані на позашкільну освіту;
2. Інші заклади освіти як центри ПО, до числа яких належать: ЗНЗ, незалежно від підпорядкування, типів і форм власності, в тому числі школи соціальної реабілітації, міжшкільні навчально–виробничі комбінати, заклади професійної (професійно–технічної) та фахової передвищої освіти;
3. Гуртки, секції, клуби, культурно–освітні, спортивно–оздоровчі, науково–пошукові об'єднання на базі закладів загальної середньої освіти, закладів професійної (професійно–технічної) та фахової передвищої освіти;
4. Клуби та об'єднання за місцем проживання незалежно від підпорядкування, типів і форм власності;
5. Культурно–освітні, фізкультурно–оздоровчі, спортивні та інші заклади освіти, установи;
6. Фонди, асоціації, діяльність яких пов'язана із функціонуванням ПО.

Оскільки ЗНЗ, такі як центри ПО, в позакласній та позашкільній роботі являються частиною структури ПО, вищезазначені норми стосуються і гурткової роботи.

Гурткова робота, за думкою фахівців, класифікується за декількома рівнями об’єднань [30]:

1. Початковий рівень. До першого рівня відносять всі об’єднання учнів, переважно творчого характеру, які спрямовані на всебічний розвиток

учнів, виявлення потенціалу до різних типів діяльності, виховання інтересу до всебічної творчої діяльності;

2. Середній (основний) рівень. Об’єднання, що мають за мету розвиток інтересів всіх вихованців, надання знань та навичок, що спрямовані на професійну діяльність;
3. Вищий рівень. До представленого рівня відносяться всі об’єднання учнів, що формуються за інтересами. До даного рівня залучаються обдаровані, за певним напрямком, учні.

Відповідно до того, який рівень класифікації запроваджується, визначаються мета та можливості діяльності гурткової роботи, її чисельний склад, обирається програма за якою будуть проводитись заняття. Роль учителя полягає у правильному розміщенні перед учнями різноманітних видів діяльності, що відповідають їхнім інтересам та здібностям, для підтримки незалежних досліджень та творчості. Учень повинен мати право вибору, самоствердження, доведення своєї індивідуальності. Вчитель повинен допомогти йому реалізувати свої здібності, захопити та підтримати. Тому групова робота є одним із важливих засобів розвитку особистості учня.

Гурткова робота, як одна з складових форм викладання інформатики, за своїм насиченням є цілеспрямованою, чітко організованою, змістовною і методично оснащеною системою пізнавального та виховного спілкування, взаємодії, відносин між учителем та учнями. Сама гурткова робота реалізується цілеспрямованою організацією змісту, засобів навчання та методів.

Різні групові роботи допомагають розкрити індивідуальні здібності дитини, які не завжди знаходять своє відображення на уроках інформатики.

Різноманітність такої діяльності передбачає підтримку самореалізації дитини, підвищує її самооцінку, впевненість у собі. Залучення учнів старшої школи до різних видів групової роботи збагачує їх особистісний досвід, знання про різноманітність людської діяльності, формує необхідні практичні навички та вміння, підготовляє до подальшої професійної діяльності.

Гурткові (групові) позакласні заходи сприяють виявленню та розвитку інтересів та творчих здібностей учнів у певних галузях науки, техніки, мистецтво, спорт, поглиблення знань програмного матеріалу, дає нова інформація, формує навички та вміння.

Означення 2.3.1. Гурток – одна з основних форм позаурочної діяльності [31].

Зміст роботи гурткової роботи для учнів старших класів з інформатики визначається їх інтересами та підготовкою, хоча для деяких існують вже готові програми для реалізації. Гурткова робота з інформатики може мати різну спрямованість відповідно до різних можливостей комп'ютера: комп'ютерна графіка, програмування, комп'ютерне моделювання тощо. Заняття різних типів відбуваються в груповій роботі. Це можуть бути проектні роботи, екскурсії, виготовлення візуальних інструментів та обладнання для офісів, лабораторні курси, зустрічі з цікавими людьми, віртуальні екскурсії тощо.

Робота гуртка фіксується в щоденнику. Підсумок може проводитися у формі вечора, конференції, виставки, огляду. У деяких школах результати діяльності підсумовуються на шкільних канікулах, що є оглядом роботи, виконаної протягом року, наприклад під час навчального тижня інформатики для шкіл.

Існує два типи групової роботи з інформатики для старших класів: робота з учнями, які відстають від інших у вивченні програмного матеріалу; робота з учнями, які продемонстрували вивчення інформатики на високому рівні, порівняно з іншими, за інтересом та здібностями (насправді позакласна робота в традиційному розумінні).

1. Групова робота зі студентами, які відстають від навчальної програми. Представлений вид позакласної роботи зі студентами інформатики в цей час відбувається у кожній школі. Однак підвищення ефективності викладання інформатики повинне призвести до зменшення необхідності проведення гурткової навчальної роботи, що має за мету зменшення відставання у старшокласників. В ідеалі, перший тип групової роботи повинен

мати яскраво виражений індивідуальний характер і повинен проявлятися лише у виняткових випадках (наприклад, у випадку тривалої хвороби учня, переведення з іншого типу школи тощо). Однак у цей час ця робота все ще вимагає значної уваги з боку вчителя інформатики. Його основною метою є своєчасне усунення (та запобігання) існуючих прогалин у знаннях та вміннях учнів.

2. Групова робота що зосереджена на роботі за збільшеним інтересом учнів. Напрямок групової роботи з інформатики, для якого характерні заняття з учнями старших, які виявляють підвищений інтерес до її вивчення, відповідає наступним основним цілям:

1. Пробудження та розвиток стійкого інтересу до інформатики;

2. Поширення та поглиблення знань за програмними матеріалами;

3. Оптимальний розвиток здібностей учнів та прищеплення певних дослідницьких здібностей;

4. Виховання культури мислення;

5. Розвиток здатності учнів самостійно та творчо працювати з навчальною та науково-популярною літературою;

6. Розширення та поглиблення розуміння учнями практичного значення інформатики в суспільстві;

7. Розширення та поглиблення розуміння старшокласниками культурно-історичної цінності інформатики, ролі інформатики у світовій науці;

8. Виховувати в учнів почуття колективізму та вміння поєднувати самостійну роботу з колективною;

9. Налагодження тісніших ділових контактів між викладачем інформатики та учнями та на цій основі глибшого вивчення пізнавальних інтересів учнів;

10. Створення інструменту, який може надати вчителю інформатики допомогу в організації ефективного викладання інформатики всією командою цього класу (допомога у виробництві наочних посібників, занять з учнями, що

відстають від навчальної програми, у розповсюдженні знань з інформатики серед інших учнів).

Висновки до розділу 2

В представленому розділі описуються основні сучасні форми навчання, їх класифікації. Описано особливості гурткової роботи, як прагматичного варіанту для вивчення допоміжної інформації, яка не передбачена навчальною програмою, для учнів старших класів з інформатики.

Говорячи про зміст гурткової роботи з учнями старших класів, які цікавляться інформатикою, ми помічаємо, що традиційні теми уроків, як правило, обмежуються розглядом питань, які, виходячи за рамки офіційної програми, мали багато точок дотику до питань, що розглядаються в ній. Наприклад, на уроках інформатики необхідно враховувати вивчення історичної інформації, проблему підвищених труднощів програмування, елементи математичної логіки, системи числення тощо. Участь у груповій роботі, де учням наочно демонструється зв’язок інформатики з життям, безпосередньо з майбутньою професією, створює умови для активної роботи в класі: їх цікавить сам предмет інформатики та формується пізнавальний інтерес.

РОЗДІЛ 3. ОПАНУВАННЯ КРИПТОГРАФІЧНИХ МЕТОДІВ УЧНЯМИ СТАРШИХ КЛАСІВ В УМОВАХ ГУРТКОВОЇ РОБОТИ

3.1. План реалізації представленої гурткової роботи

Метою гурткової роботи є ознайомлення учнів старших класів з основними поняттями ЗІ, основними принципами побудови систем захисту інформації, а також основними категоріями заходів ЗІ, їх можливостями з точки зору ЗІ, сильними і слабкими сторонами. В процесі освоєння курсу учні отримають навички вибору рішень з різних категорій методів і засобів ЗІ, що відповідають вимогам ЗІ в конкретних інформаційних системах, оцінки відповідності існуючих рішень таким вимогам, розробки пропозицій щодо вдосконалення системи забезпечення інформаційної безпеки. Для освоєння матеріалу курсу будуть корисні основні знання із загального курсу фізики, вищої алгебри, теорії чисел, інформаційних технологій. Їх наявність дозволить зрозуміти принципи дії КМЗІ, засобів технічного ЗІ, а також цифрових стеганографічних систем, саме тому дана гурткова робота передбачена для старших класів, які вже володіють необхідним базисом.

Назва курсу гурткової роботи: «Криптографічні методи захисту інформації».

Класи, для яких передбачено проходження курсу: 10-11 класи.

Кількість годин, передбачених на вивчення курсу: 30.

Методи навчання, застосування яких передбачено в ході проведення гурткової роботи:

1. Словесний. За допомогою даного методу учням надається теоретичний базис, на якому будується подальша робота – засвоєння нових знань, умінь, виконання відповідних практичних завдань. Словесний метод реалізується у вигляді лекцій, бесід, тощо;

2. Наочний. Представлений метод передбачає ілюстрацію обраного КМ, для кращого сприйняття матеріалу, за допомогою схем, рисунків;
3. Інтерактивний. За допомогою даного методу передбачається залучення дітей до роботи в класі, встановлення зворотного зв'язку. Доречною реалізацією є проведення дискусій, тренінгів, «мозкових штурмів;
4. Проблемно-пошуковий. Метод навчання, що полягає в вирішенні поставленої проблеми колективно, апелюючи раніше здобутими знаннями, залучення учнів до пошуку розв'язку задачі.
5. Практичний. Представлений метод полягає у вирішенні практичних завдань за допомогою вивчених знань, умінь та навичок;

Етапи, передбачені програмою гурткової роботи, можна представити у вигляді схеми *(Рис.3.1.1)*.

Рис.3.1.1. Етапи проведення гурткової роботи

1. Підготовчий етап. На першому етапі проведення гурткової роботи формуються основи, необхідного для вивчення курсу, алгоритмічного мислення. З учнями проводиться психологічна підготовка учнів перед початком курсу КМЗІ.

2. Базовий етап. Представлений етап передбачає ознайомлення учнів з необхідною теоретичною інформацією за програмою курсу, оволодіння

навички роботи з КМЗІ, їх характеристикою, принципами роботи процесу шифрування та дешифрування.

3. Практичний етап. Останній етап полягає в застосуванні набутих знань, умінь та навичок на практиці. На прикладі гурткової роботи з КМЗІ, практичний етап передбачає вміння шифрувати та дешифрувати повідомлення за існуючим методом.

Аналізуючи дані етапи проведення гурткової роботи, було складено навчально-тематичний план гурткової роботи з КМЗІ, де передбачені кожен з вищеперерахованих етапів (Додаток А).

Перед створенням програмованого матеріалу для курсу, було проведено опитування серед учнів старших класів, для усвідомлення актуальності проведення гурткової роботи за даною тематикою (Додаток Б).

В опитуванні прийняли участь 116 учнів 10 та 11 класів Краснопільської гімназії Краснопільської селищної ради Сумської області та Краснопільської загальноосвітньої школи. Перелік питань, мета та результати зазначені в Додатку В.

До опитування, з самим терміном «Криптографія» стикалися лише 37,5% від усієї кількості опитаних учнів *(Рис.3.1.2)*.

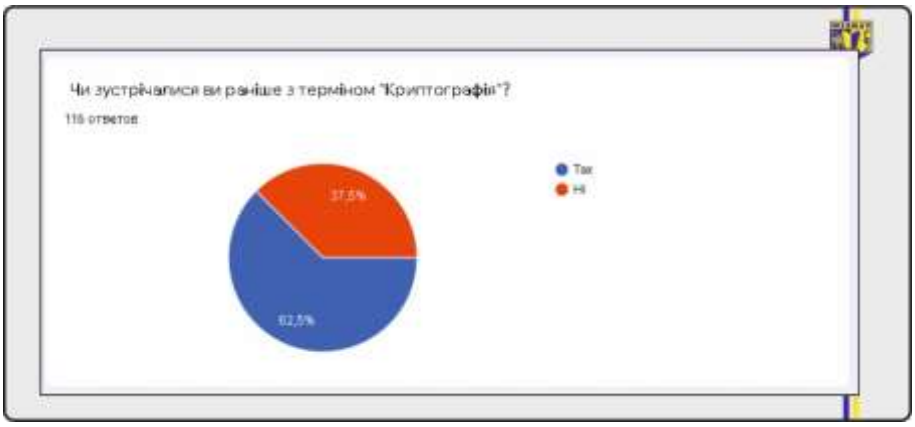

Рис.3.1.2. Показник обізнаності

За результатами даного опитування, було виявлене бажання у переважної кількості учнів вивчення теми КМЗІ, її особливостей та практичного значення *(Рис.1.3.3)*.

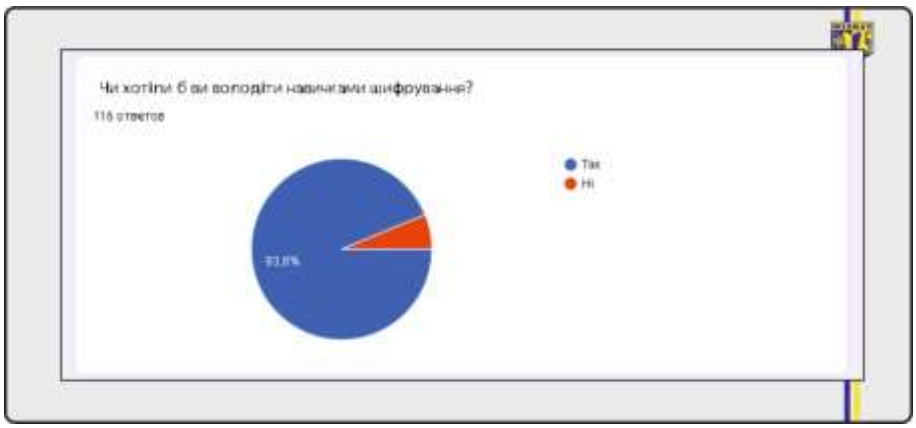

Рис.3.1.3. Показник зацікавленості

Аналізуючи результати представлених діаграм спостерігаємо актуальність гурткової роботи стосовно КМЗІ.

Управління Державної служби якості освіти у Сумській області надає рекомендації закладам освіти щодо розбудови внутрішньої системи забезпечення якості освіти. В ході проведеного дослідження було проведено бесіду з головою Сумського ДСЯО – Рябухою А.П. та головним спеціалістом сектору інформаційно-організаційного забезпечення Хроленко О.М., що висловили власну позицію щодо необхідності та актуальності введення курсу КМЗІ для учнів старших класів загальноосвітніх закладів (Додаток Г).

За твердженням керівника ДСЯО, ведення курсу дозволить оволодіти знаннями та вміннями, які створять теоретичне та практичне підґрунтя для отримання компетентностей щодо проведення аналізу загроз, які виникають при зберіганні, обробці та передаванні інформації; побудови систем захисту з використанням методів традиційної криптографії; демонстрації здатності критично вивчати, аналізувати і оцінювати з різних точок зору.

Хроленко О.М., головний спеціаліст сектору інформаційно-організаційного забезпечення, зазначає, що курс з КМЗІ повинен ознайомити учнів з

класичними та сучасними криптографічними системами, а також з новими перспективними напрямками розвитку криптології. На запитання «Чи буде доречним введення такого курсу для учнів старших класів, в якості гурткової роботи», зазначає, що це є необхідним та доречним.

3.2. Конспект уроку

План-конспект уроку з курсу проведення гурткової роботи «Криптографічні методи захисту інформації»

Тема уроку: Криптографія як передовий метод захисту інформації

Тип уроку: комбінований

Мета:

- *навчальна* полягає в формуванні знань та умінь учнів з теми КМЗІ; вивчення таких понять, як «захист інформації», «криптографія», «криптоаналіз», «криптологія»; засвоєння знань щодо основних способів ЗІ; ознайомлення з історією розвитку криптографії; ілюструванні видів криптосистем; роз'яснення практичного значення теми;
- *розвиваюча* передбачає розвиток логічного та алгоритмічного мислення, уяви учнів; передбачає виконання таких завдань, як вміння застосовувати набуті знання поза навчальним процесом;
- *виховна* мета за основу має стимулювання потреби в формуванні соціальної комунікації та культури мовлення; передбачає виконання таких завдань, як вміння працювати в колективі, висловлювати власну думку.

Форми навчання: фронтальна.

Методи навчання: пояснювально-ілюстративний, проблемно-пошуковий, інтерактивний, практичний.

Матеріальне забезпечення: персональний комп'ютер, методичний посібник.

Структура уроку		
1	Організаційний момент	2 хв.
2	Визначення теми та мети уроку	2 хв.
3	Вивчення нового матеріалу	20 хв.
4	Практична робота	15 хв.
5	Узагальнення вивченого матеріалу	3 хв.
6	Домашнє завдання	2 хв.
7	Підведення підсумків уроку	1 хв.

Хід уроку

І. Організаційний момент

Створення робочої атмосфери, перевірка присутніх на уроці, готовності методичного обладнання.

ІІ. Визначення теми та мети уроку

Тема сьогоднішнього уроку: «Криптографія як передовий метод захисту інформації». Сьогодні на уроці ми ознайомимося з поняттям криптографії та способами захисту інформації, проведемо екскурс в історію розвитку криптографії та проведемо роботу в групах над вивченням криптографічних алгоритмів.

ІІІ. Вивчення нового матеріалу

На сьогоднішній день гостро представлена проблема захисту інформації. Питанням захисту інформації, на сьогоднішній день, приділяється велика увага, і це не випадково. Телекомунікаційні системи, що активно розвиваються останнім часом, є артеріями сучасних глобальних інформаційних систем. Інформація, що циркулює в таких системах, становить суттєву цінність і тому є вразливою до різного роду зловживань. Тому саме в останні десятиліття стала настільки актуальною проблема захисту інформації.

Криптографічні методи, що спрямовані на захист інформації, займають одне з передових місць в сфері захисту інформації в цілому. Їх особливість полягає в незалежності від властивостей матеріальних носів інформації, а орудують лише її характеристиками.

Оскільки в сьогоденні комп'ютерні технології застосовуються в кожній сфері діяльності, без виключень, і приріст інформаційного оснащення зростає з кожним днем – стрімко зростає і попит на вивчення криптографії. На відміну від апаратних криптосистем, програмні засоби набули більшого застосування, адже немає потреби в великих фінансових витратах. Проблема реалізації криптографічних методів завжди залишатиметься актуальною, проте саме такі методи гарантують повний захист даних.

Будь-який користувач, навіть школяр, не раз стикається зі словами "шифр", "ключ", "криптограма" ...

(Запропонувати учням навести приклади використання цих термінів.)

Наприклад, ви користуєтесь мережею Internet; в меню багатьох засобів навігації Мережі задається питання щодо необхідності режиму шифрування, і якщо відповісти "потрібен", починається процедура створення ключа. Щоб правильно діяти, користувач повинен мати уявлення про основи криптографії.

Другий приклад, не менше яскравий - це банківські картки. Раніше картки були тільки магнітними і трималися на магнітній непідробності. Потім з'явилися інтелектуальні картки, в них вшитий процесор, який виконує криптографічні функції.

Третій приклад - цифровий підпис. Це у всіх на слуху, всі про це говорять, але не всі розуміють, що це таке, і тим більше не розуміють математичну основу. Цифровий підпис - це деяка криптографічна конструкція, але відмінна від шифрів, і від неї необхідні інші якості: не просто захист відкритого тексту, а й непідробність, захист від відмови від підпису. Саме це має виняткове значення у всіх справах, пов'язаних з використанням в бізнесі електронних документів.

Шифрувати необхідно лише ту інформацію, що потребує захисту. Зазвичай в таких випадках кажуть, що інформація містить таємницю, або що вона є захищеною, приватною, конфіденційною, таємною. Для найбільш типових ситуацій що зустрічаються введені такі спеціальні поняття, як державна таємниця, комерційна таємниця, юридична таємниця, тощо.

Для запобігання втрати інформації розробляються різні механізми її захисту, які використовуються на всіх етапах роботи з нею.

Для захисту інформації використовують різні способи захисту:

- контроль доступу;
- розмежування доступу;
- дублювання каналів зв'язку;
- криптографічне перетворення інформації за допомогою шифрів.

Проблемою захисту інформації шляхом її перетворення займається *криптологія*. Криптологія розділяється на два напрямки - криптографію та криптоаналіз. Мета цих напрямків прямо протилежна.

Розробкою методів перетворення (шифрування) інформації з метою її захисту від незаконних користувачів займається *криптографія.* Такі методи і способи перетворення інформації називаються *шифрами*.

Шифрування - процес застосування шифру до інформації, що захищається, тобто перетворення повідомлення, що захищається (відкритого тексту) в шифрування повідомлення (шифртекст, криптограму) за допомогою певних правил, що містяться в шифрі. Сфера інтересів криптоаналізу - дослідження можливості розшифровки інформації без знання ключів.

Дешифрування - процес, зворотний процес шифрування, тобто перетворення шифрованого повідомлення в початкову інформацію за допомогою певних правил, що містяться в шифрі.

Ще в стародавні часи збереженню важливої інформації надавали великого значення, та зберігали її в таємниці від сторонніх осіб. В часи, коли лише з’явилася писемність, з’явилася і необхідність захищати нову інформацію

від небажаного прочитання. Оскільки йдеться про початок самої писемності, то будь–які написи вважалися криптографію в оригінальному вигляді, адже володіли майстерністю письма одиниці.

Найпершим прикладом шифрування, що був документально зафіксованим є шифр Цезаря, що полягає в заміні кожної літери потрібного вихідного тексту віддаленою на k кроків, де k – ключ.

Також, відомим шифром є «Квадрат Полібія», автором якого вважають грецького письменника та філософа Полібія. Даний шифр є елементарним шифром заміни. В квадраті прописувалися букви відповідного алфавіту (наприклад, для грецького алфавіту розмір такого квадрату становив 5x5). Кожна літера вихідного тексту замінювалося на пару цифр – номер рядка і стовпчика, на перетині їх – зашифрована буква.

В стародавні часи широкого застосування знайшли різні найпростіші криптографічні пристрої.

Грецьким поетом Архілохом, що жив в VII столітті до н.е., згадується пристрій під назвою скитала (Рис.1.2.4). Достовірно відомо, що скитала використовувалася у війні Спарти проти Афін в кінці V століття до н. е. Даний пристрій являє собою циліндр і вузьку смужку пергаменту, що обмотують навколо нього по спіралі, на якій в свою чергу писалося повідомлення [20].

Зашифроване повідомлення писали на пергаментній стрічці по всій довжині палички, і після того як остання виявлялася вичерпаною, її повертали і продовжували писати повідомлення далі, поки воно не закінчиться, або поки не списувалася вся пергаментна стрічка, в разі чого використовувався наступний шматок такої ж стрічки. Для дешифрування адресат використовував паличку аналогічного діаметру, на яку потрібно було намотувавати пергамент, до тих пір, поки повідомлення не було прочитано. Такі народи як античні греки чи спартанці, використовували цей шифр за допомогою скитали, для зв'язку під час військових дій. Проте, як виявилося, такий шифр було легко зламати. Наприклад, перший метод злому скитали був запропонований ще Арістотелем. Він полягає в використанні конуса, який мав регулюючий діаметр, і навіть не

знаючи точного діаметру палички, що була використана при шифруванні, переміщаючи пергамент з повідомленням по його довжині текст почне читатися – таким чином знаходиться потрібний діаметр скитали.

Як на вашу думку, яка основна задача криптографії? *(Питання студентам)*

Відповідь: Завдання полягає в побудові абсолютно секретних криптографічних схем.

Криптосистеми поділяються на симетричні (з секретним ключем) і асиметричні (з відкритим і закритим ключем).

У симетричних криптосистемах для шифрування і дешифрування повідомлення використовується секретний загальний ключ.

В асиметричних криптосистемах для шифрування і дешифрування повідомлення використовуються різні ключі: для шифрування повідомлення використовується відкритий ключ, який є загальнодоступним, а для дешифрування повідомлення використовується закритий ключ, який є секретним.

IV. Практична робота

Практична робота передбачає використання нових знань та навичок в ході розв'язання завдань. Використовуючи навчальний посібник (Додаток Ґ), учні виконують Практичну роботу №1.

V. Узагальнення вивченого матеріалу

Фронтальне опитування:

1. В чому полягає сутність шифру Цезаря?
2. В чому полягає сутність шифрування за «квадратом Полібія»?
3. Назвіть криптографічні пристрої, та опишіть механізм їх роботи.

Отже, всі традиційні криптографічні системи можна поділити на:

- шифрування перестановкою;
- шифрування заміною;

- гамма-шифрування;
- шифрування аналітичним перетворенням

Шифрування перестановкою полягає в тому, що символи шифрованого тексту переставляються за певним правилом в межах деякого блоку цього тексту. При достатній довжині блоку, в межах якого здійснюється перестановка, і складному неповторним порядку перестановки можна досягти прийнятної для простих практичних застосувань стійкості шифру.

Шифрування заміною (підстановкою) полягає в тому, що символи шифрованого тексту замінюються символами того ж самого (проста заміна), також одного або декількох інших алфавітів (складна заміна) відповідно до заздалегідь обумовленої схемою заміни.

Гамма-шифрування полягає в тому, що символи шифрованого тексту складаються з символами деякої випадкової послідовності, іменованої гамою шифру. Стійкість шифрування визначається в основному довжиною (періодом) є повторюваною частини гами шифру. Даний спосіб є одним з основних для шифрування інформації в автоматизованих системах.

Шифрування аналітичним перетворенням полягає в тому, що шифрованого тексту перетворюється за певним аналітичним правилом (формулою). Наприклад, можна використовувати правило множення вектора на матрицю, причому матриця є ключем шифру, а символами множити вектора послідовно служать символи шифрованого тексту. Іншим прикладом може служити використання так званих односпрямованих функцій для побудови криптосистем з відкритим ключем.

VI. Домашнє завдання

В якості домашнього завдання учням запропоновано засвоєння знань, вивчених на занятті.

VII. Підведення підсумків уроку

Учням запропонована рефлексія:

Дайте відповідь на питання

1. Сьогодні я дізнався ...
2. Було зрозуміло ...
3. Було тяжко…
4. Я зрозумів, що…
5. Тепер я можу ...
6. Я хочу дізнатися …

Висновки до розділу 3

В представленому розділі розглянуто план реалізації та передумови щодо курсу «КМЗІ» для учнів старших класів загальноосвітніх закладів.

Відмітна особливість даного курсу полягає в тому, що рішення виділених в програмі завдань стане додатковим фактором формування позитивної мотивації до вивчення математики, розумінні єдності світу, усвідомленні положення про універсальність математичних знань. Не можна не відзначити прикладне та освітнє значення: розвиток логічного мислення учнів, використання міжпредметних зв'язків.

З метою підвищення пізнавальної активності учнів, формування здатності самостійного освоєння матеріалу школярі мають можливість познайомитися з науково - популярною літературою з проблеми застосування математики. Передбачається використання комп'ютерів в практичній частині курсу.

З метою профорієнтації учнів і для підготовки їх до професійної діяльності, учням запропоновано курс криптографії, за яким учні знайомляться з історією криптографії, вивчають найпростіші криптографічні системи і отримують навички вирішення криптографічних завдань.

ВИСНОВКИ

Криптографія сьогодні - це наука про забезпечення безпеки даних або, як кажуть, інформаційної безпеки. Шифрування, основна дія в криптографії, дозволяє забезпечити конфіденційність, зберігаючи інформацію потай від того, кому вона не призначена.

Криптографія набула нові сфери застосування і потрібна не тільки для захисту державних інтересів, а й необхідна для захисту приватного життя кожної сучасної людини.

Значення математичних основ криптографії має першорядне значення для учнів, які бажають досягнень успіху в програмах комп'ютерних наук із зосередження на безпеці.

Способи криптографії постійно ускладнюються. Зараз без шифрування і захисту інформації не може існувати жодне підприємство, що має будь-які цінні або наукові відомості. Необхідно внести матеріал по криптографії в навчальний план, для розвитку пластичності розуму і гнучкості мислення, що допоможе хлопцям при виборі будь-якої професії.

Актуальність цієї роботи обумовлюється виникненням протиріччя між зростаючими вимогами суспільства до рівня знань молодого покоління в області захисту інформації та сучасним станом процесу навчання в загальноосвітній школі з даного питання. Розгляд питань, пов'язаних з даною тематикою носить як теоретичну, так і практичну значимість. Висока значимість і недостатня практична розробленість цієї проблеми визначають безсумнівну новизну даного дослідження.

У нашому житті ми часто зустрічаємо шифри. Їх можна знайти в багатьох областях: граючи на музичних інструментах, читаючи літературні твори, знаходячи по координатам потрібне місце, вивчаючи генетичний код свого роду, спілкуючись за допомогою азбуки Морзе.

Курс «КМЗІ» має своєю метою дати учням знання в галузі теоретичної криптографії та криптоаналізу. Дисципліна знайомить з основними принципами

роботи криптографічних систем, математичними моделями джерел інформації, поняттями теоретичної та практичної секретності. Конкретні типи алгоритмів шифрування та криптографічних перетворень розглядаються у відповідності з їх класифікацією на класичні схеми, системи потокового шифрування, системи блочного шифрування та системи захисту інформації з відкритим ключем. Багато уваги приділяється криптографічним протоколам та їх застосуванням у захисті сучасних інформаційних технологій.

Поки конфіденційні дані вимагають захисту, криптографія буде продовжувати розвиватися.