Міністерство освіти і науки України
Сумський державний університет
Навчально-науковий інститут
бізнесу, економіки та менеджменту
Кафедра економічної кібернетики

# 5105 Методичні вказівки

до лабораторних робіт
із курсу «Безпека інформації»
для студентів усіх спеціальностей
денної форми навчання

Затверджено
на засіданні кафедри
економічної кібернетики
як лабораторні роботи із курсу
«Безпека інформації».
Протокол № 10 від 12.05.2021 р.

Суми
Сумський державний університет
2021

Методичні вказівки до лабораторних робіт із курсу «Безпека інформації» / укладач О. С. Кушнерьов. – Суми : Сумський державний університет, 2021. – 33 с.

Кафедра економічної кібернетики

**Зміст**

## Вступ

Розвиток суспільства не можна уявити без комп'ютерів, комп'ютерних мереж та інтернету. У повсякденному спілкуванні слово «інтернет» означає не лише глобальну мережу, що об'єднує мільйони комп'ютерів і локальних мереж усього світу, а єдиний глобальний інформаційний простір – сукупність взаємозв'язаних інформаційних ресурсів, програмного забезпечення, баз і банків даних, що обробляються в комп'ютерних мережах. З появою цього феномену величезна кількість користувачів одержали можливість дуже швидко одержувати потрібну інформацію з найбільш трастових і компетентних джерел. Мільйони людей можуть блискавично здійснювати обмін інформацією, спілкуватися незалежно від того, в якому місці земної кулі вони перебувають, переглядати книги і кінофільми, зберігати особисті фотоальбоми.

За короткий проміжок часу інтернет значно змінив наш спосіб життя, враховуючи робочі процеси, способи навчання та розваг. Останнім часом до інтернету здійснюється підключення не лише комп'ютерів, а й всіляких фізичних пристроїв – «речей», оснащених сенсорами, датчиками і пристроями передачі інформації, які людина може використовувати в повсякденному житті, наприклад, холодильників, кондиціонерів, автомобілів, велосипедів і навіть кросівок.

Усі види організацій та установ нині використовують цю мережу для ефективного функціонування, зокрема для збирання, оброблення, обміну та зберігання великої кількості цифрової інформації.

Проте поряд із перевагами сучасного цифрового світу і розвитком інформаційних технологій у цей час активно поширюються випадки незаконного збирання, зберігання, використання, знищення, поширення персональних даних, незаконних фінансових операцій, крадіжок і шахрайства в мережі Інтернет. Сучасні інформаційно-комунікаційні технології використовуються навіть для вчинення терористичних актів.

Хакерські атаки відбуваються щодня і здається, що в жодної організації немає від цього імунітету. З огляду на те, наскільки легко в сучасному світі зловмисники можуть викрадати і використовувати інформацію, зокрема персональні дані, в своїх цілях, занепокоєння про безпеку людей, процесів, даних і речей, підключених до інтернету, цілком природно.

Отже, захист інтересів держав і громадян у кіберпросторі стає життєво важливим завданням сьогодення.

**Метою навчання** є дослідження галузі інформаційної безпеки. Слухачі курсу зможуть дізнатися, як захищати в інтернеті свої особисті дані та власну особистість, ознайомитися з різними типами шкідливого програмного забезпечення, кібератак і методами організації захисту від них, дізнатися про методи соціальної інженерії, одержувати загальні уявлення про безпеку в інформаційному суспільстві й на цій основі сформувати розуміння технологій інформаційної безпеки і вміння застосовувати правила кібербезпеки в усіх сферах діяльності.

**Цілі:** формування в слухачів розуміння сутності, змісту і ролі інформаційної безпеки; набуття теоретичних і практичних осново з інформаційної безпеки; оволодіння технологіями захисту інформації.

Реалізація зазначених цілей передбачає виконання наступних завдань:

- аналіз основних загроз інформаційної безпеки;
- застосування здобутих знань для безпечної роботи з ПК у мережі Інтернет;
- застосування здобутих знань для методів соціальної інженерії.

**За результатами навчання слухачі повинні:**

***ЗНАТИ:***

- теоретичні основи забезпечення захисту інформаційних систем;
- методи захисту інформації в комп'ютерних мережах;
- сучасні методи соціальної інженерії, які використовують зловмисники;

- методи для одержання приватних даних через відкриті бездротові мережі Wi-Fi.

***УМІТИ:***

- використовувати нормативно-правові засади забезпечення захисту інформаційних систем у практичній діяльності;
- володіти основами організації захисту конфіденційної інформації;
- користуватися засобами протидії соціальної інженерії;
- володіти правилами користування відкритої бездротової мережі Wi-Fi.

## Тема 1. Розроблення політики інформаційної безпеки

**Мета** – набуття навичок та організаторських здібностей із розроблення комплексної програми захисту інформації.

**Теоретична частина**

Принципи забезпечення інформаційної безпеки містять: законність, баланс інтересів особи, суспільства і держави; комплексність; системність; інтеграція з міжнародними системами безпеки; економічна ефективність.

Неможливо створити систему, захист якої не можна буде зламати, основним принципом може бути створення такого механізму захисту, вартість злому якого буде дорожчою за інформацію, яку можна одержати. Тому необхідним є впровадження програмних засобів безпеки, які вмонтовані до складу програмного забезпечення системи і є потрібними для виконання функцій захисту. За словами експерта з кібербезпеки Дмитра Ганжело: «Усунення наслідків кібератак часто обходиться в кілька разів дорожче, ніж профілактика боротьби з ними.» В сучасних умовах, не гарантуючи належний захист інформації, не можливо забезпечити стабільний економічний розвиток як окремого підприємства, так і держави.

Розвиток ТЗІ в Україні обумовлюється такими основними чинниками:

- стрімким розвитком суспільних і міждержавних відносин;
- застосуванням технічних засобів оброблення інформації та засобів зв'язку іноземного виробництва;
- поширення засобів несанкціонованого доступу до інформації.

Існують також інші чинники. Нормативними документами у сфері ТЗІ визначені основні загрози безпеці інформації в Україні: діяльність інших держав, спрямована на отримання переваги в зовнішньополітичній, економічній, військовій та інших сферах; недосконалість організації в Україні міжнародних виставок апаратури різного призначення (особливо пересувних) і

заходів екологічного моніторингу, які можуть використовуватися для одержання інформації розвідувального характеру; діяльність політичних партій, суб'єктів підприємницької діяльності, окремих фізичних осіб, спрямована на отримання переваги у політичній боротьбі та конкуренції; злочинна діяльність, спрямована на протизаконне одержання інформації з метою досягнення матеріальної вигоди або заподіяння шкоди юридичним або фізичним особам; використання інформаційних технологій низького рівня, які призводять до впровадження недосконалих технічних засобів із захистом інформації, засобів контролю за ефективністю ТЗІ та засобів ТЗІ; недостатність документації на засоби забезпечення ТЗІ іноземного виробництва, а також низька кваліфікація технічного персоналу.

З метою протидії існуючим інформаційним загрозам в Україні триває процес створення системи ТЗІ. Система ТЗІ визначається як сукупність: суб'єктів, об'єднаних цілями і завданнями захисту інформації, організаційними та інженерно-технічними заходами; нормативно-правової бази; матеріально-технічної бази. Державна політика у сфері ТЗІ формується і реалізується з урахуванням таких принципів:

- дотримання балансу інтересів особи, суспільства й держави, їх взаємної відповідальності;
- єдності підходів до забезпечення ТЗІ, які зумовлені загрозами безпеці інформації та режимом доступу до неї;
- комплексності, повноти й безперервності заходів ТЗІ;
- відкритості нормативно-правових актів і нормативних документів із питань ТЗІ, які не містять відомостей, що становлять державну таємницю;
- узгодженості нормативно-правових актів і нормативних документів із питань ТЗІ з відповідними міжнародними договорами України;
- обов'язковості захисту інженерно-технічними заходами: інформації, яка становить державну та іншу передбачену законом таємницю;
- конфіденційної інформації, яка є власністю держави;

- відкритої інформації, важливої для держави, незалежно від того, де зазначена інформація циркулює;
- відкритої інформації, важливої для особи та суспільства, якщо ця інформація циркулює в державних органах, на підприємствах, в установах і організаціях;
- виконання на власний розсуд суб'єктами інформаційних відносин вимог щодо технічного захисту;
- ієрархічність побудови організаційної структури системи ТЗІ та керівництво її діяльністю в межах повноважень, визначених нормативно-правовими актами;
- методичне керівництво спеціально уповноваженим центральним органом виконавчої влади у сфері ТЗІ діяльністю організаційних структур системи ТЗІ;
- координація дій і розмежування сфер діяльності організаційних структур системи ТЗІ з іншими системами захисту інформації та системами забезпечення інформаційної та національної безпеки.

Спеціально уповноваженим центральним органом виконавчої влади, на який покладено відповідальність за формування та реалізацію державної політики у сфері ТЗІ, до 1 січня 2007 р. був Департамент спеціальних телекомунікаційних систем і захисту інформації Служби безпеки України (ДСТС ЗІ СБУ), а з 1 січня 2007 р. на базі та за рахунок кількості Департаменту спеціальних телекомунікаційних систем і захисту інформації і відповідних підрозділів Служби безпеки України відповідно до Закону України «Про Державну службу спеціального зв'язку та захисту інформації України» від 23.02.2006 р. створено Державну службу спеціального зв'язку та захисту інформації України (Держспецзв'язок).

Як суб'єкти в системі ТЗІ України є:

- Держспецзв'язок (колишній ДСТС ЗІ СБУ);
- органи, щодо яких здійснюється ТЗІ;
- державні наукові, науково-дослідні та науково-виробничі підприємства, установи та організації, що належать до

системи Служби безпеки України і виконують завдання технічного захисту інформації;
- військові частини, підприємства, установи й організації всіх форм власності і громадяни-підприємці, які здійснюють діяльність щодо технічного захисту інформації за відповідними дозволами або ліцензіями;
- навчальні заклади з підготовки, перепідготовки й підвищення кваліфікації фахівців із технічного захисту інформації.

Усі заходи, пов'язані із захистом інформації, що є власністю держави, координуються й контролюються Держспецзв'язком (колишнім ДСТС ЗІ СБУ). Основні завдання усіх суб'єктів системи ТЗІ України викладені в джерелі. Конкретними об'єктами захисту, зазвичай є не розрізнені носії інформації, а об'єднані загальними завданнями їх впорядковані сукупності. Тоді в цілому під об'єктом захисту розуміємо інформаційну систему (ІС), що реалізує автоматизоване збирання та оброблення даних, і що має: технічні засоби, програмне забезпечення, відповідний персонал і допоміжні засоби.

**Завдання**

Потрібно розробити комплексну політику інформаційної безпеки об'єкта дослідження, яким може бути установа – місце проходження навчальної (виробничої) практики студента. Під час розроблення політики безпеки установи потрібно розуміти, що вона повинна описувати ідеальний стан справ у вибраному об'єкті впровадження, а не наявний. Також необхідно враховувати організаційну структуру установи, для якої розробляється політика, бізнесові інтереси і пріоритети (зробити аспект на конфіденційності чи на інноваціях, наприклад, деякі банківські установи використовують програмне забезпечення лише розроблене власними програмістами).

## Тема 2. Дослідження функціональності існуючих криптографічних програм

**Мета** – набуття навичок із використання існуючих.

**Теоретична частина**

Криптовірологія (англ. Cryptovirology) — це наука, яке вивчає, як використовувати криптографію для розроблення потужного шкідливого програмного забезпечення. Дисципліна з'явилася з огляду на те, що криптографія з відкритим ключем може бути використана для порушення симетрії між сприйняттям шкідливих програм злочинцем та антивірусом. Аналітик антивірусу бачить відкритий ключ, який міститься в шкідливому програмному забезпеченні, а атакуючий бачить відкритий ключ, який міститься в шкідливій програмі, а також відповідний приватний ключ (поза зловмисним програмним забезпеченням), оскільки зловмисник створив ключову пару для атаки. Відкритий ключ дозволяє шкідливому програмному забезпеченню виконувати віддалені дії в односторонньому режимі на комп'ютері жертви, які можуть бути скасовані лише зловмисником.

Дисципліна також охоплює приховані атаки шкідливого ПЗ, в яких зловмисник непомітно краде конфіденційну інформацію, таку як, наприклад, симетричні ключі, закриті ключі, стан PRNG. Прикладами таких прихованих атак є асиметричні бекдори. Асиметричний бекдор — це бекдор (наприклад, у криптосистемі), який може використовуватися лише зловмисником, навіть після його виявлення. Це контрастує з традиційним бекдором, який є симетричним, тобто будь-хто, хто знаходить його, може його використовувати.

Клептографія, підполе криптовірології — це дослідження асиметричних бекдорів в алгоритмах генерації ключів, алгоритмах цифрового підпису, обміні ключами, генераторах псевдовипадкових чисел, алгоритмах шифрування та інших криптографічних алгоритмах. Відомий приклад асиметричного бекдора — це бекдор у генератор псевдовипадкових чисел Dual EC DRBG.

У комп'ютерній безпеці криптовірус визначається як комп'ютерний вірус, що містить і використовує відкритий ключ. Зазвичай відкритий ключ належить автору вірусу, хоча є й інші варіанти. Наприклад, вірус або черв'як можуть генерувати і використовувати свою власну пару ключів під час виконання. Криптовіруси можуть використовувати секретний канал, щоб приховати інформацію і можуть спілкуватися між собою.

Криптовірус, крипточерв або криптотроян містять публічний ключ, за допомогою якого шифруються дані на комп'ютері жертви методом асиметричної криптографії. Потім криптовірус вимагає в жертви гроші за розшифрування даних. Після отримання грошей зловмисник відправляє жертві свій приватний ключ, яким жертва розшифровує зашифровані криптовірусом дані. Тривіальний недолік цього методу в тому, що жертва може повідомити, наприклад в інтернеті іншим зараженим даними криптовірусом приватний ключ, що звільнить їх від необхідності платити за нього творцеві вірусу. Тому вже тоді в 1996 Моті Юнг і Адам Янг припустили, що криптовіруси майбутнього будуть використовувати методи симетричного та асиметричного шифрування за таким методом: зловмисник створює, наприклад, RSA пару ключів (публічний-приватний), криптовірус на комп'ютері жертви генерує випадковий таємний ключ, таємним ключем шифруються дані жертви. Потім таємний ключ шифрується публічним ключем. Для розшифрування даних жертві потрібно заплатити грошей зловмисникові за

розшифрування згенерованого вірусом таємного ключа приватним ключем зловмисника.

**Завдання**

Відповідно до виданого викладачем варіанта потрібно дослідити функціональну частину програм, що призначені для криптографічного захисту різного роду інформації. Програму потрібно встановити на віртуальну операційну систему Windows. Зробити звіт.

| Варіант | Програма |
|---|---|
| 1 | BestCrypt; fSekrit; Anubis 3.9.96 |
| 2 | SCARABAY; Dekart Private Disk 2.09; Ielogin 2.02 |
| 3 | Advanced Encryption Package 2008 Pro; Max File Encryption 1.8; Hide Folder 3.0.8 |
| 4 | Secure Disk; Aes-Up 2.0; CD Lock v03.01.2 |
| 5 | CryptoExpert 2008 Pro; КриптоАРМ v.4.0 Pre-Release; CryptoCrat 2.23 |
| 6 | Drive Encryption; PGP Desktop 9.5 beta; Articsoft FileAssurity OpenPGP 1.5 |
| 7 | Microsoft Private Folder 1.0; RIPcoder 1.5e |
| 8 | AutoKrypt; CryptoCard 2.4.0.0; Universal Shield 3.0; CodeSafe 7.31 |
| 9 | FineCrypt; STCLite 3.3; CryptoExpert 2008 Pro |
| 10 | Personal Passworder; Message Spy 4.2.1; Advanced Encryption Package 2008 Pro |
| 11 | Steganos Safe 2008; VDFCrypt 1.5.1; Drive Encryption |
| 12 | Cryptainer LE; DotFix FakeSigner; AutoKrypt |
| 13 | Crypt4Free; Nyx Password Storage 1.2; Aes-Up 2.0 |
| 14 | FlexWallet 2006; PolyEdit 5.0 RC Altiplano; CryptoCard |
| 15 | File Securer; SecurityPad 3.5; Hide Folder 3.0.8 |

## Тема 3. Розроблення програми для шифрування інформації

**Мета** – набуття навичок із шифрування інформації за одним із відомих алгоритмів.

**Теоретична частина**

Шифрування – це оборотне перетворення даних з метою приховування інформації. Шифрування відбувається з застосуванням криптографічного ключа. Ключ – це певна кількість символів, сформованих вільним чином з символів, що доступні в системі шифрування.

Припускають, що шифрування з'явилося приблизно 4 тис. років тому. Першою відомою пам'яткою шифрування прийнято вважати єгипетський текст, який було створено напевно десь в 1900 році до нашої ери, в якому використовувалися інші символи замість відомих єгипетських ієрогліфів. Загалом виділяють два методи шифрування: симетричне та асиметричне.

У симетричному шифруванні один ключ, який зберігається в секреті, служить і для шифрування, і для дешифрування. Симетричні алгоритми шифрування можна класифікувати на потокові та блочні. Потокові алгоритми шифрування поетапно опрацьовують текстове повідомлення. Блочні алгоритми співпрацюють із блоками зафіксованого розміру, найчастіше розмір блока дорівнює 64 бітам.

Симетричні алгоритми шифрування також можуть використовуватися не самостійно. У новітніх криптосистемах застосовують комбінації симетричних та асиметричних алгоритмів з метою отримання переваг обох схем.

У симетричному шифруванні можна виділити деякі переваги, такі як велика пропускна здатність, завдяки спеціальному проєктуванню; ключі мають невеликий розмір; ці шифри можна застосовувати як основу для будування

різноманітних криптографічних механізмів, включаючи з випадковими генераторами чисел, обчислювально-ефективними схемами розпису та тому подібне.

Серед недоліків цього шифрування потрібно відзначити те, що у кожній немаленькій мережі необхідно використовувати значну кількість ключів; під час зв'язку між декількома особами необхідно досить часто змінювати ключі; коли існує зв'язок між двома особами ключ потрібно засекречувати на двох кінцях.

До симетричних алгоритмів шифрування належать: Twofish, Serpent, AES (або Рейндайль), Blowfish, CAST5, RC4, TDES (3DES), та IDEA.

Асиметричне шифрування, або метод відкритого ключа, передбачає застосування в парі двох відмінних ключів, а саме секретний і відкритий. Відповідно до назви відкритий ключ безперешкодно розміщують у мережі, логічно, що секретний ключ увесь час тримається в таємниці. В асиметричному шифруванні ключі співпрацюють у парі, тобто коли інформація шифрується відкритим ключем, то розшифровування відбувається лише відповідним секретним ключем і навпаки. Неможливим є використовування відкритого ключа з однієї пари та секретного ключа з іншої пари. Математичними залежностями пов'язані всі пари асиметричних ключів.

Принцип роботи асиметричного шифрування можна простежити на прикладі роботи кейсу, для якого застосовують два ключі, першим кейс зачиняють, а другим – відчиняють.

Через певні вади швидкості дії асиметричного методу, його доводиться застосовувати разом із симетричним, так як він працює на декілька порядків швидше.

Необхідно відзначити певну проблему, яка виникає під час потрібності передачі ключа для розшифровування інформації. Під час передачі ключ може бути захоплений зловмисником.

Асиметричне шифрування допомагає одержувачеві контролювати цілісність інформації, яка передається.

До асиметричних алгоритмів шифрування належать RCA та ECC.

**Завдання**

Потрібно написати програму, що шифрує/дешифрує інформацію. Як вхідна інформація може бути довільна форма висловлювання. Як алгоритм шифрування можна взяти один із відомих алгоритмів.

Для написання програми можна використовувати будь-яку мову програмування.

## Тема 4. Пошук шахраїв на торгових площадка

**Мета** – навчитись аналізувати профілі на торгових площадках для виявлення шахраїв.

**Теоретична частина**

У контексті інформаційних технологій соціальна інженерія – це загальна кількість підходів щодо прикладних соціальних наук, які орієнтовані на спрямовану зміну організаційних структур, що визначають людську поведінку та надають контроль за нею.

Методика застосування маніпуляцією свідомістю використовувалася завжди: навіть у давнину. Багато хто досить активно застосовував ці методи для людського розуму, наприклад із гіпнозом. У Стародавній Греції та Римі у великій пошані були люди, які могли різними способами переконати співрозмовника в його очевидній неправоті. Виступаючи від імені верхів, вони вели дипломатичні переговори. Уміло використовуючи брехню, лестощі та вигідні аргументи, вони нерідко вирішували такі проблеми, які, здавалося, неможливо було вирішити без допомоги меча.

У сфері інформаційної безпеки для описання науки і психічної маніпуляції використовується термін «соціальна інженерія». За статистикою аналітичного центру компанії Infowatch 55 % збитків, пов’язані з порушеннями інформаційної безпеки, виникають по вині працівників, які мали вплив від соціальних інженерів.

Метою соціальної інженерії є спонукання людей робити певні дії, які вони за звичних умов ніколи не вчинили, наприклад, розголошувати власну конфіденційну інформацію, переходити на невідомі сайти та за сумнівними посиланнями. Вся система соціальної інженерії базується на тому факті, що саме людина є найслабкішою ланкою будь-якої системи інформаційної чи кібербезпеки. Саме тому за умови, що технічно одержувати

конфіденційну інформацію хакерам досить важко, вони впливають безпосередньо на користувача – найслабкіше місце в системі інформаційної безпеки.

**Завдання**

На торгових площадках (OLX, Prom.ua, тощо) знайти підозрілі товари та профілі можливих шахраїв. Перевірити зазначений у профілі номер телефону в пошукових системах та за відгуками інших користувачів визначити чи належить даний номер телефон шахраю. Виявити шаблони, які використовують шахраї. Зробити звіт.

## Тема 5. Аналіз методів, які використовують шахраї в соціальній інженерії

**Мета** – ідентифікувати методи соціальної інженерії.

**Теоретична частина**

Основні техніки соціальної інженерії включають в себе:

1. Фішинг-атаки – цей вид шахрайства є найбільш поширений у соціальній інженерії. Фішингова атака полягає в незаконному одержані конфіденційних даних користувача. Це може бути логін і пароль. Дуже часто фішингові листи можуть містити граматичні помилки. В таких листах зловмисники надають гіперсилку на відповідну копію сайта (наприклад, поштового клієнта) з формою, в якій необхідно ввести свій логін, пароль та іншу особисту інформацію. Одним із прикладів фішингу є збір логінів і паролів користувачів, саме шляхом розсилання листів і повідомлень, які спонукають потенційну жертву повідомити необхідну інформацію. Щоб унебезпечити користувача від таких зловмисників, необхідно ігнорувати листи від невідомих адресатів.

2. Претекстинг – це така атака, яку проводять за завчасно підготовленим сценарієм. Такі атаки націлені на появу почуття довіри потенційної жертви до зловмисника. Такі атаки зазвичай здійснюють по телефону. Такий метод зазвичай не вимагає від зловмисника попередньої підготовки і щодо пошуку даних про жертви. Основна ідея претекстинг полягає у видачі себе за іншу людину з метою одержання бажаних даних.

Джерела відкритого доступу є способом одержати інформацію про людину. Зазвичай в основному – це сторінки соціальних мереж.

3. Троянський кінь. Ця техніка заснована на якості цікавості жадібності потенційної жертви. Соціальний інженер може відправити електронний лист, який містить безкоштовне відео або оновленням будь-якої програми у вкладенні. Потенційна

жертва зберігає ці файли, які є троянськими програмами. Така техніка буде залишатися ефективною до того часу, поки відповідні користувачі будуть бездумно зберігати або відкривати будь-які вкладення.

4. Квипрокво. Під час застосування такого виду атаки зловмисники можуть обіцяти жертві якусь вигоду в обмін на факти. Зазвичай зловмисник може подзвонити в будь-яку компанію та відрекомендуватися співробітником IT-компанії і запропонувати встановити «необхідне» програмне забезпечення. Як тільки зловмисник отримає згоду на виконання такої роботи, порушник може отримати доступ як до системи, так і до усіх даних, що зберігаються в ній.

5. Tailgating (зворотний зв'язок) – це несанкціонований прохід на територію зловмисника разом із користувачем, який має права на доступ через пропускний пункт.

6. Плечовий серфінг. Такий вид застосовують у різноманітних громадських місцях. Це дозволяє зловмиснику спостерігати за комп'ютерними пристроями і телефонами через плече потенційної жертви. Інколи є ситуації, коли користувач сам пропонує зловмиснику потрібну інформацію, думаючи про порядність людини. У такому разі можна говорити про зворотну соціальну інженерію.

7. Служби миттєвого обміну повідомленнями. Сьогодні всі користувачі використовують обмін повідомленнями в режимі реального часу за допомогою мереж Skype, Viber, WhatsApp, Telegam та ін. Доступність і швидкість такого способу спілкування робить такі служби відкритими для різноманітних атак. Як рекомендація щодо безпеки краще ігнорувати повідомлення від невідомих користувачів, а також не повідомляти їм особисту інформацію, не переходити за надісланими посиланнями.

**Завдання**

Провести аналіз власних смс-повідомлень, повідомлень або дзвінків на наявність шахрайства. Дізнатися у родичів чи

друзів, чи дзвонили або писали їм шахраї. Про що саме йшла мова (заблоковані платіжні картки, виграш автомобіля або великої грошової суми тощо). Визначити в який переважно час були дзвінки від шахраїв. Якщо було повідомлення або дзвінок від шахрая про заблоковану платіжну картку, чи повідомляли ви чи ваші близькі про шахрая банку яким користуєтесь. Виявити шаблони, які використовують шахраї. Зробити звіт.

## Тема 6. Аналіз сайтів, які використовують найбільше

**Мета** – виявити сайти вразливі до перехвату даних.

**Теоретична частина**

Відомий спеціаліст з кібербезпеки Патрик Ф. Уілбур (Patrick F. Wilbur) проводив експеримент із перехоплення публічного трафіку Wi-Fi. Патрик Ф. Уілбур організував виключно з метою оцінювання рівня безпеки в інтернеті. Він перехоплював та аналізував трафік публічної мережі Wi-Fi впродовж кількох годин. І ніхто не лише не подзвонив у поліцію, а навіть не звернув на нього увагу. Люди заходили на свої улюблені сайти, такі як Netflix та Google, через протокол HTTP, здійснювали телефонні дзвінки й взагалі надсилали через інтернет купу нешифрованого трафіку, який можна було перехопити та модифікувати для подальших фішингових або vishing-атак.

Багато хто неправильно вважає, що увесь веб-трафік шифрується і тому можна спокійно пересилати конфіденційні дані навіть у публічних місцях. На жаль, експеримент призвів до вельми негативних висновків: величезний обсяг онлайн-трафіку є сьогодні абсолютно незашифрованим й це залишає великий ризик кібератаки.

У межах свого експерименту Патрик Уілбур установив SSID-ідентифікатор «Вільний гостьовий Wi-Fi». Така назва мережі є досить популярною та прийнятною. Під час під'єднання автоматично відкривалася pop-up-сторінка, що містила небагатослівну угоду про те, що користувач повинен погодитися з тим, що в мережі будуть відстежуватися його дані та комунікації.

Загалом, це був дуже дружній спосіб проведення експерименту. Справжній хакер був би набагато агресивнішим.

Щоб додатково захистити конфіденційність користувачів, Патрик Уілбур написав невелику програму для збирання

статистичних даних про протоколи та порти, що застосовували в мережі програмними додатками кінцевих споживачів.

Ця програма не записує жодних IP-адрес, MAC-адрес, імен хостів або інформації додатків і не може бути налаштована таким чином, щоб зробити це. Вона призначена лише для однієї мети – узагальнити типи пакетів і портів, що використовуються, найменш інтрузивним способом.

Як виявилося, є дуже багато охочих під'єднатися до відкритої мережі Wi-Fi. Впродовж одного дня було отримано таку статистику:

- усього під'єднано 49 пристроїв;
- усі 100 % прийняли умови у pop-up-вікні та надіслали дані;
- нуль пристроїв використовували VPN.

Дехто помітить, що в цю статистику увійшли лише ті особи, які свідомо вибрали відкриту мережу та поставили відповідну позначку на pop-up-сторінці. Та люди, які обирають публічні мережі, більш імовірно здатні виконувати ризиковані дії в інтернеті. До речі, через те, що для під'єднання до мережі потрібно було підтвердити угоду на pop-up-сторінці, це виключало зі статистики будь-які автоматичні пристрої типу Internet of Things (IoT).

На жаль, HTTPS недостатньо для повного захисту. Насправді, ця технологія неправильно реалізована навіть на великих сайтах, які всім добре відомі та яким ви довіряєте.

Крім того, близько 42 % всього трафіку, що пройшов через мережу через вищезгаданий «гостьовий Wi-Fi», був нешифрованим HTTP-трафіком.

Після збору 489330 IP-пакетів виявилося, що:

- понад 42 % трафіку від загального обсягу на 80-му порту (Port 80) відносився до незашифрованого HTTP (проти майже 57 % на Port 443, що використовується протоколом HTTPS);
- 2638 пакетів — не шифровані пакети DNS;
- 18 пакетів належили до нешифрованих пакетів NTP-протоколу.

Оскільки протоколи DNS та NTP є небезпечними, а 42 % трафіку – це потенційно незашифрований трафік HTTP, що надсилається через порт 80, така статистика справді дуже турбує. А як щодо політик HTTP Strict Transport Security (HSTS), які повинні застосовувати веб-браузери?

Якщо вивчити поведінку декількох популярних веб-сайтів, то виявиться, що:

- популярні веб-сайти не завжди впроваджують HTTPS належним чином, якщо взагалі впроваджують (це містить, зокрема Google та Netflix);
- користувачі загальнодоступних мереж Wi-Fi залишаються вразливими до атаки MITM (man-in-the-middle), перехоплення приватних даних та інших атак.

Крім того, є й альтернативна статистика. Google використовує анонімну звітність користувачів Chrome, щоб виявити частоту застосування HTTPS в інтернеті.

Відповідно до власного звіту Google (станом на 29 грудня 2018 року):

- 11–31 % усіх веб-сайтів відвідуються без шифрування (доступ через незашифрований HTTP);
- ~ 7 % трафіку до сервісів Google не шифрується (навіть до 10 % для деяких продуктів Google);
- 82,6 % цього трафіку походить із мобільних пристроїв (що змушує з великим скептицизмом дивитися на використання мобільної ОС, розробленої Google).

Базова безпека в інтернеті останнім часом значно покращилася, але все ж таки недостатньо. Досі існують величезні проблеми, які не вдалося вирішити. Тому в публічних мережах Wi-Fi навіть сьогодні зловмисник може:

- дізнатися, які сайти ви відвідуєте (просто перехопивши запити DNS);
- здійснити атаки типу MITM (людина посередині) в момент завантаження сторінки HTTP;

- обмежити запобіжні можливості HSTS, вводячи фальшивий майбутній час через сервіс NTP (адже політики HSTS мають обмежений час дії);
- виконати фішинг-атаку для збирання конфіденційної інформації;
- провести телефонну атаку типу vishing на вас, ваших друзів чи вашу родину;
- ввести фальшивий вміст/рекламу або навіть майнити криптовалюту, використовуючи ваш процесор;

обдурити вас та спонукати працювати з небезпечними плагінами, наприклад, застарілою версією Flash.

**Завдання**

Проаналізувати сайти, якими ви користуєтесь. Визначити часту сайтів, які мають захищений протокол https та ті, які не мають захищений протокол https. Чи всі сайти, на яких ви проводите онлайн-платежі (покупки в інтернет-магазині, оплата комунальних чи інших платежів, користування електронними гаманцями, сервісами для поповнення електронних гаманців, банківських карток чи балансу мобільного зв'язку, сервісу переказу грошей тощо). Зробити звіт.

## Тема 7. Аналіз власної мережі Wi-Fi на вразливість

**Мета** – виявлення слабких місць бездротової мережі Wi-Fi.

**Теоретична частина**

Існують два різновиди протоколу WPA: WPA2 Personal та WPA2 Enterprise. Їх відмінність полягає в використовуваних ключах шифрування. У невеликих приватних мережах застосовують статичний ключ довжиною 8 символів, яким може бути кодове слово, пароль, PSK (Pre-Shared Key), що задається в налаштуваннях точки доступу і однаковий у всіх клієнтів цієї бездротової мережі. Такий ключ легко скомпрометувати.

У корпоративних мережах використовують динамічний ключ, який унікальний для кожного бездротового клієнта, що працює в даний момент. За генерацію ключа відповідає сервер авторизації, зазвичай – це RADIUS-сервер. Протокол WPA2 також не позбавлений вразливостей. Одна з вразливостей була виявлена в 2008 році, яка дозволяла провести атаку «людина посередині». Для експлуатації цієї уразливості атакуючий повинен бути зареєстрований у цій мережі. Уразливість дозволяє учасникам мережі перехоплювати та розшифрувати дані, що передаються між іншими учасниками мережі з використанням їх Pairwise Transient Key.

Отже, щоб зламати мережу з OpenAuthentication, NoEncryption – нічого не потрібно, крім під'єднання до мережі. Під час використання шифрування WEP, необхідний час лише на перебір вектора ініціалізації. Під час використання шифрування TKIP або AES пряме дешифрування можливо, але важко. Внаслідок проведеного аналізу можна зробити висновок, що під час експлуатації Wi-Fi мереж рекомендується використовувати протокол захисту WPA2. Проте, вразливість протоколів захисту

мереж Wi-Fi не є єдиною вразливістю цього виду мереж. Однією з проблем їх безпеки є проблема з роутерами. Найпоширенішою проблемою з захистом роутерів залишаються заводські налаштування. Це не лише загальні для всієї серії пристроїв внутрішні IP-адреси, паролі та логін admin, але також активовані сервіси, що підвищують зручність ціною безпеки. Крім того, в роутерах є прошивки, які можуть також стати джерелами вразливостей. Роутери, що використовують протокол Universal Plug and Play (UPnP), схильні до низки вразливостей.

**Завдання**

Потрібно провести аудит безпеки власної мережі Wi-Fi. Виявити слабкі місця в захисті роутера. Перевірити пароль на стійкість до Brute force. Дізнатися версію операційної системи та за можливості знайти exploit для отримання доступу до вашого роутеру. Зробити звіт.

## Тема 8. Складання інформаційного досьє

**Мета** – набуття навичок збирання та аналізу персональної інформації із загальнодоступних джерел; формування відповідального відношення до діяльності, пов'язаної з обробленням і зберіганням інформації; набуття навичок профілактичної та попереджувальної діяльності щодо інформаційних загроз на рівні особистої інформаційної безпеки.

**Теоретична частина**

Поняття «соціальні мережі» вперше ввів соціолог Джеймс Барнс: «Соціальна мережа (Social Network) – це соціальна структура, що складається з групи вузлів, якими є соціальні об'єкти (люди або організації), і зв'язків між ними». У найпростішій формі соціальна мережа – це карта всіх релевантних зв'язків між вузлами. Формально соціальна мережа являє собою граф S (G, E), в якому G = {1, 2,..., n} – множина вершин (агентів) і E – безліч ребер, що відображають взаємодію агентів.

Агент – це вузол соціальної мережі (вершина графа). Агентами можуть стати різні субагенти, наприклад, сім'ї, групи, організації. Зв'язки між агентами – це відносини, наприклад, знайомство, дружба, співпраця, комунікації. Агенти залежно від інформації, якою вони володіють, можуть впливати на прийняття рішення, на інших агентів, інформаційне управління та інформаційне протиборство. Якщо розглядати соціальну мережу більш глибоко, можна виявити, що зв'язки діляться за типами: односторонні та двосторонні; мережі друзів, знайомих, колег, однокласників, однокурсників, однодумців тощо. Соціальна мережа – це ще й засіб спілкування. Будь-якій людині емоційно важлива думка інших людей, зокрема, коли все добре – їх визнання, а коли наступила смуга невдач – співчуття і співучасть.

Ритм життя стає таким, що часу на традиційне спілкування з друзями зараз залишається все менше і менше. І соціальні

мережі з цієї точки зору – незамінна річ, оскільки дають можливість спілкуватися, не витрачаючи часу на дорогу, не погоджуючи зручні проміжки часу. Одним із результатів взаємодії людей за допомогою таких мереж є одержання величезної кількості інформації різних форматів: тексти, картинки, аудіо, відео та ін. Сьогодні соціальні мережі надають користувачам широкий функціонал для обміну інформацією, їх відвідує більш ніж дві третини онлайн-аудиторії у всьому світі, і це четверта за популярністю онлайн-категорія після пошукових та інформаційних порталів і програмного забезпечення.

На першому етапі соціальна мережа попросить вас заповнити ваш профіль. Які дані необхідні? Звісно ж, прізвище, ім'я, по батькові, рік народження. Де народилися, де вчилися. Фото, друзі, родина. А що ви зазначаєте в полі «пароль» і «контрольне запитання»? Свій день народження і дівоче прізвище матері? Так вони ж у вас на головній сторінці в профілі опубліковані! Фактично ви самі віддали їх зловмисникові. Які ще є стандартні контрольні питання? Кличка улюбленої тварини? Улюблене чоловіче (жіноче) ім'я? Все це легко знайти у вашому профілі, якщо неуважно поставитися до цінності інформації, яку ви публікуєте. Тому пароль повинен бути досить складним, не містити жодних персональних даних, на зразок імені або дня народження, і відповідь на контрольне запитання повинні знати тільки ви. Також під час заповнення профілю особливу увагу потребує приділити налаштуванням приватності – хто може бачити ваші фото, хто може їх коментувати, хто має доступ до вашої інформації – будь-хто чи лише ваші друзі?

Перше, на що звертають увагу – на профіль у соцмережі. З аватарки (зображення користувача), дати народження, роду занять і груп, в яких зареєстрований користувач, зрозуміло, чим живе і займається та чи інша людина. У середньому, досвідченому зловмиснику достатньо дві-три хвилини, щоб оцінити «корисність» цілі. Загалом, ці дві хвилини найбільш важливі, оскільки показавши про себе інформацію також, що ти маєш велике коло знайомств, то знай – ти їхній «клієнт».

Тим не менше, не стати «клієнтом» досить просто – достатньо не надавати реальної інформації про себе або надавати її частково.

**Завдання**

Перед студентами ставлять завдання зібрати і систематизувати як можна більше інформації один про одного з використанням загальнодоступних інтернет-ресурсів (сайтів соціальних мереж, блогів тощо), оцінити загрозу злочинного застосування інформації та виробити рекомендації щодо забезпечення необхідного рівня безпеки приватного життя.

Для виконання лабораторної роботи студенти розбиваються на пари.

**Перше завдання.** Знайти якомога більше особистої інформації про колегу, використовуючи загальнодоступні мережеві ресурси:

- пошукові системи (google.com.ua та ін.);
- соціальні мережі: linkedin.com, facebook.com, twitter.com та ін.;
- сайти професійних спільнот;
- сайти шкіл та ВНЗ;
- інші джерела.

**Завдання друге.** Створити з використанням зібраної інформації досьє з такими основними розділами:

- П.І.П/б, дата народження, сімейний стан, місце проживання, контактна інформація, перелік профілів у соціальних мережах;
- професія, області професійних інтересів, життєві цілі;
- коло спілкування: родичі, друзі, колеги, знайомі;
- улюблені місця відпочинку, пристрасті в їжі, одязі, музиці та ін.;
- розпорядок типового дня;
- фотографії;
- інше.

**Третє завдання.** Оцінити можливість використання знайденої інформації зовнішніми користувачами, наприклад:

- правоохоронними органами;
- роботодавцями;
- розповсюджувачами рекламної продукції;
- зловмисниками (шахраями, злодіями) тощо.

**Четверте завдання.** Передати зібрані матеріали «колезі» та отримати досьє з інформацією про себе. Оцінити рівень конфіденційності, актуальності та достовірності зібраної інформації. Проаналізувати висновки колеги про можливість використання знайденої інформації зовнішніми користувачами, зокрема і зловмисниками. Оцінити рівень впливу цифрових технологій на своє приватне життя і продумати кроки щодо забезпечення бажаного рівня безпеки.

**Підсумки.** Внаслідок виконання лабораторної роботи студенти повинні:

- навчитися дивитися на свої персональні дані з позиції зломщика;
- зрозуміти важливість забезпечення особистої інформаційної безпеки в сучасному суспільстві.

Навчальне видання

**Методичні вказівки**
до лабораторних робіт
із дисципліни «Безпека інформації»
для студентів усіх спеціальностей
денної форми навчання

Відповідальний за випуск О. В. Кузьменко
Редактор Н. М. Мажуга
Комп'ютерне верстання О. С. Кушнерьов

Підписано до друку 18.08.2021,  поз.
Формат 60х84/16. Ум. друку. арк. 2,99. Обл.-вид. арк. 1,95.
Тираж 6 пр. Зам. №

Видавець і виготовлювач
Сумський державний університет,
вул. Римського-Корсакова, 2, м. Суми, 40007
Свідоцтво суб'єкта видавничої справи ДК № 3062 від 17.12.2007.