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

Кушнерьов О. С.

БЕЗПЕКА ІНФОРМАЦІЇ

Конспект лекцій

Суми
Сумський державний університет
2021

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

БЕЗПЕКА ІНФОРМАЦІЇ

Конспект лекцій
для студентів усіх спеціальностей
денної форми навчання

Затверджено
на засіданні кафедри
економічної кібернетики
як конспект лекцій
із дисципліни «Безпека
інформації».
Протокол № 10 від 12.05.2021.

Суми
Сумський державний університет
2021

Безпека інформації : конспект лекцій / укладач О. С. Кушнерьов. – Суми : Сумський державний університет, 2021. – 99 с.

Кафедра економічної кібернетики

Зміст **С.**

РОЗДІЛ 1. ОСНОВНІ ПОНЯТТЯ ТА СТРУКТУРА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1. Терміни та визначення

Словосполучення «інформаційна безпека» в різних контекстах може мати різне значення.

У цьому курсі наша увага буде зосереджена на зберіганні, обробленні та передаванні інформації незалежно від того, якою мовою (українською чи будь-якою іншою) вона закодована, хто або що є її джерелом та який психологічний вплив вона має на людей. Тому термін «інформаційна безпека» використовують у вузькому змісті, так, як це прийнято, наприклад, в англомовній літературі.

Під інформаційною безпекою ми будемо розуміти захищеність інформації й інфраструктурою, яка її підтримує від випадкових або навмисних впливів природного або штучного характеру, які можуть завдати неприйнятної шкоди суб'єктам інформаційних відносин, зокрема власникам і користувачам інформації й підтримувальної інфраструктури. (Далі ми пояснимо, що варто розуміти під підтримувальною інфраструктурою).

Захист інформації – це комплекс заходів, спрямованих на забезпечення інформаційної безпеки.

Отже, правильний із методологічної точки зору підхід до проблем інформаційної безпеки починається з виявлення суб'єктів інформаційних відносин й інтересів цих суб'єктів, пов'язаних із використанням інформаційних систем (ІС). Загрози інформаційної безпеки – це зворотний бік використання інформаційних технологій.

Із цього положення можна вивести два важливі висновки:

1. Трактування проблем, пов'язаних з інформаційною безпекою, для різних категорій суб'єктів може істотно розрізнятися. Для ілюстрації досить зіставити режимні

державні організації й навчальні інститути. У першому випадку «нехай краще все зламається, ніж ворог довідається хоч один секретний біт», у другому – «так немає в нас ніяких секретів, аби тільки все працювало».

2. Інформаційна безпека не зводиться винятково до захисту від несанкціонованого доступу до інформації, це принципово більш широке поняття. Суб'єкт інформаційних відносин може постраждати (зазнати збитків й/або одержати моральний збиток) не лише від несанкціонованого доступу, а й від поломки системи, що викликала перерву в роботі. Більше того, для багатьох відкритих організацій (наприклад, навчальних) власне захист від несанкціонованого доступу до інформації перебуває по важливості аж ніяк не на першому місці.

Повертаючись до питань термінології, відзначимо, що термін» комп'ютерна безпека» (як еквівалент або замінник ІБ) видається нам занадто вузьким. Комп'ютери – лише одна зі складових інформаційних систем, і хоча наша увага буде зосереджена насамперед на інформації, що зберігається, обробляється й передається за допомогою комп'ютерів, її безпека визначається всією сукупністю складових й, насамперед, найслабшою ланкою, якою переважно є людина, яка написала, наприклад, свій пароль на «гірчичнику», наклеєному на монітор.

Відповідно до визначення інформаційної безпеки вона залежить не лише від комп'ютерів, а й від інфраструктури, яка її підтримує, до якої можна віднести системи електро-, водо- і теплопостачання, кондиціонери, засоби комунікацій і звичайно обслуга. Ця інфраструктура має самостійну цінність, але нас цікавить не лише те, як вона впливає на виконання інформаційною системою запропонованих їй функцій.

Звернемо увагу, що у визначенні ІБ перед іменником «збиток» стоїть прикметник «неприйнятний». Вочевидь, застрахуватися від усіх видів збитків неможливо, тим більше неможливо зробити це економічно доцільно, коли вартість захисних засобів і заходів не перевищує розмір очікуваного

збитку. Тому із чимось доводиться миритися й захищатися потрібно тільки від того, з чим змиритися ніяк не можна. Іноді таким неприпустимим збитком є нанесення шкоди здоров'ю людей або стану довкілля, але частіше поріг неприйнятності має матеріальне (грошове) вираження, а метою захисту інформації стає зменшення розмірів збитків до припустимих значень.

Захист інформації є важливою складовою частиною підтримання національної безпеки України. Організація захисту інформації здійснюється за допомогою системи правових, організаційних та інженерно-технічних заходів. Реалізація організаційних та інженерно-технічних заходів становить суть процесів технічного захисту інформації. Правові заходи захисту інформації є базисом, на який спираються організаційні та інженерно-технічні заходи захисту інформації. Що ж є об'єктом захисту? На сьогодні існує декілька сотень варіантів визначення суті терміна «інформація».

Одне з визначень таке: інформація – це зафіксоване на носії уявлення про предмети, процеси, події, явища тощо. Під фіксацією (від лат. fixus – міцний, закріплений) розуміють закріплення чого-небудь у певному положенні або вигляді. Найпростішим прикладом є письмове закріплення відомостей, думок. Інформація для свого функціонування завжди вимагає наявності носія. Водночас носієм інформації може бути поле або речовина. У деяких випадках як носій інформації може розглядатися людина. У процесі інформаційних відносин носії можуть бути або носіями-джерелами, або носіями-одержувачами залежно від напряму переміщення інформації.

У Законі України «Про інформацію» під джерелами інформації розуміємо передбачені або встановлені Законом носії інформації: документи або інші носії інформації, які є матеріальними об'єктами, що зберігають інформацію. Щодо одержувачів, то вони сприймають інформацію через той чи інший сенсор (датчик, вимірювальний перетворювач). Процес сприйняття є досить складним, враховуючи процеси приймання

та перетворення інформації, що забезпечує віддзеркалення об'єктивної реальності й орієнтування в довкіллі.

Сприйняття може містити:

- виявлення об'єкта в полі сприйняття;
- розрізнення окремих ознак усередині об'єкта;
- виділення в ньому інформативного змісту, адекватного меті дії;
- формування образу сприйняття.

У наведеному вище визначенні терміна «інформація» під уявленням розуміємо образ та/або суть предмета, процесу, події, природного явища тощо, сприйняті датчиками приладів або безпосередньо органами чуття, а також створені відтворювальною і/або творчою уявою людини чи елементами штучного інтелекту різних пристроїв.

Водночас уява – це психічна діяльність, що полягає в створенні уявлень та уявних ситуацій, яка в цілому не сприймалася людиною в реальній дійсності (творча уява) або відтворюють колишні враження і спогади, що спираються на життєвий досвід (відтворювальна уява). Як бачимо з вищевикладеного, вчені аналітично розрізняють відтворювальну й творчу уяву, але насправді обидва ці компоненти тісно взаємодіють між собою в процесі створення уявлень. Інформація має деякі істотні з погляду її захисту властивості. Ці властивості для користувача або власника інформації можна розглядати як деякі бажані стани інформації (носіїв інформації).

Такими властивостями є:

- конфіденційність – властивість інформації бути захищеною від несанкціонованого ознайомлення;
- цілісність – властивість інформації бути захищеною від несанкціонованого спотворення, руйнування або знищення;
- доступність – властивість інформації бути захищеною від несанкціонованого блокування.

Відповідно до цих властивостей, ТЗІ – це діяльність, спрямована на забезпечення організаційними та інженерно-

технічними заходами конфіденційності, цілісності й доступності інформації, яка визначена власником або уповноваженою ним особою як об'єкт захисту. Події, які потенційно можуть порушити одну з названих властивостей інформації відповідно називають загрозами порушення конфіденційності, цілісності та доступності інформації. Закон України «Про інформацію» класифікує всю інформацію за режимом доступу, тобто відповідно до передбаченого правовими нормами порядку її одержання, використання, поширення та зберігання (рис. 1.1).

До секретної (особливої важливості – ОВ, цілком таємної – ЦТ, таємної – Т) належить інформація, що містить відомості, які становлять державну або іншу передбачену законом таємницю, розголошення якої завдає шкоди суспільству (державі).

До конфіденційної інформації належать відомості, якими володіють, які використовують або якими розпоряджаються окремі фізичні або юридичні особи, котрі поширюють їх відповідно до визначених ними самостійно умов.

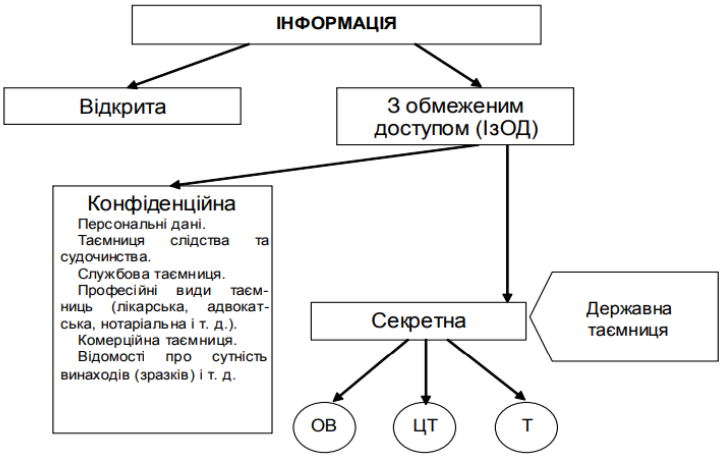

Рисунок 1.1 – Законодавча класифікація видів інформації в Україні

Секретна та конфіденційна інформація потребують захисту від загроз порушення конфіденційності, цілісності та доступності, а відкрита інформація важлива для особи, суспільства та держави – захисту від загроз порушення цілісності та доступності.

Спираючись на вищенаведене визначення інформації і суть технічного захисту інформації, можна сформулювати парадигму захисту інформації: **інформація вважається захищеною, якщо під час її переміщення дотримуються режимної адекватності комунікабельних носіїв інформації.** Розглянемо цю парадигму докладніше. Порушення інформаційної безпеки можливе лише у разі переміщення інформації.

Наприклад, під час несанкціонованого ознайомлення (читання) документа з паперового носія відбувається переміщення (копіювання) інформації в мозок людини, яка стає носієм-одержувачем цієї інформації. У формулюванні парадигми під поняттям переміщення інформації будемо розуміти зміну просторових координат носіїв з інформацією або знищення інформації зі збереженням або руйнуванням носія. У процесі переміщення інформації може відбуватися зміна її носія.

Наприклад, носіями інформації під час її переміщення можуть бути: матеріальні середовища (повітря, вода, метал та ін.); сенсори або датчики; перетворювачі та інші об’єкти живої й неживої природи, що виконують функцію проміжних носіїв інформації. Поняття «режимна адекватність» складається з термінів «режим» і «адекватність».

Режим – це сукупність норм для досягнення якої-небудь мети. Наприклад, для захисту інформації. Тут обов’язково враховують режим доступу до інформації як передбачений правовими нормами порядок отримання, використання, поширення та зберігання інформації.

Адекватність (від лат. adaequatus – прирівняний, рівний) це відповідність, правильність, точність. Термін «комунікабельність» (від пізньолатинського – communicabilis – той, що з’єднується) означає суміщуваність (здатність до спільної

роботи) різнотипних систем передачі інформації (наприклад, в електрозв'язку – аналогових і дискретних, у телебаченні – з різною кількістю рядків розкладання телевізійного кадру тощо).

Тому комунікабельні носії інформації – це носії інформації, здатні до взаємодії. Приклад некомунікабельності носіїв: через такий сенсор, як органи зору (очі) людина не здатна сприйняти голосову (акустичну) інформацію. Приклад комунікабельності носіїв: через сенсор – органи зору (очі) людина здатна сприйняти інформацію, зафіксовану на паперовому носії зрозумілою для нього мовою.

Смислове значення складових поняття «режимна адекватність носіїв інформації» є таким: це відповідність режимів доступу носіїв інформації (джерела та одержувача) під час їх взаємодії. Приклад режимної неадекватності: ознайомлення зі змістом секретного документа без права на доступ до секретної інформації. Приклад режимної адекватності: особиста розмова двох людей, охочих передати й відповідно одержати інформацію з обмеженим доступом, що є власністю одного з них. Проміжні носії інформації, так само, як і носій-джерело, і носій-одержувач, повинні відповідати вимогам режимної адекватності та комунікабельності.

Отже, іншими словами, режимна адекватність комунікабельних носіїв інформації – це здатність носіїв інформації брати участь в інформаційному обміні під час відповідності режимів доступу. Сформульована вище парадигма враховує основні інформаційні загрози таким чином. Загрози конфіденційності спрямовані на заборонене режимом доступу переміщення інформації від носія-джерела до носія-одержувача. Інформація зберігає конфіденційність, якщо додержується, насамперед, режимна адекватність носіїв інформації.

Загрози цілісності інформації направлені на заборонену режимом доступу (порядком отримання, використання, поширення та зберігання інформації) її зміну або спотворення, що призводить до порушення її якості або повного знищення. Цілісність інформації може бути порушена сумісно, а також

унаслідок об'єктивного впливу з боку середовища, що оточує носій інформації. Інформація зберігає цілісність, якщо дотримується встановлена режимна адекватність щодо правил її модифікації (видалення). Будь-якого суб'єкта, що впливає на носій-джерело інформації з метою модифікації інформації, можна розглядати як носія інформації, що несе в собі уявлення про необхідну модифікацію (видалення) інформації носія-джерела інформації.

У процесі модифікації також відбувається переміщення інформації, що модифікується. Вплив об'єктів, процесів зовнішнього середовища та інших чинників, які часто відносять до розряду «випадкових» – це невідповідність носія-джерела інформації встановленому режиму доступу, що часто призводить до порушення комунікабельності. Такий вплив є порушенням режимної адекватності, і як наслідок – комунікабельності носіїв інформації. Загрози доступності (відмова в обслуговуванні) спрямовані на навмисне або ненавмисне порушення комунікабельності носіїв інформації у процесі їх взаємодії. Порушення комунікабельності перериває дозволені режимом доступу процеси переміщення інформації. Інформація зберігає доступність, якщо зберігається комунікабельність носіїв інформації під час їх взаємодії.

Для правильного визначення об'єкта захисту необхідно знати основні поняття, пов'язані із секретною інформацією. Державна таємниця – вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки й техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані в порядку, встановленому Законом України «Про державну таємницю», державною таємницею і підлягають охороні державою. Матеріальні носії секретної інформації – матеріальні об'єкти, зокрема фізичні поля, в яких відомості, що становлять державну таємницю, відображені у вигляді текстів, знаків, символів, образів, сигналів, технічних рішень, процесів тощо.

Система захисту державної таємниці – сукупність органів захисту державної таємниці, використовуваних ними засобів і методів захисту відомостей, що становлять державну таємницю та їх носіїв, а також заходів, що проводяться з цією метою. Допуск до державної таємниці – процедура оформлення права громадян на доступ до відомостей, що становлять державну таємницю, а підприємств, установ і організацій – на проведення робіт із використанням таких відомостей. Доступ до відомостей, що становлять державну таємницю, – надання повноважною посадовою особою дозволу громадянину на ознайомлення з конкретною секретною інформацією та провадження діяльності, пов'язаної з державною таємницею, або ознайомлення з конкретною секретною інформацією та провадження діяльності, пов'язаної з державною таємницею, цією посадовою особою відповідно до її службових повноважень.

Гриф секретності – реквізит матеріального носія секретної інформації, що засвідчує ступінь секретності цієї інформації. Засекречування відомостей та їх носіїв – введення у передбаченому порядку для відомостей, що становлять державну таємницю, обмежень на їх поширення. Комерційна таємниця – відомості, що не є державними секретами, пов'язані з виробництвом, технологіями, фінансами, процесами управління та іншою діяльністю організацій або фірм, розголошування яких може завдати збитку їх інтересам.

Ступінь секретності – категорія, що характеризує важливість такої інформації, можливі збитки внаслідок її розголошування, ступінь обмеження доступу до неї та рівень її охорони державою. Критерій визначення ступеня секретності інформації встановлює відповідний державний орган. Переліки конфіденційної інформації, яка є власністю держави і якій надається гриф обмеження доступу «Для службового користування», розробляються і вводяться в дію міністерствами, іншими центральними органами виконавчої влади, обласними, міськими державними адміністраціями.

У разі потреби на державних підприємствах, в установах і організаціях з урахуванням особливостей їх діяльності розробляються і за узгодженням із міністерством, іншим центральним органом виконавчої влади, до сфери управління якого вони належать, вводяться в дію переліки конкретних видів документів у відповідній сфері діяльності.

Наприклад, тим самим наказом МВС України № 207 від 06.03.2003 р. затверджено відповідний Перелік конфіденційної інформації в системі МВС України, якій надається гриф обмеження доступу «Для службового користування». Отже, для державної інформації з обмеженим доступом вже визначені відомості, які в обов'язковому порядку є об'єктом захисту. На підставі Розгорнутого переліку відомостей, що становлять державну таємницю, і Переліку конфіденційної інформації, якій надається гриф обмеження доступу «Для службового користування», в організації необхідно скласти і затвердити Перелік відомостей організації, які містять інформацію з обмеженим доступом і потребують захисту.

1.2. Принципи безпеки

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 отримати. 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, неможливо забезпечити стабільний економічний розвиток як окремого підприємства, так і держави.

Розвиток ТЗІ в Україні обумовлюється таким основними чинниками:

- стрімким розвитком суспільних і міждержавних відносин;
- застосуванням технічних засобів оброблення інформації та засобів зв'язку іноземного виробництва;
- поширенням 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, що 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, що становить державну та іншу передбачену законом таємницю;
- конфіденційної інформації, що 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 та організаціях;

- виконання на власний розсуд суб'єктами інформаційних відносин вимог щодо технічного захисту;
- ієрархічність побудови організаційної структури системи ТЗІ і 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 та 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, які належать до системи Служби безпеки України і виконують завдання технічного захисту інформації;
- військові частини, підприємства, установи та організації всіх форм власності та 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 з захистом інформації, що є власністю держави, координуються й контролюються Держспецзв’язком (колишнім ДСТС ЗІ СБУ). Основні завдання всіх 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 й оброблення даних, і яка містять: технічні засоби, програмне забезпечення, відповідний персонал і допоміжні засоби (рис. 1.2). Систему захисту інформації (СЗІ) для конкретних об’єктів (інформаційних систем), відповідно до джерела [2], можна подати у вигляді:

– основ побудови системи захисту інформації;
– напрямів захисту інформації;
– етапів побудови СЗІ.

Рисунок 1.2 – Складові ІС

Основою побудови СЗІ є:

1. Законодавча, нормативно-правова, наукова і методична бази забезпечення захисту інформації.
2. Структура й завдання органів (підрозділів), що забезпечують безпеку інформаційних технологій.
3. Організаційно-технічні та режимні заходи і методи захисту інформації.

4. Програмно-технічні методи й засоби, використовувані для захисту інформації.

Напрями захисту інформації визначаються з урахуванням конкретних особливостей інформаційної системи як об'єкта захисту.

Як найбільш поширені, з урахуванням типової структури ІС і видів робіт із захисту інформації, що історично склалися, можна виділити такі напрями:

1) Захист об'єктів інформаційних систем.
2) Захист процесів, процедур і програм оброблення інформації.
3) Захист каналів зв'язку.
4) Блокування побічних електромагнітних випромінювань і наведень.
5) Керування системою захисту.

Етапи побудови СЗІ необхідно пройти однаково для всіх і кожного окремо напрямів (з урахуванням усіх основ). Виходячи з практичного досвіду, можна виділити такі етапи побудови СЗІ, зміст яких дещо відрізняється від запропонованих у джерелі [7]:

1) Визначення інформаційних ресурсів (ІР), що потребують захисту.
2) Виявлення повної множини загроз безпеці ІР, що потребують захисту.
3) Проведення оцінювання вразливості й ризиків для ІР, що потребують захисту, відповідно до виявленої множини загроз.
4) Розроблення проєкту (плану) системи захисту інформації, що знижує за вибраним критерієм ризики для ІР, які потребують захисту, відповідно до виявленої множини загроз.
5) Реалізація проєкту (плану) захисту інформації.
6) Визначення якості реалізованої системи захисту.
7) Здійснення контролю функціонування та керування системою захисту.

Взаємозв’язок усіх елементів системи захисту інформації відображено на рисунку 1.3.

Рисунок 1.3 – Взаємозв’язок елементів СЗІ

Проходження етапів необхідно здійснювати за можливості безперервно за замкненим циклом, із проведенням відповідного аналізу стану СЗІ та уточненням вимог до неї після кожного кроку (рис. 1.4).

Для опису логічних зв’язків і повнішого представлення процесу захисту інформації для кожної ІС пропонується формувати так звану матрицю знань інформаційної безпеки (ІБ). Матриця знань ІБ логічно об’єднує складові блоків «основи», «напрями» і «етапи» за принципом кожен із кожним.

Рисунок 1.4 – Цикл етапів (кроків) побудови СЗІ

Матриця формується з урахуванням конкретних завдань зі створення конкретної СЗІ для конкретної ІС. Наочно процес формування СЗІ з використанням матриці знань ІБ зображений на рисунку 1.5.

Рисунок 1.5 – Процес формування СЗІ з використанням матриці знань ІБ

Елементи матриці мають відповідну нумерацію (табл. 1). Позначення кожного з елементів матриці такі:

– перше знакомісце (x00) відповідає номерам складових блоку – етапи;
– друге знакомісце (0x0) відповідає номерам складових блоку – напрями;
– третє знакомісце (00x) відповідає номерам складових блоку – основи.

Таблиця 1.1 – Відповідна нумерація елементів матриці

<< Етапи	Напрями >>	x1x				x2x				x3x				x4x				x5x			
		Захист об'єктів ІС				Захист процесів і програм				Захист каналів зв'язку				ПЕМВН				Керування системою захисту			
	Основи >>	База	Структура	Заходи	Засоби	База	Структура	Заходи	Засоби	База	Структура	Заходи	Засоби	База	Структура	Заходи	Засоби	База	Структура	Заходи	Засоби
		x11	x12	x13	x14	x21	x22	x23	x24	x31	x32	x33	x34	x41	x42	x43	x44	x51	x52	x53	x54
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
1xx	Визначення ІР, які потрібно захистити	111	112	113	114	121	122	123	124	131	132	133	134	141	142	143	144	151	152	153	154
2xx	Виявлення поіноїмножини загрози безпеці ІР, які потребують захисту	211	212	213	214	221	222	223	224	231	232	233	234	241	242	243	244	251	252	253	254
3xx	Проведення оцінки вразливості та ризиків для ІР, які потребують захисту	311	312	313	314	321	322	323	324	331	332	333	334	341	342	343	344	351	352	353	354
4xx	Розроблення проєкту (плану) СЗІ, який зменшує за обранимкритерієм ризики для ІР, що потребують захисту	411	412	413	414	421	422	423	424	431	432	433	434	441	442	443	444	451	452	453	454
5xx	Реалізація проєкту (плану) захисту інформації	511	512	513	514	521	522	523	524	531	532	533	534	541	542	543	544	551	552	553	554
6xx	Визначення якості реалізації СЗІ	611	612	613	614	621	622	623	624	631	632	633	634	641	642	643	644	651	652	653	654
7xx	Здійснення контролю функціонування й керування системою захисту	711	712	713	714	721	722	723	724	731	732	733	734	741	742	743	744	751	752	753	754

У загальному випадку кількість елементів матриці може бути визначена із співвідношення

$$K = O_i \cdot H_j \cdot M_k \qquad (1.1.)$$

де К – кількість елементів матриці;
Оі – кількість складових блоку основи;
Нj – кількість складових блоку напряму;
Мk – кількість складових блоку.

У загальному випадку вся кількість елементів дорівнює 140. К = 4 × 5 × 7 = 140. Зміст кожного з елементів матриці описує взаємозв'язок складових створюваної СЗІ. Комплекс питань створення й оцінювання СЗІ розглядається шляхом аналізу різних груп елементів матриці й залежно від вирішуваних завдань.

Використовуючи міжнародний стандарт ISO/IEC 15408 «Загальні критерії оцінки безпеки інформаційних технологій», можна показати (рис. 1.6) динаміку побудови СЗІ і процеси, що відбуваються при цьому.

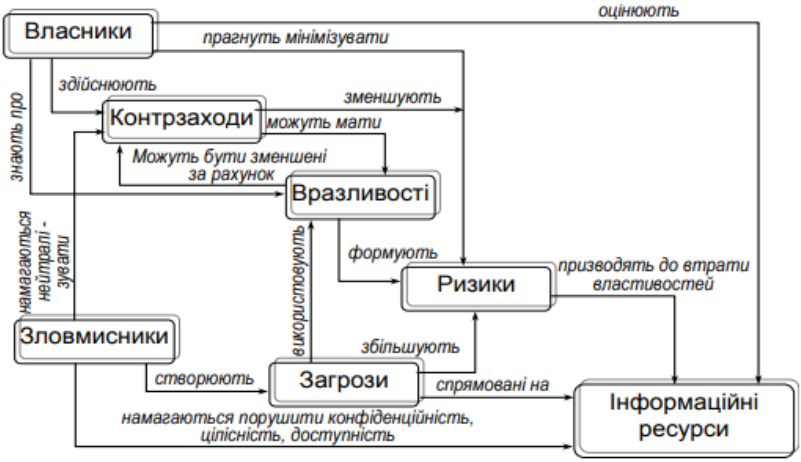

Рисунок 1.6 – Динаміка побудови СЗІ та супровідні процеси

РОЗДІЛ 2. МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ В ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

2.1. Методи проведення атак на інформацію (хакінг, крекінг, фрикінг)

Хакінг – внесення змін у програмне забезпечення для досягнення певних цілей, що відрізняються від цілей творців програм, дуже часто зміни є шкідливими.

Людину, яка займається хакінгом, називають хакером. Це зазвичай досвідчений програміст. Проте існують й інші хакери, які мають більш небезпечні мотиви, ніж просто демонстрація своєї майстерності. Вони спрямовують свої знання на крадіжку особистої інформації, несанкціонований доступ тощо.

Хакінг – є серйозною проблемою індустрії. Він отримав величезний розвиток після створення мережі Інтернет через легкість доступу до комп'ютерів у будь-якій точці світу. Крім того, легкий доступ практично до будь-якої інформації допомагає розширювати знання хакерів. Із такою інформацією не потрібно бути програмістом, щоб зламати приватну мережу.

Хакери стали настільки «просунутими», що навіть такі гіганти, як Microsoft, не застраховані від їх дій, і щорічно зазнають багатомільйонних збитків. До такого прикладу можна навести появи Хакінтоша. Але хакери зовсім не обмежуються лише великими компаніями. Над окремими користувачами також висить ця загроза. Крадіжка особистої інформації, фінансових даних – лише деякі з погроз.

Злом програмного забезпечення – дії, спрямовані на усунення захисту програмного забезпечення (ПЗ), вбудованої розробниками для обмеження функціональних можливостей. Останнє необхідно для стимуляції покупки такого програмного забезпечення, після якої обмеження знімаються.

Крек (також спотворене кряк і, вкрай рідко, крак) (англ. Crack) – програма, що дозволяє здійснити злом програмного забезпечення. Зазвичай крек придатний для масового

використання. По суті, крек є втіленням одного з видів злому, найчастіше – це звичайний патч. Для слова «крек» використовують такі евфемізми: «ліки», «таблетка», «аспірин» тощо.

Практично будь-який злом зводиться до використання одного з таких способів.

Введення серійного номера – злом програми за допомогою введення правильного реєстраційного ключа (або фрази), отриманого нелегальним способом. Ключ може генеруватися на основі будь-якої інформації (імені власника ПО, характеристик апаратної частини комп'ютера тощо), а мати фіксоване значення. Для генерації реєстраційного ключа використовують той самий алгоритм, що і в програмі.

Реєстраційний код може поширюватися в ключовому файлі, який зазвичай поміщають у каталог із встановленою програмою.

Для масового злому, найчастіше створюють (і в подальшому використовується) генератор ключів – програма для генерації реєстраційних ключів. Цей вид злому найбільш затребуваний. Ключ генерується на основі якоїсь інформації і тому найбільш цінується. Зазвичай вимагає більшої кваліфікації зломщика порівняно з іншими видами злому, але не завжди.

Використання завантажувача – спосіб обходити деякі види захисту ПЗ, які полягають у використанні зовнішніх (навісних) систем захисту. Полягає у зміні певних фрагментів програми в оперативній пам'яті відразу після її завантаження в цю пам'ять, але перед її запуском (тобто перед виконанням коду в точці входу).

Застосування (бінарного) патча) – спосіб, схожий на «завантажувач», але модифікація виробляється статично в файлах програми. Зазвичай це один із найпростіших і швидких способів злому ПЗ.

Використання зламаної версії файлу – спосіб полягає в підміні оригінальних файлів програми файлами, які вже зламані.

Використання емулятора ключа – спосіб використовують для обману захистів, побудованих на використанні як захисту електронного ключа (зазвичай під'єднуються до LPT або USB порту комп'ютера). Полягає в знятті дампа внутрішньої пам'яті ключа. Файл із вмістом цієї пам'яті подається на вхід спеціальною програмою – емулятора, яка під'єднує свій драйвер-фільтр у стек драйверів і обманює захищену програму, емулюючи роботу з апаратним ключем. У разі наявності в програмі звернень до ключа для апаратного шифрування ділянки пам'яті цей метод використовують у зв'язці з методом Бінарний патч.

Підміна офіційного сайту програм і/або відповідна зміна налаштувань із метою обійти перевірку ключа, якщо вона була винесена розробниками на будь-який інтернет-ресурс (в абсолютній більшості випадків – для запобігання злому, рідше – для обліку і ведення статистики, збирання відомостей). Найчастіше здійснюється на примітивному рівні шляхом модифікування файлу hosts і запуску різних емуляторів, іноді – використання різних програм (Денвер) або використання реально існуючого веб-ресурсу.

Заборона доступу програми до інтернету полягає в комплексі дій, спрямованих на здійснення примусової заборони доступу програми до інтернету. Виконується в тому разі, коли програма вимагає активації ліцензійного ключа через інтернет (зазвичай офіційний сайт розробника), або у разі, коли програма зв'язується з сервером розробника для обміну даними або поновлення. Зазвичай, установлюється спеціальна утиліта, яка блокує доступ програми в мережу Інтернет, більш примітивний спосіб – фізичне відключення від інтернету. Ця дія зазвичай проводиться після введення ключа, згенерованого кейгеном.

Скачування з інтернету або з іншого комп'ютера вже зламаної або купленої гри. Перекачування ліцензійної копії гри з одного комп'ютера зломом не є, але суть та сама.

Під часу злому складних захистів, а також за необхідності досягти максимального ефекту, застосовується комбінація

перерахованих вище способів. У рідкісних випадках це відбувається під час недостатньої кваліфікованості зломщика.

Цей список не є вичерпним, а лише позначає найчастіші способи злому.

Вид злому здебільшого обумовлений видом захисту. Для деяких захистів можна використовувати різні види злому, для інших – спосіб може бути єдиним.

Фрикінг – сленговий вираз, що означає злом телефонних автоматів, телефонних мереж і мереж мобільного зв'язку, з використанням прихованих від користувача або недокументованих функцій. Зазвичай фрикінг здійснюється для безкоштовних дзвінків, поповнення особистого мобільного рахунку.

Згодом внутрішньо-канальна службова міжстанційна сигналізація, яку часто зламували фрикери, була витіснена в загальні канали, відокремлені від потоку передачі голосу (CCS, Common Channel Signalling), зокрема у вигляді ОКС7 (SS–7, CCITT Signalling System № 7), і багато фрикінг-пристрої втратили можливості незаконного втручання в міжкомутаторну сигналізацію для вчинення актів шахрайства з оплатою голосових викликів.

Фрикінг почав свою історію на рубежі кінця 60-х – початку 70-х років XX ст. Його зародження пов'язують із неабиякими навичками американського незрячого підлітка Джо Енгрессі, який навчився дуже точно відтворювати звукові сигнали телефонної лінії за допомогою звичайного свисту. Комбінуючи це вміння з спритним маніпулюванням технічним персоналом, який обслуговує лінію, Джо почав експлуатувати телефонні мережі для безкоштовних дзвінків по всьому світу. На перших порах фрикінг поширився в співтоваристві сліпих підлітків, потім фрикінг почали використовувати молоді технічні фахівці, які для генерування тональних телефонних сигналів використовували кустарні електронних схем, що створюються в домашніх умовах. Деякі з цих саморобних пристроїв (на сленгу тих часів – «коробок») отримали низку стійких неформальних найменувань:

1) «Блакитна коробка» (англ. Blue box) – пристрій для генерування системних керувальних сигналів і дозволяє робити дзвінки безкоштовно.
2) «Чорна коробка» (англ. Black box) – пристрій для безкоштовного прийому телефонних дзвінків.
3) «Червона коробка» (англ. Red box) – пристрій для безкоштовних дзвінків із платних телефонних апаратів.

2.2. Класифікація методів і засобів захисту інформації

Завдання забезпечення інформаційної безпеки необхідно вирішувати системно. Це означає, що засоби захисту інформації повинні застосовуватися одночасно і під централізованим управлінням. Водночас компоненти системи повинні «знати» про існування один одного, взаємодіяти і забезпечувати захист від зовнішніх і від внутрішніх загроз.

Технології захисту даних ґрунтуються на застосуванні сучасних методів, які запобігають витоку інформації та її втраті. Сьогодні використовують шість основних способів захисту: перешкода, маскування, регламентація, управління, примус, спонукання. Усі перераховані методи націлені на побудову ефективної технології захисту інформації, під час якої виключено витрати через недбалість і успішно відображено різні види загроз. Під перешкодою розуміємо спосіб фізичного захисту інформаційних систем, завдяки якому зловмисники не мають можливості потрапити на територію, що охороняється.

Маскування – способи захисту інформації, що передбачає перетворення даних у форму, не придатну для сприйняття сторонніми особами. Для розшифрування потрібне знання принципу.

Управління – способи захисту інформації, за яких здійснюється управління над всіма компонентами інформаційної системи.

Регламентація – найважливіший метод захисту інформаційних систем, що припускає введення особливих інструкцій, згідно з якими повинні здійснюватися всі маніпуляції з даними, що охороняються.

Примус – методи захисту інформації, тісно пов'язані з регламентацією, що припускають введення комплексу заходів, за яких працівники змушені виконувати встановлені правила. Коли використовують способи впливу на працівників, за яких вони виконують інструкції з етичних і особистісних міркувань, то йдеться про спонукання. Способи захисту інформації передбачають використання певного набору засобів.

Для запобігання втрати та витоку таємних даних використовують такі засоби:

- фізичні;
- апаратні;
- програмні;
- апаратно-програмні;
- законодавчі;
- криптографічні та організаційні методи.

Фізичні засоби захисту – це засоби, необхідні для зовнішнього захисту засобів обчислювальної техніки, території та об'єктів. Вони реалізуються на базі ЕОМ, які спеціально призначені для створення фізичних перешкод на можливих шляхах проникнення і несанкціонованого доступу до компонентів інформаційних систем, що захищаються.

Апаратні засоби захисту – це різні електронні, електронно-механічні та інші пристрої, які вмонтовуються в серійні блоки електронних систем оброблення та передавання даних для внутрішнього захисту засобів обчислювальної техніки: терміналів, пристроїв введення та виведення даних, процесорів, ліній зв'язку тощо.

Програмні засоби захисту, які вмонтовані до складу програмного забезпечення системи, необхідні для виконання логічних та інтелектуальних функцій захисту.

Апаратно-програмні засоби захисту – це засоби, які засновані на синтезі програмних та апаратних засобів.

Законодавчі засоби – комплекс нормативно-правових актів, що регулюють діяльність людей, які мають доступ до відомостей, що охороняються, і визначають міру відповідальності за втрату або крадіжку секретної інформації.

Організаційні заходи захисту інформації складають сукупність заходів щодо підбору, перевірки та навчання персоналу, який бере участь у всіх стадіях інформаційного процесу [16].

РОЗДІЛ 3. НАЙПОШИРЕНІШІ ЗАГРОЗИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

3.1. Загрози інформаційної безпеки

Загроза інформаційної безпеки – сукупність умов і чинників, що створюють небезпеку порушення інформаційної безпеки.

Під загрозою (в загальному) розуміємо потенційно можливу подію, дію (вплив), процес або явище, які можуть призвести до заподіяння шкоди чиїм-небудь інтересам.

Під загрозою інтересів суб'єктів інформаційних відносин розуміють потенційно можливу подію, процес або явище, яке за допомогою впливу на інформацію або інші компоненти інформаційної системи, може прямо або опосередковано призвести до заподіяння шкоди даним того чи іншого суб'єкта. Зокрема, А. Антонов і В. Балашов визначають загрозу як процес настання таких змін у стані особи, суспільства й держави, що оцінюються ними як здатні створити перешкоди або унеможливити реалізацію їхніх інтересів.

Водночас слово «загроза» в словнику С. Ожегова означає можливу небезпеку, тому припускає не лише процес настання змін, а й можливість їх настання. Під загрозою також розуміють «можливість або неминучість виникнення чогось небезпечного, прикрого, тяжкого для кого-, чого-небудь», «те, що може заподіювати яке-небудь зло, якусь неприємність».

Під загрозою (в загальному сенсі) зазвичай розуміють потенційно можливу подію (дію, процес або явище), яка може призвести до нанесення збитку чиїмось інтересам. Надалі під загрозою безпеки автоматизованої системи (AS) оброблення інформації будемо розуміти можливість впливу на AS, який прямо або побічно може завдати шкоди її безпеці.

У той час відомо великий перелік загроз інформаційної безпеки AS, що містить сотні позицій.

Розгляд можливих загроз інформаційної безпеки проводять із метою визначення повного набору вимог до розроблюваної системи захисту.

Перелік загроз, оцінювання ймовірностей їх реалізації, а також модель порушника є основою для аналізу ризику реалізації загроз і формулювання вимог до системи захисту AS. Крім виявлення можливих загроз доцільне проведення аналізу цих загроз на основі їх класифікації за низкою ознак. Кожне з ознак класифікації відбиває одне з узагальнених вимог до системи захисту. Загрози, відповідні кожній ознаці класифікації, дозволяють деталізувати відображувану цією ознакою вимогу.

Необхідність класифікації загроз інформаційної безпеки AS обумовлена тим, що інформація, яка зберігається та обробляється в сучасних AS піддається впливу надзвичайно великої кількості чинників, через що стає неможливим формалізувати задачу опису повної множини загроз. Тому для системи, що захищається, зазвичай визначають не повний перелік загроз, а перелік класів загроз.

Класифікація можливих загроз інформаційної безпеки AS може бути проведена за таким базовими ознаками.

1. За природою виникнення:

- природні загрози, викликані впливами на AS об’єктивних фізичних процесів або стихійних природних явищ;
- штучні загрози безпеки AS, викликані діяльністю людини.

2. За ступенем навмисності прояву:

- загрози, викликані помилками чи халатністю персоналу, наприклад, некомпетентне використання засобів захисту, введення помилкових даних тощо;
- загрози навмисної дії, наприклад дії, зловмисників.

3. За безпосереднім джерелом загроз:

- природне середовище, наприклад, стихійні лиха, магнітні бурі тощо;
- людина, наприклад, вербування шляхом підкупу персоналу, розголошення конфіденційних даних тощо;

– санкціоновані програмно-апаратні засоби, наприклад, видалення даних, відмова в роботі OS;
– несанкціоновані програмно-апаратні засоби, наприклад, зараження комп'ютера вірусами з деструктивними функціями.

4. За розміщенням джерел загроз:

– поза контрольованої зони AS, наприклад, перехоплення даних, переданих за каналами зв'язку, перехоплення побічних електромагнітних, акустичних та інших випромінювань пристроїв;
– у межах контрольованої зони AS, наприклад, застосування підслуховувальних пристроїв, розкрадання роздруківок, записів, носіїв інформації тощо;
– безпосередньо в AS, наприклад, некоректне використання ресурсів AS.

5. За ступенем залежності від активності AS:

– незалежно від активності AS, наприклад, розтин шифрів криптозахисту інформації;
– лише в процесі оброблення даних, наприклад, загрози виконання і поширення програмних вірусів.

6. За ступенем впливу на AS:

– пасивні загрози, які під час реалізації нічого не змінюють у структурі та змісті АС, наприклад, загроза копіювання секретних даних;
– активні загрози, які під час дії вносять зміни в структуру і зміст AS, наприклад, упровадження троянських коней і вірусів.

7. За етапами доступу користувачів або програм до ресурсів:

– загрози, які проявляються на етапі доступу до ресурсів AS, наприклад, загрози несанкціонованого доступу в AS;
– загрози, які проявляються після дозволу доступу до ресурсів AS, наприклад, загрози несанкціонованого або некоректного використання ресурсів AS.

8. За способом доступу до ресурсів AS:

- загрози, що здійснюють із використанням стандартного шляху доступу до ресурсів АС, наприклад, незаконне отримання паролів та інших реквізитів розмежування доступу з подальшим маскуванням під зареєстрованого користувача;
- загрози, що здійснюються з використанням прихованого нестандартного шляху доступу до ресурсів AS, наприклад, несанкціонований доступ до ресурсів AS шляхом використання недокументованих можливостей OS.

9. За поточним місцем розміщення інформації, що зберігається та обробляється в AS:

- загрози доступу до інформації, що розміщена на зовнішніх запам'ятовувальних пристроях, наприклад, несанкціоноване копіювання секретної інформації з жорсткого диска;
- загрози доступу до інформації, що розміщена в оперативній пам'яті, наприклад, читання залишкової інформації з оперативної пам'яті, доступ до системної області оперативної пам'яті з боку прикладних програм;
- загрози доступу до інформації, що циркулює в лініях зв'язку, наприклад, незаконне підключення до ліній зв'язку з подальшим введенням помилкових повідомлень або модифікацією переданих повідомлень, незаконне підключення до ліній зв'язку з метою прямої підміни законного користувача з подальшим введенням дезінформації та нав'язуванням хибних повідомлень;
- загрози доступу до інформації, яка відображається на терміналі або надрукованої на принтері, наприклад, запис відображуваної інформації на приховану відеокамеру.

3.2. Атаки на інформаційні системи

Хакерська атака – спроба реалізації загрози, тобто – це дії кіберзловмисників (хакерів) або шкідливих програм, які спрямовані на захоплення інформаційних даних віддаленого комп'ютера, отримання повного контролю над ресурсами комп'ютера або на виведення системи з ладу.

Під атакою на інформаційну систему розуміють дії (процеси) або послідовність зв'язаних між собою дій порушника, які приводять до реалізації загроз інформаційних ресурсів, шляхом використання уразливостей цієї інформаційної системи.

Типи атак на інформаційні системи:

- Віддалене проникнення (remote penetration).
- Локальне проникнення (local penetration).
- Атака на відмову в обслуговуванні (denial of service).
- Мережні сканери (network scanners).
- Сканери вразливостей (vulnerability scanners).
- Зламувачі паролів (password crackers).
- Аналізатори протоколів (sniffers).
- Спам e-mail (Mailbombing).
- Перехоплення каналу зв'язку (Man-in-the-Middle).

Віддалене проникнення. Атаки, які дають змогу реалізувати віддалене керування комп'ютером через мережу. Приклади програм, що реалізують цей тип атак: NetBus, BackOrifice (див. рис. 3.1.).

1) NetBus або Netbus – програма дистанційного керування комп'ютерною системою Microsoft Windows по мережі. Вона була створена в березні 1998 року на Delphi Карлом-Фредріком Неіктером. Автор стверджував, що його програма створювалася, як «жарт», а не як програма, що дозволяє незаконно проникати в комп'ютерні системи. NetBus має клієнт-серверну архітектуру.
2) «Back Orifice» (традиційно скорочують BO) – комп'ютерна програма, яку було розроблено для віддаленого адміністрування системи. Дозволяє

користувачу керувати комп'ютером з ОС Microsoft Windows із віддаленого розміщення. Назва є грою слів ПЗ Microsoft BackOffice Server. Також дозволяє керувати кількома комп'ютерами одночасно, використовуючи образи.

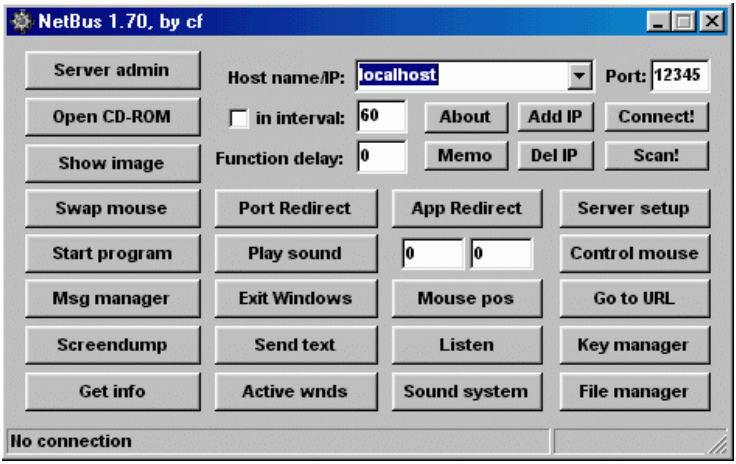

Рисунок 3.1 – NetBus (Віддалене проникнення)

Локальне проникнення (local penetration). Атака, що призводить до отримання несанкціонованого доступу до вузла ІКСМ, на якому вона запущена. Прикладом такої програми є GetAdmin.

GetAdmin

GetAdmin. exe є різновидом файлу EXE, пов'язаного з Guide to Hacking Software Security 2002 який розроблений Silver Star Publishing для ОС Windows. Остання відома версія GetAdmin. exe: 1.0.0.0, розроблена для Windows. Цей файл EXE має рейтинг популярності 1 зірок і рейтинг безпеки «Невідомо».

Що являють собою файли EXE?

Файли EXE («виконувані»), такі як GetAdmin. exe – це файли, що містять покрокові інструкції, якими комп'ютер користується, щоб виконати ту чи іншу функцію. Коли ви двічі

«клацаєте» по файлу EXE, ваш комп'ютер автоматично виконує ці інструкції, створені розробником програми (наприклад, Silver Star Publishing) з метою запуску програми (наприклад, Guide to Hacking Software Security 2002) на вашому комп'ютері.

Кожний програмний додаток на вашому комп'ютері використовує виконуваний файл: ваш веб-браузер, текстовий процесор, програма для створення таблиць тощо. Це робить виконувані файли одними з найбільш корисних видів файлів в операційній системі Windows. Без таких виконуваних файлів, як GetAdmin. exe, ви не змогли б використовувати жодну програму на вашому комп'ютері.

Чому спостерігаються помилки в файлах типу EXE?

Через свою корисність і настирливість файли EXE зазвичай використовують як спосіб зараження вірусами / шкідливим ПЗ. Найчастіше віруси маскуються під безпечні файли EXE (наприклад, GetAdmin. exe) і поширюються через поштовий СПАМ або шкідливі веб-сайти, а потім можуть заразити ваш комп'ютер, коли будуть запущені на виконання (наприклад, коли ви двічі клацаєте по файлу EXE).

На додаток, віруси можуть заразити, перемістити або пошкодити існуючі файли EXE, що згодом може призвести до повідомлень про помилки, коли виповнюється Guide to Hacking Software Security 2002 або пов'язані програми. Отже, будь-який виконуваний файл, який ви завантажуєте на свій комп'ютер, необхідно перевірити на віруси перед відкриттям, навіть якщо ви вважаєте, що він отриманий з надійного джерела.

Помилки EXE, наприклад, пов'язані з GetAdmin. exe, найчастіше з'являються під час запуску комп'ютера, запуску програми або під час спроби використання специфічних функцій у вашій програмі (наприклад, друк).

Поширені повідомлення про помилки в GetAdmin. exe:

- «Помилка програми GetAdmin. exe.»
- «GetAdmin. exe не є додатком Win32.»

- «Виникла помилка в додатку GetAdmin. exe. Додаток буде закрито. Приносимо вибачення за незручності.»
- «Файл GetAdmin. exe не найден.»
- «GetAdmin. exe не найден.»
- «Помилка запуску програми: GetAdmin. exe.»
- «Файл GetAdmin. exe не запущено.»
- «Відмова GetAdmin. exe.»
- «Неправильний шлях до програми: GetAdmin. exe.»

Такі повідомлення про помилки EXE можуть з'являтися в процесі установки програми, коли запущена програма, пов'язана з GetAdmin. exe (наприклад, Guide to Hacking Software Security 2002), під час запуску або завершення роботи Windows, або навіть під час установки операційної системи Windows. Відстеження моменту появи помилки GetAdmin. exe є важливою інформацією під час усунення проблеми (рис. 3.2.).

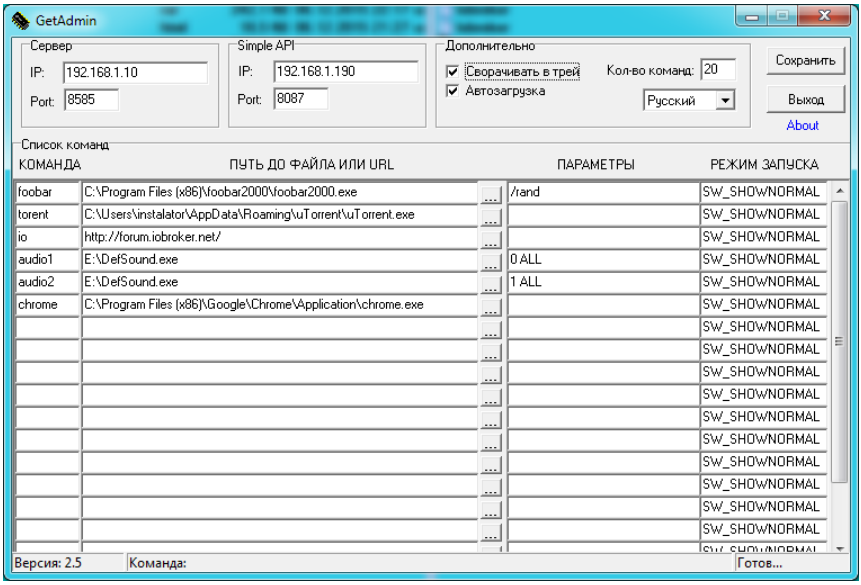

Рисунок 3.2 – GetAdmin (локальне проникнення)

Атака на відмову в обслуговуванні, розподілена атака на відмову в обслуговуванні (англ. DoS attack, DDoS attack, (Distributed) Denial-of-service attack) – напад на комп'ютерну систему з наміром зробити комп'ютерні ресурси недоступними користувачам, для яких комп'ютерна система була призначена.

Одним із найпоширеніших методів нападу є насичення атакованого комп'ютера або мережевого устаткування великою кількістю зовнішніх запитів (часто безглуздих або неправильно сформульованих), таким чином, атаковане устаткування не може відповісти користувачам, або відповідає настільки повільно, що стає фактично недоступним. Взагалі відмова сервісу здійснюється:

- примусом атакованого устаткування до зупинення роботи програмного забезпечення / устаткування або до витрат наявних ресурсів, унаслідок чого устаткування не може продовжувати роботу;
- заняттям комунікаційних каналів між користувачами і атакованим устаткуванням, внаслідок чого якість сполучення перестає відповідати вимогам (див. рис. 3.3).

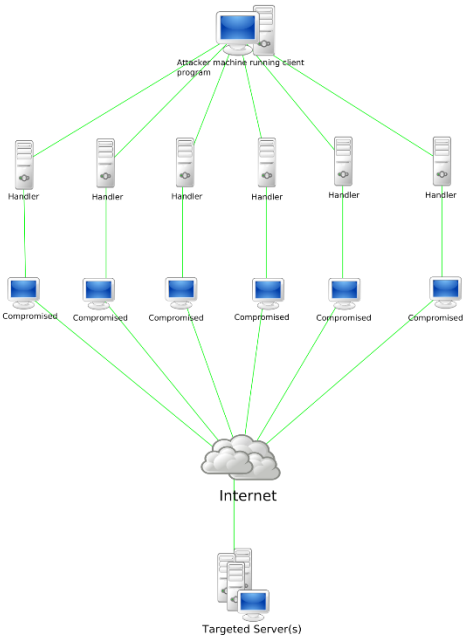

Рисунок 3.3 – DoS attack (Атака на відмову в обслуговуванні)

На сьогоднішній день існує досить багато різних видів атак на відмову, кожна з яких використовує певну особливість побудови мережі або вразливості програмного забезпечення. Наприклад, атаки можуть здійснюватися шляхом безпосереднього пересилання великої кількості пакетів (SYN, UDP, ICMP flood), використання проміжних вузлів (Smurf, Fraggle), передавання занадто довгих пакетів (Ping of Death), некоректних пакетів (Land) або великої кількості трудоємних запитів. Зауважимо, що впродовж останнього часу відбувається бурхливий розвиток цього напряму діяльності та поява нових видів і способів атак. З останніх тенденцій можна відзначити появу атак погіршення якості (Quality Reduction Attack) та низькочастотних атак (Low Rated Attack) і, безумовно, цей процес буде продовжуватися, потребуючи нових досліджень і

розроблення нових методів протидії. Основні існуючі класи атак досить добре вивчені. Однак, різні підходи до їх класифікації. У роботі атаки класифіковані згідно з протоколами, за якими вони здійснюються. Виділені такі атаки: SYN flood, TCP reset, ICMP flood, UDP flood, DNS request, CGI request, Mail bomb, ARP storm і атаки на алгоритмічну складність (див. рис. 3.4.).

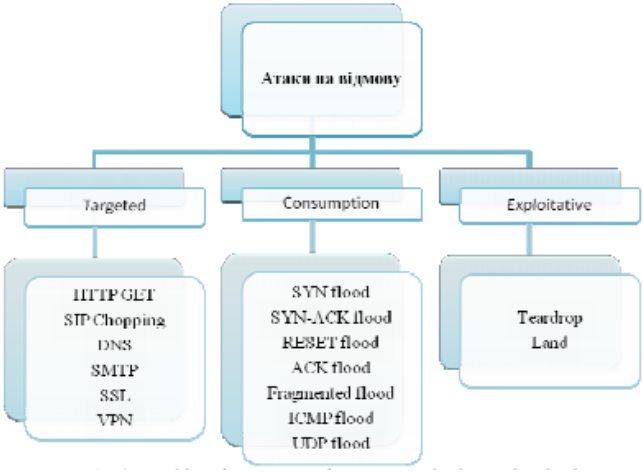

Рисунок 3.4 – Класифікація атак на відмову. Prolexic Technologies

3.3. Механізми захисту від атак

Багатошаровий захист – це стратегія безпеки, в якій кілька захисних шарів розміщені через усю інформаційну систему. Це допомагає уникнути прямих атак проти інформаційної системи і даних, оскільки злом одного шару призводить зловмисника лише до наступного рівня.

Управління інцидентами – це набір певних процесів для ідентифікації, аналізу, присвоювання пріоритетів і рішення інцидентів безпеки для відновлення нормальних сервісних

операцій так швидко, як це можливо і уникнення майбутнього повторення інциденту.

Політика безпеки – це документ або набір документів, який описує управління безпекою, яке буде реалізовано в організації.

Процес дослідження вразливостей і помилок проєктування, який відкриває операційну систему та її застосування для атаки або зловживання.

Тестування на проникнення – це метод оцінювання інформаційної безпеки системи або мережі симуляцією атаки для пошуку вразливостей, які може використовувати зловмисник. Тестування містить активний аналіз конфігурації системи, пошук недоліків проєктування, архітектури мережі, технічних недоліків і вразливостей.

РОЗДІЛ 4. СОЦІАЛЬНА ІНЖЕНЕРІЯ

4.1. Поняття соціальної інженерії

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 і 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 середовищі шпигунів соціальний інжиніринг завжди був головною зброєю. Видаючи себе за іншу особу, агенти спеціальних служб могли вивідати секретні державні таємниці. «Заговорювати людям зуби» по телефону, щоб отримати необхідну інформацію або просто змусити їх щось зробити, прирівнювалося до мистецтва. Професіонали в цій області за правильними запитаннями, за інтонацією голосу, могли визначити комплекси та страхи людини і, миттєво зорієнтувавшись, використовувати їх. Також це комплексний підхід до навчання і можливих змін соціальної реальності, що засновано на застосуванні інженерного підходу і наукових технологій. Соціальну інженерію застосовують для:

- збирання відомостей про мету підприємства;
- одержання конфіденційної інформації;
- прямого доступу до системи.

У сфері інформаційної безпеки для описання науки і психічної маніпуляції використовують термін «соціальна інженерія». За статистикою аналітичного центру компанії Infowatch, 55 % збитків, пов'язані з порушеннями інформаційної безпеки, виникають із вини 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 одержати конфіденційну інформацію хакерам досить важко, вони впливають безпосередньо на користувача – найслабше місце в системі інформаційної безпеки.

У світовій практиці ідея соціальної інженерії впроваджується шляхами впровадження новітніх освітніх технологій, а також із використанням активних методів навчання, за допомогою наповнення навчального процесу дисциплінами соціоінженерного та організаційного циклу, зокрема:

- теорія та методи соціальної інженерії;
- діагностика організацій;
- прогнозування й моделювання розвитку організацій;
- організаційне проєктування та програмування;
- соціальне планування;
- упровадження соціальних нововведень в організації;
- практикум із соціальних технологій;
- методи вирішення конфліктів.

У загальному випадку інциденти соціальної інженерії, можна пов'язати з роботою персоналу, де спостерігається низький рівень знань обов'язків користувачів. Тому, якщо навчати своїх працівників основним правилам поведінки в сфері інформаційної безпеки, підприємства можуть достатньо знизити ризики таких порушень інформаційної безпеки. Тому існують стандарти для

навчання, навчання персоналу – як приклад, одна з основних вимог міжнародного стандарту управління інформаційною безпекою ISO / IEC 27001 Особливості атак із використанням людського чинника:

- не вимагають значних витрат;
- не вимагають спеціальних знань;
- можуть тривати впродовж тривалого терміну;
- важко відслідковуються.

Людина часто набагато вразливіша, ніж система. Головна мета соціальної інженерії – це спрямована робота на отримання інформації за рахунок людини, особливо це застосовується у разі, коли неможливо отримати доступ до системи (наприклад, комп'ютер із важливими даними відключений від мережі). Соціальна інженерія складається з декількох технік, що застосовуються для досягнення поставлених задач. Усі вони опираються на помилки, які допускає людина в поведінці.

4.2. Види соціального інжинірингу в інформаційних системах

Основні техніки соціальної інженерії містять:

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 сайту (наприклад, поштового клієнта) з формою, в якій необхідно ввести свій логін, пароль та іншу особисту інформацію. Одним із прикладів фішингу є збирання 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 за телефоном. Такий метод зазвичай не вимагає від зловмисника попередньої підготовки і щодо пошуку даних про жертви. Основна ідея претекстингу полягає в тому, що зловмисник видає 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. Наприклад, зловмисник може подзвонити в будь-яку компанію та представитись співробітником IT-компанії і запропонувати встановити «необхідне» програмне забезпечення. Як тільки зловмисник отримає згоду на виконання такої роботи, порушник може одержати доступ як до системи, так і до всіх 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.

Зазвичай соціальна інженерія може завдати великої шкоди будь-якій компанії чи організації. Саме тому необхідно застосовувати всі можливі заходи з метою запобіганню атак на людський чинник. Особливість проведення соціального інжинірингу в тому, що спочатку необхідно сформувати мету впливу на відповідний об'єкт. Під «об'єктом» розуміємо жертву, на яку націлена така атака зловмисника. Наступним кроком збирається інформація про відповідний об'єкт, мета якого є виявлення найбільш зручних мішеней впливу або жертви. Далі настає етап, який у психології називають атракцією. Тобто створення необхідних умов для проведення впливу зловмисника на об'єкт. Примушення жертви до необхідної для соціального інженера дії зазвичай досягається виконанням початкових етапів. Тобто, як тільки досягнена атракція, потенційна жертва сама виконує необхідні для зловмисника дії. Всі атаки соціальних інженерів можна подати у вигляді простої схеми (рис. 4.1).

Соціальна інженерія спрямована на користувача, а не на його комп'ютерну техніку. Тут інтерес виникає до всіх платоспроможних осіб. Це також стосується користувачів, що володіють або мають доступ до цінної інформації (наприклад, співробітники підприємств і державних установ). Такий метод використовують із метою виконання фінансових операцій, зламу, крадіжки конфіденційних даних, наприклад, клієнтських баз, персональних даних або несанкціонованого доступу до

інформації. Соціальну інженерію використовують конкурентні компанії, щоб здійснювати розвідку, виявляти слабкі сторони компанії, переманювати цінних співробітників.

Рисунок 4.1 – Основна схема впливу в соціальній інженерії

4.3. Техніки соціальної інженерії

Усі техніки соціальної інженерії засновані на особливостях прийняття рішень людьми, що називаються когнітивним базисом. Вони також можуть бути названі особливістю прийняття рішення людської та соціальної психології, заснованої на тому, що людина повинна кому-небудь довіряти в соціальному середовищі виховання.

Природно, що під час проведення атаки з використанням соціального інжинірингу так само, як і в звичайних атаках,

присутня класифікація ступеня доступу для успішного проведення атаки. Цей ступінь залежить від рівня підготовленості соціального інженера і того, ким є жертва. Всього рівнів чотири, нижче вони перелічені в порядку убування повноважень:

1) адміністратор;
2) начальник;
3) користувач;
4) знайомий.

У таблиці 4.1 показано ймовірність отримання доступу різних рівнів і засоби застосування (1 – низька; 2 – середня; 3 – висока). Тепер розглянемо найпоширеніші техніки і види атак, якими користуються соціальні інженери. Всі вони засновані на особливостях прийняття людьми рішень, відомих як когнітивні упередження.

Ці забобони використовують у різних комбінаціях, із метою створення найбільш відповідної стратегії обману в кожному конкретному разі. Але спільною рисою всіх цих методів є введення в оману, метою яких є змусити людину вчинити будь-яку дію, необхідну соціальному інженеру. Для досягнення поставленого результату використовують цілу низку різноманітних тактик:

– видача себе за іншу особу;
– відволікання уваги;
– нагнітання психологічної напруги тощо.

Кінцеві цілі обману так само можуть бути дуже різними.

Таблиця 4.1 – Імовірність отримання доступу різних рівнів

Клас атак / підготовленість зловмисника	**Новачок**	**Звичайний користувач**	**Професіонал**
Засоби застосування			
Телефон	3	3	3
Електронна пошта	2	3	3
Спілкування в мережі Інтернет	3	3	3
Особиста зустріч	1	2	3
Рівень відношень			
Офіційний	2	3	3
Товариський	3	3	3
Дружній	1	2	3
Ступінь доступу			
Адміністратор	1	2	3
Начальник	1	2	3
Користувач	3	3	3
Знайомий	2	3	3

Техніки соціального інжинірингу:

1. Претекстинг – це набір дій, який здійснюється за певним сценарієм (претексту). Ця техніка передбачає використання голосових засобів, таких як телефон, «Skype» тощо для одержання потрібної інформації. Зазвичай називаючись третьою особою або вдаючи, що хтось потребує допомоги, соціальний інженер просить жертву повідомити йому пароль або авторизуватися на фішинговій веб-сторінці, тим самим змушуючи зробити необхідну дію або надати певну інформацію. Здебільшого ця техніка вимагає яких-небудь початкових даних про об’єкт атаки. Найпоширеніша стратегія за цієї техніки – використання на початку невеликих запитів і згадування імен

реальних людей з організації, в подальшому соціальний інженер пояснює, що потребують допомоги (більшість людей можуть виконати завдання, які не сприймаються ними як підозрілі). Як тільки довірчий зв'язок встановлено, соціальний інженер може попросити щось більш істотне й важливе.

2. Фішинг – це вид інтернет-шахрайства, метою якого є одержання доступу до конфіденційних даних користувачів. Досягається шляхом проведення масових розсилок електронних листів від імені популярних брендів, а також особистих повідомлень усередині різних сервісів (наприклад: від імені банків (Сітібанк, Альфа-банк), сервісів (Rambler, Mail. ru) або всередині соціальних мереж (Facebook, Вконтакте, Однокласники.ru).

У листі міститься пряме посилання на сайт, який зовні не відрізняється від справжнього, або на сайт, що містить редирект (автоматичне перенаправлення користувачів з одного сайту на інший). Після потрапляння на підроблену сторінку відбуваються різні спроби застосувати психологічні прийоми спонукати користувача ввести свої логін і пароль, які він використовує для доступу до певного сайту, що дозволяє шахраям одержати доступ до акаунтів, банківських рахунків тощо. Техніка фішингу перший раз була докладно описана в 1987 році, а сам термін з'явився 2 січня 1996 року в новій групі «alt. online-service. America-Online» мережі «Usenet».

Мабуть це найпопулярніша схема соціального інжинірингу на сьогоднішній день. Жодний великий витік персональних даних не обходиться без хвилі фішингових розсилок. Найчастіше метою фішерів є клієнти банків і електронних платіжних систем. Соціальні мережі також мають великий інтерес для фішерів, дозволяючи збирати особисті дані користувачів. На сьогодні безліч посилань на фішингові сайти націлені на крадіжку реєстраційних даних. За оцінками фахівців понад 70 % фішингових атак у соціальних мережах успішні. Фішинг стрімко набирає свої оберти, а оцінки збитку сильно різняться: за даними компанії «Gartner», «у 2008 році жертви

фішерів втратили 2,4 мільярда доларів США, у 2009 році – збиток становив 2,8 мільярда доларів, у 2010 – 3, 2 мільярди.

3. Вішинг – це техніка заснована на використанні системи попередньо записаних голосових повідомлень, метою яких є відтворення «офіційних дзвінків» від банківських та інших IVR (англ. Interactive Voice Response) систем. Зазвичай жертва одержує запит (найчастіше через фішинг електронної пошти) про необхідність зв'язку з банком для підтвердження або поновлення будь-якої інформації. Система вимагає аутентифікації користувача за допомогою введення PIN-коду або пароля. Основна відмінність вішингу в тому, що, так чи інакше, використовується телефон. Принцип дії IVR систем показаний на рисунку 4.2.

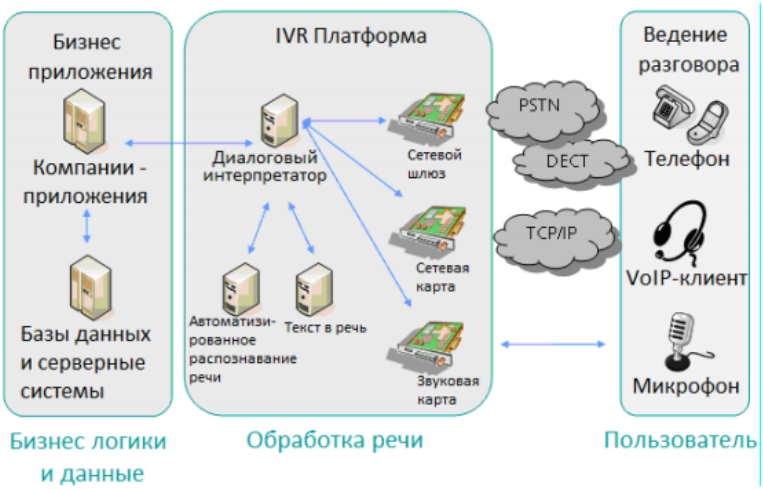

Рисунок 4.2 – Принцип дії IVR-систем

Згідно з інформацією від «Secure Computing», шахраї конфігурують автонабирач, який набирає номери в певному регіоні й під час відповіді на дзвінок відбувається таке:

– автовідповідач попереджає споживача, що з банківською картою виробляються шахрайські дії, і дає інструкції – передзвонити за певним номером негайно;
– за подальшого передзвонювання, на іншому кінці дроту відповідає комп'ютерний голос, який повідомляє, що людина повинна пройти звірку даних і ввести 16-значний номер картки з клавіатури телефону;
– після введення номера Вішер стає володарем усієї необхідної інформації (номер телефону, повне ім'я, адреса);
– потім, використовуючи цей дзвінок, можна зібрати і додаткову інформацію, таку, як PIN-код, термін дії карти, дата народження, номер банківського рахунку тощо.

4. Фармінг (англ. Pharming) – перенаправлення жертви за помилковою інтеренет-адресою. Для цього використовують будь-яку навігаційну структуру (файл «hosts», система доменних імен – «domain name system»). Суть роботи фармінгу має багато спільного зі стандартним вірусним зараженням. Жертва відкриває лист або відвідує будь-який веб-сервер, на якому виконується скрипт-вірус, водночас відбувається спотворення файлу «hosts», в результаті жертва потрапляє на один із помилкових сайтів. Механізмів захисту від фармінгу на сьогодні просто не існує.

5. Послуга за послугу – цей вид атаки має на увазі дзвінок соціального інженера в організацію з корпоративного (внутрішнього) телефону. Здебільшого соціальний інженер відрекомендовується співробітником технічної підтримки, який виробляє опитування на виникнення технічних проблем. Під час процесу «рішення» технічних проблем соціальний інженер «змушує» вводити команди, які дозволяють йому запустити або встановити шкідливе ПЗ на комп'ютер користувача.

6. Троянський кінь (або троянська програма) – це шкідлива програма, яку використовує соціальний інженер для збирання і використання інформаційних ресурсів у своїх цілях [8]. Ця техніка використовує цікавість або інші емоції людини.

Розробники троянських програм використовують ті самі прийоми, що і маркетологи. Для досягнення своєї мети «вірусописателі» використовують людські слабкості:

- недостатня підготовка;
- бажання виділитися;
- жалість і милосердя;
- бажання перегляду «цікавого» контенту;
- інтерес до продукту, який потрібен населенню або який дуже складно дістати; інтерес до методик швидкого збагачення за допомогою фінансових пірамід, супер-ідей для успішного ведення бізнесу або безпрограшної гри в казино.

Відкриваючи прикріплений до листа файл, співробітник встановлює на комп'ютер шкідливе ПЗ, яке дозволяє соціальному інженеру одержати доступ до конфіденційної інформації. Поширення троянських програм відбувається шляхом розміщення їх на відкритих ресурсах (файл-сервери, відкриті для запису накопичувачі самого комп'ютера), носіях інформації або надсилаються за допомогою служб обміну повідомленнями (наприклад: електронна пошта, ICQ) з розрахунку на їх запуск на якомусь конкретному або випадковому комп'ютері.

Рідко використання «троянів» є лише частиною спланованої багатоступінчастої атаки на певні комп'ютери, мережі або ресурси. Троянські програми найчастіше розробляють для шкідливих цілей. Існує класифікація, де вони розбиваються на категорії, засновані на тому, як «трояни» впроваджуються в систему і завдають їй шкоди. Існує 5 основних типів:

- віддалений доступ;
- знищення даних;
- завантажувач;
- сервер;
- дезактиватори програм безпеки.

Метою троянської програми може бути:

- закачування або скачування файлів;

– копіювання помилкових посилань, що ведуть на підроблені веб-сайти, чати або інші сайти з реєстрацією;
– створення перешкод роботі користувача;
– викрадення даних, що мають цінність або таємницю, зокрема інформації для аутентифікації, для несанкціонованого доступу до ресурсів;
– поширення інших шкідливих програм, таких як віруси;
– знищення даних (стирання або переписування даних на диску, важко помічаються пошкодження файлів) і обладнання, виведення з ладу або відмови обслуговування комп'ютерних систем, мереж;
– збирання адрес електронної пошти і використання їх для розсилання спаму;
– шпигунство за користувачем і таємне повідомлення третім особам будь-яких відомостей;
– реєстрація натискань клавіш із метою крадіжки інформації такого роду як паролі та номери кредитних карток;
– дезактивація або створення перешкод роботі антивірусних програм і брандмауера.

7. Збирання інформації з відкритих джерел. Застосування технік соціального інжинірингу вимагає не лише знання психології, а й уміння збирати про людину необхідну інформацію. Відносно новим способом одержання такої інформації стало її збирання з відкритих джерел, в основному з соціальних мереж.

8. «Дорожнє яблуко» – являє собою адаптацію троянського коня, і полягає у використанні фізичних носіїв. Соціальний інженер підкидає «інфікований» диск, або флеш-карту в місце, де носій може бути легко знайдений (туалет, ліфт, парковка). Носій підробляється під офіційний, і супроводжується підписом, що викликає цікавість (наприклад, соціальний інженер може підкинути диск, забезпечений корпоративним логотипом і посиланням на офіційний сайт організації, забезпечивши його написом «Заробітна плата керівного складу». Диск залишається на підлозі ліфта або у вестибюлі. Співробітник через незнання

підбирає диск і вставляє його в комп'ютер, щоб задовольнити цікавість).

9. Зворотний соціальний інжиніринг. Про нього згадують у тому разі, коли жертва сама пропонує зловмиснику потрібну йому інформацію (наприклад, співробітники служби підтримки для вирішення проблеми ніколи не питають у співробітників ідентифікатор або пароль. Проте багато користувачів для якнайшвидшого усунення проблем добровільно повідомляють ці конфіденційні відомості).

Зворотний соціальний інжиніринг будується на трьох чинниках:

- створення ситуації, яка змушує людину звернутися за допомогою;
- реклама своїх послуг або випередження надання допомоги іншими людьми;
- надання допомоги і вплив.

10. Human denial service (HDoS. Людська відмова в обслуговуванні) – суть атаки полягає в тому, щоб змусити людину (непомітно для нього) не реагувати на будь-які ситуації. Тобто робиться так, щоб кожне слово соціального інженера сприймається як правда беззастережно і без осмислення. До такого роду атак належать і відволікання уваги. Соціальний інженер здійснює хибне уявлення про виконання однієї операції, а насправді виконує зовсім іншу. Отже, поки жертва зайнята одним, іншого вона не помічає. Атаки такого роду виконуються досить складно, тому що необхідно добре прорахувати психологію жертви, її знання і реакції на такі дії [11].

11. Технічний соціальний інжиніринг. До цього виду атак можна адресувати ті атаки, в яких немає ні «жертви», ні «впливу на неї». В атаках цього типу використовують принципи і стереотипи соціуму, що і відносить їх до соціального інжинірингу. Наприклад, можна навести такі міркування: «Раз стоять камери, то, швидше за все, ніхто не полізе» або «Чим більша організація, тим твердіша у людей думка про її захищеності». Такий спосіб більш широко відомий як аналіз

ситуації. Людина бачить, що пройти звичайним шляхом (стандартним) не вийде, і починає переглядати інші варіанти, тобто займається аналізуванням ситуації.

12. Особистий візуальний контакт – є найскладнішою технікою. Здійснити цю техніку можуть лише професійні психологи або спеціально підготовлені люди. Техніка здійснюється так: до жертви знаходять підхід, знаходиться слабке місце, обчислюється це за допомогою аналізу відповідей на питання. Головне для соціального інженера в такому разі – розмовляти з жертвою «в межах слабкого місця», що згодом призведе до того, що він дуже сподобається жертві як людина, і та викладе все, що необхідно, вважаючи, що нічого особливо важливого не розповідає.

13. Системи обміну миттєвими повідомленнями (ММ) (рис. 4.3.). Нині в інтернеті існує безліч програм, які можуть тим чи іншим способом впливати на роботу ICQ, Viber. У список їх можливостей входить відсилання повідомлення від імені іншого користувача. Також зловмисник може проводити атаку в вигляді спеціально сформованого тексту, але основним шляхом поширення вірусів через ICQ є передача файлів, тому необхідно бути дуже обережним із пропозиціями завантажити файл від сторонньої людини, тому що операційна система не завжди здатна правильно видати інформацію про запущений файл. Microsoft Windows за замовчуванням не показує розширення імен (наприклад, ім’я файлу «foto. jpg. exe» буде показано як «foto. jpg»). Для маскування реального розширення застосовується подвійне розширення на зразок «xxx. jpg. exe» (у цьому разі може допомогти те, що деякі поштові сервери відмовляються пропускати виконувані файли) або додається велика кількість прогалин, через що ім’я файлу відображається не повністю.

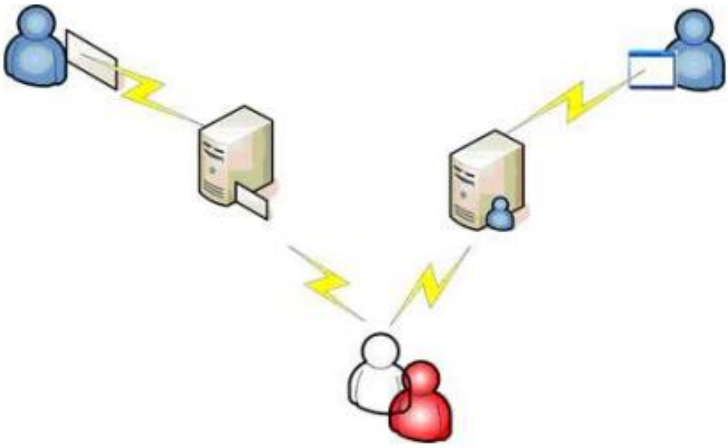

Рисунок 4.3 – Імітація під час використання ММ

Соціальний інженер (на рисунку виділено червоним кольором) виконує роль відомого користувача і посилає електронну пошту або ІМ-повідомлення, розраховуючи на те, що одержувачі візьмуть їх за повідомлення від того, кого вони знають.

14. Аналіз сміття – це цінна діяльність для соціальних інженерів. Ділові паперові відходи неоціненні, тому що під час атаки це може допомогти впливати на співробітників організації.

15. Особистісні підходи. Найпростіший шлях одержання інформації – це попросити про це безпосередньо.

Існує чотири різновиди такого підходу:

- залякування (цей підхід може використовувати уособлення повноважень, щоб примусити жертву виконати запит);
- переконання (звичайнісінькі форми переконання враховуючи лестощі);
- використання довірчих відносин (цей підхід вимагає більш тривалого терміну, впродовж якого підлеглий або

колега формують відносини, щоб одержати довіру та інформацію від жертви);

– допомога (в цьому підході пропонують допомогу жертві. Для цього потрібно, щоб жертва оприлюднила особисту інформацію).

4.4. Теоретичні аспекти методики протидії соціальній інженерії

Ніякі технічні заходи захисту інформації практично не допоможуть захиститися від соціального інжинірингу. Пов'язано це з тим, що соціальні інженери використовують слабкості нетехнічних засобів, а як говорилося, людський чинник. У зв'язку з цим, єдиний спосіб протидіяти соціальним інженерам – це постійна і правильна робота з персоналом.

Для підвищення безпеки в організації весь час повинні проводитися спеціальні навчання, постійно контролюватися рівень знань у співробітників, повинно проводитися тестування, а так само відбуватися внутрішні диверсії, які дозволять виявити рівень підготовленості співробітників у реальних умовах. Найважливіший момент у підготовці користувачів, на який необхідно звернути увагу – це те, що навчання – це циклічний процес, який повинен повторюватися з періодичністю в часі.

Форма навчання може складатися з таких видів, як:

1) теоретичні заняття;
2) практикум;
3) онлайн-семінари;
4) рольові ігри (тобто створення моделі атаки).

Для того щоб створити методику навчання персоналу, яка буде працювати, необхідно зрозуміти, чому люди вразливі для атак. Для виявлення цих тенденцій необхідно звернути на них увагу завдяки дискусії – цим можна допомогти співробітникам зрозуміти, як соціальний інженер може маніпулювати людьми.

Маніпуляція як метод впливу почала вивчатися соціальними дослідниками в останні 50 років. Роберт Чалдіні (відомий американський експериментальний соціальний психолог, відомий за книгою «Психологія впливу») написав статтю в «Американській науці» (лютий 2001 року) і об'єднав там результати досліджень, і виділив 6 типів «рис людської натури», які використовують у спробі одержання потрібної відповіді. Це 6 прийомів, які застосовують соціальні інженери найбільш часто і успішно в спробах маніпулювання:

1. Авторитетність – людям властиво бажання прислужитися людині з авторитетом (приклад атаки: соціальний інженер намагається видати себе за авторитету особу з IT-відділу або посадову особу, яка виконує завдання організації).

2. Уміння прихилити до себе – люди мають звичку привернути до себе або людину зі схожими інтересами, думкою, поглядами, або бідами і проблемами (наприклад, у розмові атакуючий намагається з'ясувати захоплення та інтереси жертви, а потім з ентузіазмом повідомляє, що все це йому знайоме. Також він може повідомити, що він із тієї ж школи або місця. Соціальний інженер може навіть наслідувати цілі, щоб створити подібність, видиму спільність).

3. Взаємність – людина здатна машинально відповісти на питання, коли отримує що-небудь натомість. Це один із найбільш ефективних шляхів вплинути на людину, щоб одержати прихильність (наприклад, співробітник отримує дзвінок від людини, який називає себе працівником IT-відділу. Той, хто телефонує розповідає, що деякі комп'ютери компанії заражені новим вірусом, який не виявляється антивірусом. Цей вірус може знищити (пошкодити) всі файли на комп'ютері. Той, хто телефонує пропонує поділитися інформацією, як вирішити проблему. Потім він просить співробітника протестувати недавно оновлену утиліту, що дозволяє користувачеві змінити паролі. Службовцю незручно відмовити, тому що той, хто телефонує, лише пропонує допомогу, яка захистить користувачів від вірусу).

4. Відповідальність – люди мають звичку виконувати обіцяне (наприклад, атакуючий зв'язується з відповідним новим співробітником і радить ознайомитися з угодою про політиків безпеки, тому що це – основний закон, завдяки якому можна користуватися інформаційними системами компанії. Після обговорення кількох положень про безпеки атакуючий просить пароль співробітника «для підтвердження згоди» з угодою. Він повинен бути складним для вгадування. Коли користувач видає свій пароль, той, хто телефонує дає рекомендації, як вибирати паролі в наступний раз, щоб хакерам було складно підібрати їх. Жертва погоджується прислухатись до порад, тому що це відповідає політиці компанії. До того ж робочий передбачає, що той, хто дзвонив, щойно підтвердив його згоду дотримуватися угоди).

5. Соціальна належність до авторизованих користувачів – людям властиво не виділятися у своїй соціальній групі. Дії інших є гарантом істинності в питанні поведінки (наприклад, той, хто телефонує, говорить, що він перевіряє і називає імена інших людей із відділу, які займаються перевіркою разом із ним. Жертва вірить, тому що інші названі імена належать справжнім співробітникам названого відділу. Потім атакуючий може задавати будь-які питання, аж до того, які логін і пароль використовує жертва).

6. Обмежена кількість «безкоштовного сиру» – віра в те, що об'єкт ділиться частиною інформації, на яку претендують інші, або, що ця інформація доступна лише в цей момент (наприклад, атакуючий розсилає електронні листи, що повідомляють, що перші 500 зареєстрованих на новому сайті компанії виграють 3 квитки на прем'єру відмінного фільму. Коли нічого не підозрюючи співробітник реєструється на сайті, його просять ввести свою адресу електронної поштової скриньки на робочому місці і вибрати пароль. Багато людей, щоб не забути безліч паролів, часто використовують один і той самий у всіх системах. Скориставшись цим, атакуючий може спробувати одержати

доступ до цільового робочого або домашнього комп'ютера зареєстрованого).

Організація відповідальна за те, щоб попередити співробітників наскільки серйозною може бути видача «непублічної» інформації. Добре продумана інформаційна політика безпеки разом із належним навчанням і тренуваннями поліпшать розуміння співробітників про належну роботу з корпоративною інформацією. Навчання безпеки в межах політики організації із захисту інформації повинно проводитися для всіх співробітників без винятку, а не лише для співробітників, в яких є електронний або фізичний доступ до інформаційних активів організації. В умовах сьогодення майже все, чим займаються співробітники, пов'язане з обробленням інформації. Ось чому політика безпеки організації повинна поширюватися по всьому підприємству, незалежно від положення співробітників.

Розроблення протидій соціальному інжинірингу необхідно почати зі створення групи людей, які будуть відповідати за безпеку. Вони повинні відповідати за розроблення політик і процедур безпеки, які повинні бути спрямовані на захист окремих співробітників і мережі організації в цілому. Ця група повинна мати співробітників із різних відділів.

До завдань цієї групи повинні входити такі речі як:

1. Забезпечення підтримки політик і процедур безпеки.

2. Допомога з розроблення навчально-методичних матеріалів для співробітників. Співробітник, відповідальний за розроблення програми інформаційної безпеки повинен виробити специфічні вимоги для окремих груп співробітників, що беруть участь у роботі з інформацією, яка обробляється організацією.

Тренінги повинні проводитися для таких груп персоналу:

1) менеджери;

2) IT-співробітники;

3) користувачі ПК;

4) обслуговувальний персонал;

5) адміністратори та їх асистенти;

6) техніки зв'язку;

7) охоронці (потрібно короткий курс навчання).

Технічні засоби навчання повинні мати:

1) демонстрацію соціального інжинірингу за допомогою гри за ролями;

2) оглядові медіазвіти щодо останніх атак на інші організації;

3) обговорення шляхів запобігання втрати інформації;

4) перегляд спеціальних відеоматеріалів із безпеки. Організація зобов'язана не лише мати прописані правила політик безпеки, а й спонукати співробітників, які працюють із корпоративною інформацією або комп'ютерною системою, старанно вивчати і дотримуватися цих правил.

Більше того, необхідно переконатися, що всі співробітники організації розуміють причину прийняття тих чи інших положень у правилах, тоді вони не будуть намагатися обходити ці правила для отримання власної вигоди. Правила безпеки повинні бути реалістичними, вони не повинні закликати співробітників виконувати занадто обтяжливі речі, які, швидше за все, будуть ними проігноровані.

Також програма навчання з безпеки повинна переконати співробітників, що необхідно виконувати доручення по роботі швидко, але найкоротший шлях, який нехтує системою безпеки, виявляється шкідливим для організації самої та співробітників. Але, навіть ознайомившись з усіма документами і навчанням, багато співробітників навряд чи змінять свою щоденну поведінку.

Для цього необхідно подбати про відповідну підкріплення. Воно може бути двох типів:

– негативне;
– позитивне.

Негативне означає покарання за якусь провину щодо дотримання заходів безпеки (наприклад, якщо під час перевірки виявилося, що співробітник прикріпив аркуш із паролем на монітор, то йому повинна бути зроблена догана). Інший метод – «прив'язати» турботу про безпеку до річного звіту про діяльність

співробітника, що, в свою чергу, змушує зрозуміти її важливість і, врешті-решт, відповідальність за безпеку лягає на кожного. Негативне підкріплення може служити для запобігання серйозних порушень (наприклад, установка неавторизованої точки доступу або модему). Позитивне підкріплення забезпечує натхненням співробітників щодо турботи про безпеку (наприклад, замість пошуку порушників політики – встановлення, кого з користувачів необхідно заохотити за точне дотримання інструкцій).

РОЗДІЛ 5. ВРАЗЛИВІСТЬ БЕЗДРОТОВОЇ МЕРЕЖІ WIFI

5.1. Бездротові мережі передачі даних (WLAN)

Бездротова мережа – тип комп'ютерної мережі, що використовує бездротове з'єднання для передавання даних і під'єднання до мережевих вузлів.

Рисунок 5.1 – Бездротова мережа

Wireless LAN (WLAN) – бездротова локальна мережа. За такого способу побудови мереж передавання даних здійснюється через радіоефір; об'єднання пристроїв у мережу відбувається без використання кабельних з'єднань. Найпоширенішими на сьогоднішній день способами побудови є Wi-Fi і WiMAX.
Безпечна мережа залишається важливою проблемою для WLAN. Під час під'єднання до бездротової локальної мережі зазвичай клієнти бездротового зв'язку повинні підтверджувати свою особу (процес, який називається автентифікацією). Такі технології, як WPA, підвищують рівень безпеки бездротових мереж, щоб конкурувати з традиційними провідними мережами.

Рисунок 5.2 – Wireless LAN (WLAN)

Плюси і мінуси WLAN

Плюси

1) Підтримання великої кількості пристроїв.
2) Легке налаштування бездротової мережі особливо порівняно з прокладкою кабелів для дротових мереж.
3) Простий доступ до WLAN, ніж дротовий ЛВС, оскільки довжина кабелю не є чинником.
4) Поширення бездротових локальних мереж навіть далеко від бізнесу чи будинку, як, наприклад, у громадських приміщеннях.

Мінуси

1) Зламати WLAN простіше, тому необхідне шифрування.
2) Бездротові перешкоди можуть викрасти швидкість і стабільність бездротової мережі.
3) Для розширення бездротової мережі потрібно більше бездротових пристроїв, як ретранслятори.
4) Бездротові локальні мережі, безумовно, мають свої переваги, але ми не повинні випускати з уваги падіння.

WLAN-пристрої

WLAN може містити від двох пристроїв до ста і більше. Однак бездротовими мережами стає все важче керувати, оскільки кількість пристроїв збільшується.

Бездротові локальні мережі можуть містити багато різних типів пристроїв, зокрема:

1) мобільні телефони;
2) ноутбуки та планшети;
3) інтернет аудіосистеми;
4) ігрові приставки;
5) будь-який інший пристрій чи пристрій із підключенням до інтернету.

Обладнання та з'єднання для бездротової локальної мережі WLAN-з'єднання працюють за допомогою радіопередавачів і приймачів, убудованих у клієнтські пристрої. Для бездротових мереж не потрібні кабелі, але для їх побудови зазвичай використовують декілька пристроїв спеціального призначення (які також мають власні радіоприймачі та приймачі антен).

Наприклад, локальні мережі Wi-Fi можуть бути побудовані в будь-якому з двох режимів: спеціальному або інфраструктурному.

Спеціальні бездротові локальні мережі Wi-Fi складаються з однорангових прямих з'єднань між клієнтами без залучення проміжних апаратних компонентів. Спеціальні локальні мережі можуть бути корисними для встановлення тимчасових зв'язків у деяких ситуаціях, але вони не мають масштабів для підтримання декількох пристроїв, а також можуть становити загрозу безпеці.

З іншого боку, Wi-Fi інфраструктурний режим WLAN використовує центральний пристрій, який називається точкою бездротового доступу (AP), до якого під'єднуються всі клієнти. У домашніх мережах бездротові широкосмугові маршрутизатори виконують функції AP, включаючи WLAN для домашнього доступу до Інтернету. Кілька точок доступу можна з'єднати з будь-якими і під'єднати кілька WLAN до більшої.

Деякі бездротові локальні мережі існують для розширення існуючої дротової мережі. Цей тип бездротової локальної мережі будується шляхом приєднання точки доступу до краю дротової мережі та налаштування точки доступу до роботи в мостовому режимі. Клієнти спілкуються з точкою доступу через бездротове з'єднання і можуть дістатися до мережі Ethernet через мостове з'єднання AP.

WLAN проти WWAN

Стільникові мережі підтримують мобільні телефони, що з'єднуються на великі відстані, тип так званих бездротових мереж широкої площі (WWAN). Що відрізняє локальну мережу від широкої мережі – це моделі використання, які вони підтримують, а також деякі обмеження щодо фізичної відстані та площі.

Локальна мережа охоплює окремі будівлі або громадські гарячі точки, що охоплюють сотні чи тисячі квадратних футів. Мережі широкої площі охоплюють міста чи географічні регіони, що охоплюють кілька кілометрів.

5.2. Протоколи та вразливості бездротової мережі

Існують два різновиди протоколу WPA: WPA2 Personal та WPA2 Enterprise. Їх відмінність полягає у 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 й 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 цей момент. За генерацію ключа відповідає сервер авторизації, зазвичай, це RADIUS-сервер. Протокол WPA2 також не позбавлений уразливостей. Одна з уразливостей була виявлена в 2008 році, яка дозволяла провести атаку «людина посередині». Для експлуатації такої уразливості атакуючий повинен бути

зареєстрований у цій мережі. Уразливість дозволяє учасникам мережі перехоплювати і 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. Унаслідок 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 ввімкнені 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:

CVE–2012–5958 – CVE–2012–5965 – уразливості, пов'язані з переповненням буфера і дозволяють зловмисникові віддалено виконати довільний код.

CVE–2013–0229 – CVE–2013–0230 – уразливості, що дозволяють виконати відмову в обслуговуванні пристроєм. Цим уразливостям схильні роутери фірм Broadcom, Asus, Cisco, TP-Link, Zyxel, D-Link, Netgear, US Robotics. Так як багато роутерів взаємодіють із UPnP через WAN, це робить їх вразливими не лише до атаки з локальної мережі, а і з віддалених мереж. Здебільшого атака на роутери з такою вразливістю в UPnP виконується через модифікований soap-запит, який призводить до помилки оброблення даних і потрапляння решти коду в довільну область оперативної пам'яті маршрутизатора, де він виконується з правами суперкористувача.

Механізм WPS (Wi-Fi Protected Setup), який використовується в роутерах і покликаний забезпечувати безпеку бездротової мережі, як виявилося, сам володіє серйозними вразливостями. WPS використовує восьмизначний PIN, підібравши який, можна витягти ключ WPA. Так як величина PIN невелика, отже, він уже потенційно схильний до атаки типу bruteforce (перебір значень). Так як PIN-код складається з восьми цифр, то існує 108 варіантів для підбирання. Остання цифра PIN-коду є контрольною сумою, отже, кількість комбінацій уже 107. Крім того, PIN-код ділиться на дві рівні частини, і кожна частина перевіряється окремо. У підсумку можливо 104 варіанти комбінацій для першої половини і 103 – для другої. У підсумку маємо всього лише 11 000 варіантів для повного перебору.

Використання «популярного» SSID також належить до ризиків безпеки бездротових мереж. SSID (Service Set Identifier, ідентифікатор точки доступу) – це ім'я мережі, яке відображається для всіх, хто шукає доступні бездротові мережі. Під «популярним» SSID маємо на увазі такі імена мережі, як Home або ASUS. Для відновлення пароля мережі з SSID можливе використання райдужної таблиці (rainbow table). У райдужних таблицях зберігаються списки всіх допустимих паролів кожного користувача, в разі несанкціонованого доступу до цього списку зловмисник дізнається всі призначені для користувача паролі.

Для підвищення безпеки домашньої бездротової мережі необхідно використовувати унікальне SSID. Крім того, існують уразливості бездротових мереж, пов'язані з фізичною природою переданого сигналу. Оскільки бездротові мережі використовують радіохвилі, якість роботи мережі залежить від багатьох чинників. Найбільш яскравим прикладом є інтерференція радіосигналів, здатна значно погіршити показники пропускної здатності та кількість підтримуваних користувачів, аж до повної неможливості використання мережі.

Джерелом інтерференції може бути будь-який пристрій, що випромінює сигнал достатньої потужності в тому ж частотному діапазоні, що і точка доступу: від сусідніх точок

доступу в умовах густонаселеного офісного центру до електромоторів на виробництві, гарнітур Bluetooth і навіть мікрохвильовок. З іншого боку, зловмисники можуть використовувати інтерференцію для організації DoS атаки на мережу (самовільно встановлені точки доступу, що надають можливість неавторизованого доступу до корпоративної мережі в обхід механізмів захисту, визначених корпоративною політикою безпеки), що працюють на тому самому каналі, що і легітимні точки доступу, відкривають не лише доступ у мережу, а і порушують працездатність «правильної» бездротової мережі.

Крім того, для реалізації атак на кінцевих користувачів і для проникнення в мережу за допомогою атаки Man-In-The Middle (людина посередині) зловмисники перемикають легітимну точку доступу на себе з тим самим ім'ям мережі. Низькі швидкості роботи точок доступу дозволяють підключатися на більшій дальності, що дає додаткову можливість безпечного віддаленого злому. Отже, бездротові мережі піддаються множинним загрозам як на фізичному, так і на канальному й мережевому рівнях. Тому під час побудови безпечної Wi-Fi мережі дуже важливо правильно вибирати правильне обладнання, протоколи і конфігурацію мереж.

Обладнання бездротових локальних мереж WLAN (Wireless Local Area Network) містить точки бездротового доступу та робочі станції для кожного абонента. Точки доступу AP (Access Point) виконують роль концентраторів, які забезпечують зв'язок між абонентами і між собою, а також функцію мостів, які здійснюють зв'язок із кабельної локальної мережі з Інтернетом. Кожна точка доступу може обслуговувати кілька абонентів. Кілька близько розміщених точок доступу утворюють зону доступу Wi-Fi, в межах якої всі абоненти, забезпечені бездротовими адаптерами, отримують доступ до мережі. Такі зони доступу створюються в місцях масового скупчення людей: в аеропортах, студентських містечках, бібліотеках, магазинах, бізнес-центрах тощо. У точці доступу є

ідентифікатор набору сервісів SSID (Service Network Idetnifier). SSID – це 32-бітний рядок, що використовується як ім'я бездротової мережі, з якої асоціюються всі вузли. Ідентифікатор SSID необхідний для під'єднання робочої станції до мережі. Щоб зв'язати робочу станцію з точкою доступу, обидві системи повинні мати один і той самий SSID.

Якщо робоча станція не має потрібного SSID, то вона не зможе зв'язатися з точкою доступу і з'єднатися з мережею. Основна відмінність між провідними і бездротовими мережами пов'язана з наявністю неконтрольованої області між кінцевими точками бездротової мережі. Це дозволяє атакуючим, які перебувають у безпосередній близькості від бездротових структур, виробляти цілу низку нападів, які неможливі в дротовому світі. Під час використання бездротового доступу до локальної мережі загрози безпеки істотно зростають. Перелічимо основні вразливості та загрози бездротових мереж.

Мовлення радіомаяка. Точка доступу містить із певною частотою широкомовний «радіомаяк», щоб оповіщати навколишні бездротові вузли про свою присутність. Ці широкомовні сигнали містять основну інформацію про точку бездротового доступу, враховуючи зазвичай SSID, і запрошують зареєструватися бездротові вузли в цій сфері.

Будь-яка робоча станція, що перебуває в режимі очікування, може отримати SSID і додати себе у відповідну мережу. Мовлення радіомаяка є вродженою патологією бездротових мереж. Багато моделей дозволяють відключати показ SSID, щоб утруднити бездротове підслуховування, але SSID проте посилається під час під'єднання, тому все одно існує невелике вікно уразливості.

Виявлення WLAN. Для виявлення бездротових мереж WLAN використовується, наприклад, утиліта NetStumber спільно з супутниковим навігатором глобальної системи позиціонування GPS. Ця утиліта ідентифікує SSID мережі WLAN, а також визначає, чи використовується в ній система шифрування WEP. Застосування зовнішньої антени на портативному комп'ютері

уможливлює виявлення мереж WLAN під час обходу потрібного району або поїздки по місту. Надійним методом виявлення WLAN є обстеження офісної будівлі з переносним комп'ютером у руках.

Підслуховування. Підслуховування ведуть для збирання інформації про мережу, яку передбачається атакувати згодом. Перехоплювач може використовувати здобуті дані для того, щоб отримати доступ до мережевих ресурсів. Обладнання, що використовується для підслуховування в мережі, може бути не складніше того, яке застосовується для звичайного доступу до цієї мережі. Бездротові мережі за своєю природою дозволяють з'єднувати з фізичної мережею комп'ютери, що перебували безпосередньо в мережі. Це дозволяє під'єднатися до бездротової мережі, розміщеної в будівлі, людині, яка сидить у машині на стоянці поруч із ним. Атаку за допомогою пасивного прослуховування практично неможливо виявити.

Помилкові точки доступу в мережу. Досвідчений атакуючий може організувати неправдиву точку доступу з імітацією мережевих ресурсів. Абоненти, нічого не підозрюючи, звертаються до цієї помилкової точки доступу і повідомляють їй свої важливі реквізити, наприклад, аутентифікаційну інформацію. Цей тип атак іноді застосовують у поєднанні з прямим глушінням, щоб заглушити справжню точку доступу в мережу.

Відмова в обслуговуванні. Повну паралізацію мережі може викликати атака типу «відмова в обслуговуванні» (Dos). Мета будь-якої DoS-атаки полягає в створенні перешкоди під час доступу користувача до мережевих ресурсів. Бездротові системи особливо сприйнятливі до таких атак. Фізичний рівень у бездротовій мережі – абстрактний простір навколо точки доступу. Зловмисник може ввімкнути пристрій, що заповнює весь спектр на робочій частоті перешкодами і нелегальним трафіком, – таке завдання не викликає особливих труднощів. Сам факт проведення DoS-атаки на фізичному рівні в бездротовій мережі важко довести.

Атаки типу «людина-в-середині». Атаки типу «людина-в-середині» виконуються на бездротових мережах набагато простіше, ніж на провідних, так як до провідної мережі потрібно реалізувати певний вид доступу. Зазвичай атаки «людина-в-середині» використовуються для порушення конфіденційності та цілісності сеансу зв'язку. Атаки «людина-в-середині» більш складні, ніж більшість інших атак: для їх проведення потрібна детальна інформація про мережу. Зловмисник зазвичай підміняє ідентифікацію одного з мережевих ресурсів. Зловмисник використовує можливість прослуховування і нелегального захоплення потоку даних із метою зміни його вмісту, необхідного для задоволення деяких своїх цілей, наприклад, спуфінгу IP-адрес, зміни MAC-адреси для імітування іншого хоста тощо.

Анонімний доступ в Інтернет. Незахищені бездротові ЛОМ (локальні обчислювальні мережі) забезпечують хакерам найкращий анонімний доступ для атак через Інтернет. Хакери можуть використовувати незахищену мережу WLAN організації для виходу через неї в Інтернет, де вони будуть здійснювати протиправні дії, не залишаючи при цьому своїх слідів. Організація з незахищеною ЛОМ формально стає джерелом атакуючого трафіку, націленого на іншу комп'ютерну систему, що пов'язано з потенційним ризиком правової відповідальності за заподіяну шкоду жертві атаки хакерів. Атаки, які використовуються хакерами для злому бездротових мереж, не обмежуються описаними вище.

5.3. Методи захисту інформації в мережах Wi-Fi

Одним із способів авторизації користувачів у бездротовій мережі є фільтрація за MAC ідентифікатором. Кожний бездротовий адаптер має свій унікальний фізичний ідентифікатор, який установлюється на заводі. За первинного під'єднання до точки доступу адміністратор повинен додати такий ідентифікатор клієнта у спеціальний список точки доступу.

Такий список зберігається на точці доступу. Під час під'єднання будь-якого клієнта точка доступу перевіряє його фізичний ідентифікатор шляхом пошуку його в спеціальному списку ідентифікаторів. Якщо ідентифікатор знайдено, то точка доступу починає обслуговувати клієнта, якщо ж ні – просто ігнорує його. Недоліком такого способу захисту є можливість зміни фізичного ідентифікатора на сучасних клієнтських адаптерах. Дізнатися фізичний ідентифікатор іншого користувача також не є проблемою – для цього існує спеціальне програмне забезпечення, яке дозволяє прослуховувати ефір та ідентифікувати окремих користувачів.

Важливо відзначити, що зазначені методи не забезпечують конфіденційність даних, що передаються в мережі, вони просто обмежують доступ до мережі. Тобто навіть якщо всі ці засоби включені на точці доступу, зловмисник зможе, ввімкнувши свій бездротовий адаптер у режимі «monitor mode», слухати ефір і виловлювати всю передану інформацію.

Очевидно, що для захисту мережі потрібно активізувати механізм захисту, що вбудований в обладнання, яке надає сервіс бездротових мереж. На сьогодні налаштування захисту обладнання бездротових мереж вимагає введення пароля. В деяких випадках (наприклад, недосвідчений користувач) пароль може бути найбільш уразливим місцем усієї системи. Все обладнання завжди має певні налаштування за замовчуванням. Інформація про ці налаштування повинна бути в інструкції до цього обладнання. Іншими словами, така інформація є загальновідомою. Якщо користувач не змінить налаштування пароля для точки доступу, зловмисник зможе легко підібрати пароль і отримати доступ до всієї мережі. Також важливим чинником є складність пароля. Загальновідомо, що чим довший і складніший пароль, тим вищу він має криптостійкість, і для його підбору потрібно більше часу. Тому рекомендують використовувати випадково згенеровані паролі достатньої довжини. Рекомендують також змінювати пароль через певні проміжки часу.

Існує декілька алгоритмів захисту для бездротових мереж стандарту 802.11. Це WEP, WPA і WPA2. Кожен із них має декілька режимів роботи.

Технологія WEP (Wired Equivalent Privacy) була затверджена у 1997 році, при цьому в 2000 році було написано статтю про недоліки цієї технології. У WEP використовується алгоритм RC4 на статичному ключі. Для підвищення захисту частина ключа є статичною, а інша частина – динамічною (вектор ініціалізації), що змінюється в процесі роботи мережі. Основним недоліком WEP є те, що вектор ініціалізації повторюється через деякі проміжки часу. Для того щоб зламати це шифрування необхідно лише зібрати ці повтори і за секунди отримати іншу частину ключа. Весь процес взлому становить 5–10 хвилин. Саме через це не рекомендують застосовувати цей алгоритм захисту за будь-яких умов (див. рис. 5.3).

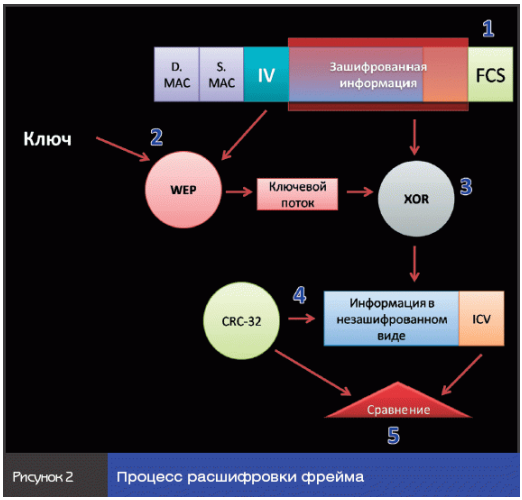

Рисунок 5.3 – Технологія WEP

Технологія WPA (Wi-Fi Protected Access) була впроваджена замість застарілого протоколу WEP. WPA була перехідною технологією між WEP та відносно новим стандартом безпеки

802.11i. За шифрування даних у WPA відповідає протокол TKIP, який, хоча і використовує самий алгоритм шифрування – RC4 – що й у WEP, але на відміну від останнього, використовує динамічні ключі (тобто ключі часто змінюються). Він застосовує більш довгий вектор ініціалізації і використовує криптографічну контрольну суму (MIC) для підтвердження цілісності пакетів (остання є функцією від адреси джерела і призначення, а також поля даних). Можна виділити два основних режими роботи технології WPA: WPA-PSK і WPA-Enterprise.

Будь-яке сучасне бездротове обладнання стандарту 802.11 підтримує обидва ці режими. Під час використання режиму WPA-PSK (так званий персональний режим) на точці доступу прописується ключ доступу, ввівши який користувач може почати користуватися ресурсами мережі. Такий спосіб захисту досить стійкий, але не досить зручний для адміністрування, оскільки для кожного користувача мережі потрібно ввести пароль точки доступу для його успішного під'єднання. За досить малих розмірів мережі це припустимо, але зі зростанням кількості клієнтів це перетворюється на досить важку задачу. Також, якщо є потреба відключити користувача від мережі, потрібно змінювати ключ точки доступу, причому після таких дій потрібно переналаштовувати всіх користувачів мережі.

Під час використання технології WPA у режимі WPA-Enterprise для аутентифікації користувачів використовують зовнішній сервер (відносно точки доступу), наприклад, RADIUS-сервер. У такому режимі користувачу необхідно ввести пару «логін – пароль», за яким і відбувається під'єднання користувача до мережі. Водночас пара «логін – пароль» унікальна для кожного користувача.

На зміну протоколу шифрування TKIP, в якому теж знайдені недоліки, прийшов покращений алгоритм шифрування AES (Advanced Encryption Standard). AES також відомий під назвою Rijndael – симетричний алгоритм блочного шифрування (розмір блока 128 біт, ключ 128 / 192 / 256 біт). Сучасне обладнання надає вільний вибір між цими двома протоколами. Рекомендують

вибирати AES як більш надійний метод шифрування.

Технологія WPA2. На зміну протоколу WPA прийшов протокол WPA2, який входить до стандарту безпеки бездротових мереж 802.11i. Протоколи WPA2 працюють у двох режимах аутентифікації: персональному (Personal) та корпоративному (Enterprise). У режимі WPA2-Personal з введеної відкритим текстом парольної фрази генерується 256-розрядний ключ PSK (PreShared Key). Ключ спільно з ідентифікатором SSID (Service Set Identifier) використовують для генерації тимчасових сеансових ключів PTK (Pairwise Transient Key), для взаємодії бездротових пристроїв. Як і протоколу WPA-PSK, протоколу WPA2-Personal притаманні певні проблеми, пов'язані з необхідністю розподілу та підтриманням ключів на бездротових пристроях мережі, що робить його більш корисним для застосування в невеликих мережах із десятка пристроїв, водночас як для корпоративних мереж оптимальний WPA2 – Enterprise.

Технологія VPN. Із додаткових методів захисту бездротових мереж можна виділити технологію VPN (Virtual Private Network). Ця технологія дозволяє створити у межах будь-якої мережі або декількох мереж віртуальну персональну мережу, яка надає широкі можливості щодо забезпечення конфіденційності клієнтів. Принцип дії VPN – створення так званих безпечних «тунелів» від користувача до вузла доступу або сервера. Для шифрування трафіку в VPN найчастіше застосовують протокол IPSec (близько 70 % випадків), рідше – PPTP або L2TP. Водночас можуть використовуватися такі алгоритми, як DES, Triple DES, AES і MD5. VPN підтримується на багатьох платформах (Windows, Linux, Solaris) як програмними, так і апаратними засобами. Варто відзначити високу надійність технології. Зазвичай VPN рекомендують застосовувати у великих корпоративних мережах, для домашнього користувача встановлення та налаштування може здатися занадто громіздкою і трудомісткою. Технологію VPN можна використовувати як додатковий засіб захисту мережі у поєднанні з будь-якою технологією захисту бездротових мереж.

РОЗДІЛ 6. БЕЗПЕКА В СОЦІАЛЬНИХ МЕРЕЖАХ

6.1. Персональна інформація в соціальній мережі

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 настала 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 більше ніж дві третини онлайн-аудиторії у всьому світі, і це четверта за популярністю онлайн-категорія після пошукових та інформаційних порталів та 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 профіля особливу увагу потрібно 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» мети. Загалом, ці дві хвилини найбільш важливі, оскільки показавши про себе інформацію також, що ти маєш велике коло знайомств, то знай – ти їхній «клієнт».

Проте, не стати «клієнтом» досить просто – достатньо не надавати реальної інформації про себе або надавати її частково. Для цього в розділі «Налаштування приватності» потрібна зробити певні коригування:

– закрити доступ до персональної інформації (дата народження, номер телефону тощо) всім користувачам,

окрім друзів. Дуже важливо закрити також доступ для друзів друзів;
- у всіх соцмережах можна розділяти друзів за групами. Створи спеціальну групу для «ненадійних друзів» (яких ти не знаєш у реальному житті) та обмеж їхні права на рівні звичайних користувачів;
- закрити можливість перегляду фото та відеоматеріалів усім користувачам, окрім друзів;
- не надавати інформації про місце роботи, рік закінчення школи, вузу тощо. Якщо написав раніше, то обов'язково видали!

Налаштувавши, таким чином, доступ до власної сторінки, всі, окрім друзів, бачитимуть лише ім'я, фото та інформацію, якою користувач ділиться на своїй сторінці. Швидше за все таку сторінку проігнорують або просто не стануть морочитися із закритою сторінкою, коли в мережі повно відкритих.

Також рекомендують регулярно перевіряти ці налаштування: соцмережі можуть змінити їх без вашого відома й тоді все, що ви довіряли лише друзям, стане загальнодоступним. Для підвищення рівня безпеки своїх користувачів соцмережі постійно вдосконалюють засоби безпеки і всіляко допомагають користувачам – це і детально прописані розділи в рубриці «допомога», інструкції під час заповнення профіля та різні спільноти. Та й техпідтримка, зрештою, – не ігноруйте всю пропоновану вам допомогу. Уважно вивчіть усі можливості – це і прив'язка до мобільного телефону, і «довірені друзі», і GeoIP, і HTTPS, і багато інших способів – користуйтеся.

6.2. Інформаційні небезпеки під час використання соціальних мереж Інтернету

Розглянемо інформаційні небезпеки, які з'являються під час використання як соціальних мереж, так й Інтернету в цілому. Основним джерелом цих небезпек є діяльність хакерів. Одні

зловмисники прагнуть одержати персональну інформацію з метою отримання вигоди. Інші обирають об'єктом атак комп'ютерну систему та намагаються вивести її з ладу або використати для приховування своїх шкідливих дій. Для зламу акаунту користувача хакеру необхідно докласти зусиль, щоб дізнатися пароль, іншими словами – зламати його. Найбільш поширеними способами реалізації зламу пароля є такі технології.

Брутфорс – метод пошуку та зламу пароля, який дозволяє перебрати всі теоретично можливі варіанти, складені з певного набору символів. До нього також відносять атаку перебору пароля за словником або ручного підбору часто використовуваних простих паролів. Для захисту від цього способу зламу в паролі не потрібно зазначати дату народження, номери телефонів, ім'я, кличку домашньої тварини, прості відомі паролі та будь-які інші дані, потенційно відомі деякому колу осіб. У паролі потрібно зазначити певний набір символів, який практично неможливо вгадати (див. рис. 6.1).

Критерієм складності пароля є наявність символів із кожного пункту такого переліку:

- символи a... z (лише малі літери); – символи Aa... Zz (великі та малі літери);
- цифри; – недруковані ASCII-символи, літери інших алфавітів;
- спеціальні символи:;% «№ *? тощо.

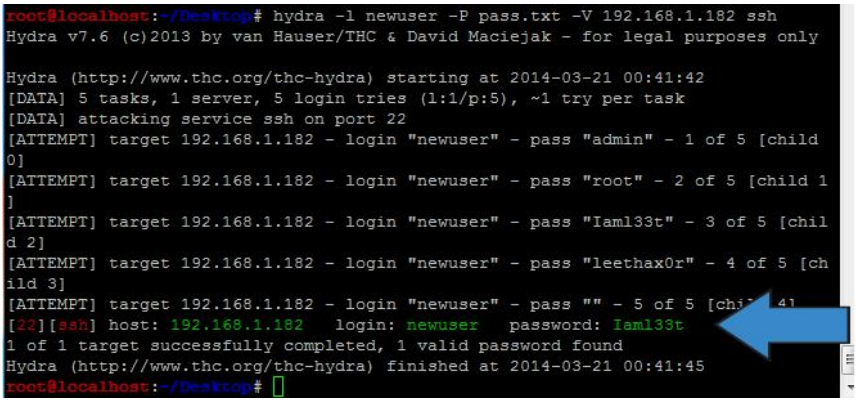

Рисунок 6.1 – «Брутфорс»

Соціальна інженерія або соціотехніка. Цей метод ґрунтується на довірі користувача. Для цього використовують сфальсифіковані сайти та фіктивні електронні повідомлення від імені реальних компаній із проханням надати особисту інформацію. Головним захистом у цьому разі є пильність користувача. Нікому не можна повідомляти або надсилати паролі (див. рис. 6.2.)

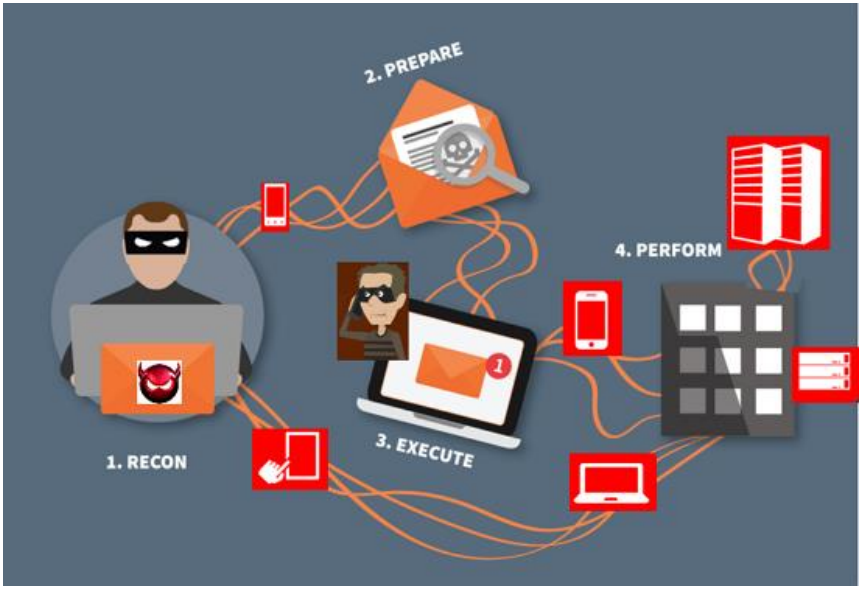

Рисунок 6.2 – «Соціальна інженерія»

Кейлогери – це програмний продукт або апаратний пристрій, що реєструє кожне натискання кнопки миші або клавіші на клавіатурі комп'ютера та записує у файл разом із датою та часом натискання. Отже, в зловмисника буде пароль у головному вигляді. Гарантованим захистом від цього методу може бути лише вихід в Інтернет і введення пароля з власного або надійного, перевіреного комп'ютера (див. рис. 6.3.).

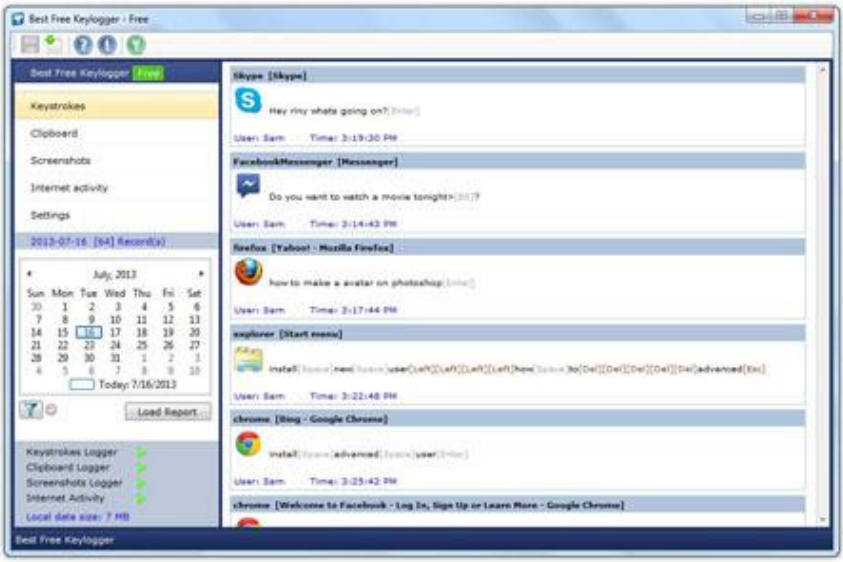

Рисунок 6.3 – «Кейлогери»

Програмний метод зламу. Цей метод доступний хакерам і полягає в пошуку помилок у коді сайтів, що дозволяють отримати доступ до бази даних із паролями. У такому разі дані можуть відновити лише адміністратори.

Фішинг – технологія інтернет-шахрайства з метою одержання ідентифікаційних даних користувачів. Реалізується за допомогою заманювання їх на підставні сайти, які є точною або майже точною копією оригіналу. Для захисту виробники основних Інтернет-браузерів домовилися про застосування однакових способів інформування користувачів про те, що вони відкрили підозрілий сайт, який може належати шахраям. Нові версії браузерів уже мають таку можливість, яка відповідно іменується «анти-фішинг». Від користувачів вимагається лише вчасно оновлювати версії браузерів (див. рис. 6.4.).

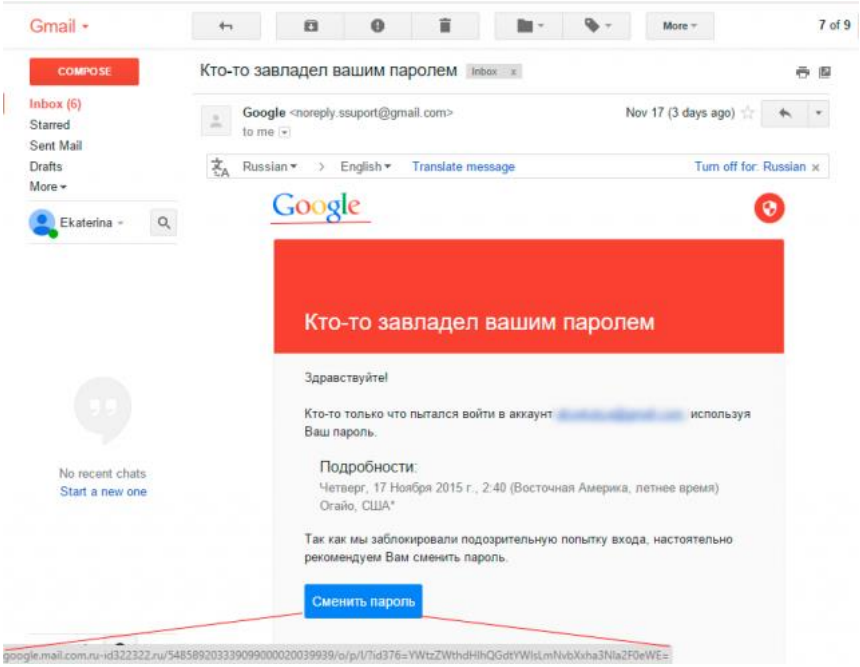

Рисунок 6.4 – «Фішинг»

Спамом називають небажану електронну пошту, тобто пошту, що надходить без згоди користувача. Він може прикріплюватися до всіх повідомлень у вигляді посилання на сторонній сайт. У цьому разі необхідно змінити браузер на Mozilla Firefox або Opera, які блокують заданий користувачем спам. А також варто дотримуватися запобіжних заходів, які не дозволять спамерам дізнатися адресу електронної пошти користувача:

- не варто без необхідності публікувати адресу електронної пошти на Webсайтах чи в групах соціальних мереж;
- не потрібно реєструватися на підозрілих сайтах, натомість краще зазначити спеціально для цього створену адресу;
- ніколи не відповідати на спам і не переходити за посиланням, які містяться в ньому, оскільки це буде

підтвердженням використання цієї електронної адреси і збільшить надходження спаму;

– обираючи ім’я електронної пошти, варто створювати його довгим і незручним для вгадування (див. рис. 6.5.).

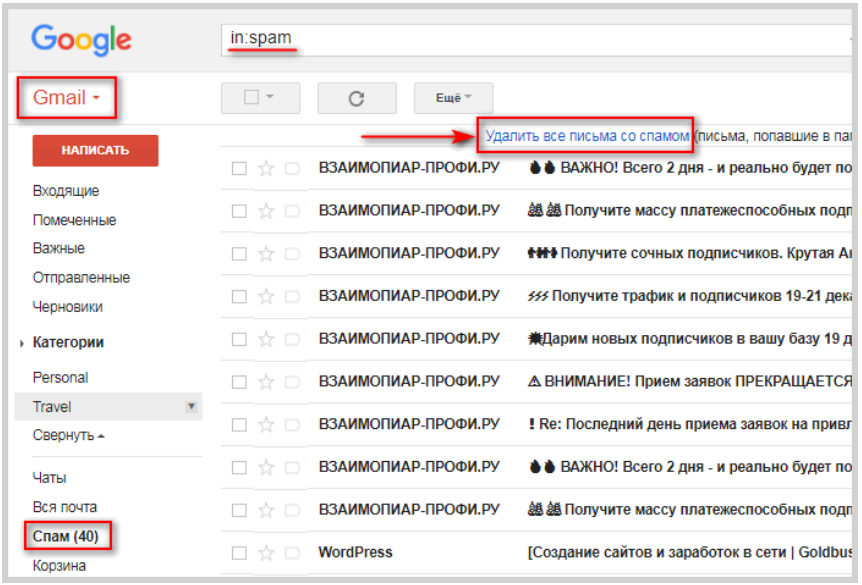

Рисунок 6.5 – «Спам»

Віруси – малі за розміром програми, які поширюються, копіюючи самих себе. Вони потрапляють до комп’ютерної системи і деякий час можуть себе не проявляти, і лише після настання певної дати чи події активізуються та завдають їй шкоди.

Рекомендують використовувати декілька антивірусних пакетів одночасно, щоденно оновлювати антивірусні бази та встановлювати найновіші версії ліцензійного програмного забезпечення. Про користь і ризики соціальних мереж можна довго розмірковувати, але в будь-якому разі це явище має місце. Тому необхідно допомогти користувачеві зробити мінімум помилок під час роботи у відповідній мережі. Необхідно

розуміти, що профіль у будь-якій соціальній мережі вразливий, особливо під час використання стандартних параметрів.

Тому потрібно дотримуватися таких рекомендацій:

- подбайте про надійний пароль для профіля;
- будьте обережні під час встановлення додатків від сторонніх розробників, ні в якому разі не встановлюйте додатки з джерел, яким не довіряєте;
- приймайте пропозиції про дружбу лише від тих людей, яких знаєте особисто і безпосередньо;
- ретельно прочитавши політику конфіденційності, обмежте особисту інформацію, яку збираєтесь зробити загальнодоступною;
- перевіряйте інформацію, яку надсилаєте на сайт;
- завжди використовуйте для кожного форуму, сайту та поштової скриньки різні паролі, інакше шанс позбавлення всіх акаунтів збільшується під час крадіжки одного пароля (див. рис. 6.6.).

Рисунок 6.6 – «Віруси»

6.3. Забезпечення інформаційної безпеки в соціальних мережах

Останнім часом користувачі все менше довіряють соціальним мережам і все частіше починають фільтрувати інформацію, яку готові довірити мережі, давати неправдиву інформацію або взагалі видаляються з мережі, однак навіть видалення не дає впевненості: часто інформація зберігається на серверах компанії і може використовуватися в подальшому. Зокрема так робить Facebook, ВКонтакте та інші мережі. Виділимо основні параметри, які є базовими для забезпечення захисту інформації:

- конфіденційність – гарантія того, що конкретна інформація доступна лише тому колу осіб, для кого вона призначена; порушення цієї категорії називається розкраданням або розкриттям інформації;
- цілісність – гарантія того, що інформація зараз існує в її початковому вигляді, тобто під час її зберігання або передачі не було проведено несанкціонованих змін; порушення цієї категорії називається фальсифікацією повідомлення;
- автентичність – гарантія того, що джерелом інформації є саме та особа, яку заявлено як її автора; порушення цієї категорії також називається фальсифікацією, але вже автора повідомлення;
- апельованість – гарантія того, що за необхідності можна буде довести, що автором повідомлення є саме заявлена людина, і не може бути ніхто інший; відмінність цієї категорії від попередньої в тому, що під час підміни автора інша людина намагається привласнити собі авторство повідомлення, а під час порушення апельованості – сам автор намагається «відхреститися» від своїх слів.

Загрози інформаційної безпеки – це зворотний бік використання інформаційних технологій. Загроза – це потенційна можливість певним чином порушити інформаційну безпеку. Під час системного розгляду різних видів порушень захисту

конфіденційної інформації в соціальній мережі відповідно до якісно-кількісних характеристик циркулюючої всередині мережі інформації необхідними для оцінювання її вразливостей за ступенем важливості для механізмів захисту можна виділити такі типи основних загроз інформації в соціальній мережі:

- загроза конфіденційності (витік конфіденційної інформації та заподіяння прямого або непрямого збитку користувачеві соціальної мережі);
- загроза цілісності (модифікація інформації усередині мережі інформації і втрата її адекватності);
- загроза доступності (порушення доступу до мережевої інформації та блокування доступу до ресурсу);
- загроза повноті (знищення інформації усередині мережі та заподіяння прямого або непрямого збитку як користувачеві соціальної мережі, так і її власнику);
- загроза актуальності (затримання надходження легальним користувачем мережі інформації);
- загроза важливості (несанкціоноване читання конфіденційної мережевої інформації, що призводить до втрати її ціннісних характеристик);
- загроза адресності (переадресація мережевої інформації, що може призводити до зниження її конфіденційності та доступності);
- загроза надмірності інформації (багаторазове дублювання мережевої інформації).

На жаль, на законодавчому рівні проблема щодо захисту інформації користувача недостатньо опрацьована. Забезпечення безпеки персональних даних у більшості випадків регламентується виключно правилами захисту інформації про користувачів і правилами користування сайтом.

Отже, для захисту від загроз необхідно мати на увазі такі:

1) Слід реєструватися не у всіх підряд соцмережах, а лише в тих, які викликають довіру та пропонують надійні механізми аутентифікації і розмежування доступу до особистої інформації користувача.

2) Авторизацію в соцмережі необхідно виконувати, вводячи її URL в адресний рядок браузера вручну або використовуючи заздалегідь збережені вкладки чи посилання.
3) Якщо є сумніви щодо знайомства з користувачем, який подав заявку в друзі, потрібно дочекатися підтвердження його особистості через інші джерела.
4) Обов'язково час від часу необхідно змінювати паролі на всіх своїх сторінках. Бажано використовувати окремі паролі для кожного акаунту – тоді, в разі зламу однієї сторінки, інші залишаться в безпеці.
5) Потрібно пам'ятати, що будь-яка інформація, розміщена в Інтернеті, з великою ймовірністю залишається там назавжди, навіть у разі її видалення автором, адже може бути збережена або поширена іншими користувачами.
6) Особливу увагу необхідно приділяти посиланням, які надходять від інших користувачів – вони можуть бути частиною фішингової чи фармінгової атаки.

Сьогодні саме системний підхід до проблеми організації інформаційної безпеки, формування загальнонаціональної інформаційної системи, скоординованої в своїй діяльності державою, може стати запорукою нейтралізації сучасних інформаційних загроз, зокрема у сфері розвитку соціальних мереж, використання позитивних чинників розвитку інформатизації в національних інтересах.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Архітектура комп'ютерних систем: конспект лекцій для студентів усіх форм навчання з курсу «Архітектура комп'ютерних систем» / укладач О. С. Голотенко. – Тернопіль : Вид-во ТНТУ імені Івана Пулюя, 2016. – 120 с.
2. Бабак В. П. Інформаційна безпека та сучасні мережеві технології. Англ.-укр.-рос. слов. термінів / укладачі: В. П. Бабак, О. Г. Корченко. – Київ : НАУ, 2003. – 670 с.
3. Бандурян А. Аналіз загроз для бездротових мереж / А. Бандурян // Комп'ютерний огляд. – 2010. – № 12 (723).
4. Бойко О. М. Розробка методології захисту інформації від атак соціальної інженерії : дипломна робота магістра за спеціальністю 125 «Кібербезпека» / О. М. Бойко. – Тернопіль : ТНТУ, 2020. – 63 с.
5. Буров Є. В. Комп'ютерні мережі : підручник / Є. В. Буров. – Львів : «Магнолія 2006», 2010. – 262 с.
6. Інформаційна кібербезпека: соціотехнічний аспект / В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа. – Київ : Державний університет телекомунікацій.
7. Гатчин Ю. А. Теория информационной безопасности и методология защиты информации / Ю. А. Гатчин, В. В. Сухостат. – Санкт-Петербург : СПбГУ ИТМО, 2010. – 98 с.
8. Гвильдис Е. А. Человеческий фактор в проблеме обеспечения информационной безопасности компании : сб. науч. тр. – Киев : НАУ, 2007. – С. 166–171.
9. Глущенко С. Д. Соціально-психологічні особливості Інтернет-адиктивної поведінки особистості / С. Д. Глущенко // Молодь: освіта, наука, духовність : тези доповідей. – Київ : Університет «Україна», 2008. – Ч. 1. – 547 с.

10. Голубєв В. О. Інформаційна безпека: проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій / В. О. Голубєв, В. Д. Гавловський, В. С. Цимбалюк ; за заг. ред. Р. А. Калюжного. – Запоріжжя : Просвіта, 2001. – 252 с.
11. Гордієнко С. Б. Методи та рекомендації забезпечення інформаційної безпеки консалтингової компанії / С. Б. Гордієнко, О. С. Микитенко, В. Г. Данильчук // Вісник ДУІКТ. – 2013. – № 1. – С. 104–107.
12. Гордійчик С. В. Безпека бездротових мереж. Гаряча лінія-Телеком / С. В. Гордійчик, В. В. Дубровін. – 2008. – 288 с.
13. Готун А. М. Нові інформаційно-комунікаційні технології в глобальній системі політичної комунікації : автореф. дис. ... канд. політ. наук : 23.00.04 / А. М. Готун ; Ін-т світ. економіки і міжнар. відносин НАН України. – Київ, 2010. – 17 с.
14. Даниленко С. І. Громадянський вимір інформаційно-комунікаційної революції : концептуально-теоретичні та політико-прикладні аспекти : автореф. дис. … д-ра політ. наук / С. І. Даниленко. – Київ, 2011. – 36 с.
15. Дзьобань О. П. До проблеми загроз інформаційній безпеці України: цивілізаційний контекст / О. П. Дзьобань // Побудова інформаційного суспільства: ресурси і технології : матеріали XVIII Міжнародної науково-практичної конференції (Київ, 19–20 верес. 2019 р.). – Київ : УкрІНТЕІ, 2019. – С. 173–176.
16. Дзюндзюк В. Б. Віртуальні співтовариства: потенційна загроза для національної безпеки [Електронний ресурс] / В. Б. Дзюндзюк // Державне будівництво. – 2011. – № 1. – Режим доступу : http://www.kbuapa.kharkov.ua.
17. Дослідження методики протидії соціальному інжинірингу для захисту інформації на об'єктах інформаційної діяльності [Електронний ресурс]. – Режим доступу : http://www.dut.edu.ua/uploads/p_422_79548521.pdf.

18. Ємельянов С. Л. Шляхи і канали витоку інформації з типового об'єкта інформатизації / С. Л. Ємельянов, В. В. Носов // Право і Безпека. – 2009. – № 1. – С. 273–279.
19. Загрози та вразливості бездротових мереж [Електронний ресурс]. – Режим доступу : http://dspace.kntu.kr.ua/jspui /bitstream/123456789/5022/1/AUConferenceCyberSecurity_ November2016_p146. pdf.
20. Захаркін О. О. Інформаційні системи та технології у фінансових установах: конспект лекцій [Електронний ресурс] / О. О. Захаркін, М. Ю. Абрамчук, М. А. Деркач. Суми : Вид-во СумДУ, 2007. – 80 с. – Режим доступу : http: //elkniga.info/book_188.html.
21. Зламати Wi-Fi за 10 годин // Журнал «Хакер». – 2012. – № 3 (158). – С. 18–22.
22. Інформаційна безпека держави : навч. посіб. для студ. спец. «Управління інформаційною безпекою», «Кібербезпека» / В. І. Гур'єв, Д. Б. Мехед, Ю. М. Ткач, І. В. Фірсова. – Ніжин : ФОП Лук'яненко В. В. ; ТПК «Орхідея», 2018. – 166 с.
23. Кавун С. В. Інформаційна безпека : навчальний посібник / С. В. Кавун, В. В. Носов, О. В. Манжай. – Харків : Вид-во ХНЕУ, 2008. – 352 с.
24. Калиновський Ю. Ю. Аксіологічний вимір інформаційної безпеки української держави / Ю. Ю. Калиновський, Є. М. Мануйлов ; редкол.: А. П. Гетьман та ін. // Вісник Національного університету «Юридична академія України імені Ярослава Мудрого». Серія: Філософія, філософія права, політологія, соціологія. – Харків : Право, 2017. – № 3 (34). – С. 13–31.
25. Калиновський Ю. Ю. Роль і місце інформаційної безпеки у розбудові сучасної української держави / Ю. Ю. Калиновський, Є. М. Мануйлов ; редкол.: А. П. Гетьман та ін. // Вісник Національного університету «Юридична академія України імені Ярослава Мудрого». Серія: Філософія, філософія права, політологія,

соціологія. – Харків : Право, 2016. – № 2 (29). – С. 144–154.
26. Кин Э. Ничего личного: как социальные сети, поисковые системы и спецслужбы используют наши персональные данные / Э. Кин. – Москва, 2016. – С. 23–173.
27. Кібератака. Термінологічний словник з питань запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму, фінансуванню розповсюдження зброї масового знищення та корупції / А. Г. Чубенко та ін. – Київ : Ваіте, 2018. – С. 331–332.
28. Корченко О. Г. Класифікація методів соціального інжинірингу / О. Г. Корченко, Є. В. Паціра, Д. А. Горніцька // Захист інформації. – 2007. – № 4 (36). – С. 37–45.
29. Ковтун С. В. Інформаційна безпека : підручник / С. В. Ковтун. – Харків : Вид. ХНЕУ, 2009. – 368 с.
30. Комп'ютерні мережі : навч. посібник / О. Д. Азаров та ін. – Вінниця : ВНТУ, 2013. – 371 с.
31. Комп'ютерні мережі: навчальний посібник / А. Г. Микитишин, М. М. Митник, П. Д. Стухляк, В. В. Пасічник. – Львів : Магнолія 2006, 2013. – 256 с.
32. Конспект лекцій з дисципліни «Інформаційно-комунікаційні системи» для студентів усіх форм навчання спеціальності 125 «Кібербезпека» за освітньою програмою «Безпека інформаційних комунікаційних систем» / упоряд. Г. З. Халімов. – Харків : ХНУРЕ, 2019. – 207 с.
33. Корнієнко Б. Я. Захист інформації в комп'ютерних системах та мережах (модульні технології навчання) / Б. Я. Корнієнко, М. М. Фомін, Л. М. Щербак. – Київ : НАУ, 2004. – 107 с.
34. Косогов О. М. Пріоритетні напрямки державної політики щодо забезпечення безпеки національного кіберпростору / О. М. Косогов // Збірник наукових праць Харківського

університету Повітряних сил. – 2014. – Вип. 3. – С. 127–130.
35. Кулаков Ю. О. Комп'ютерні мережі : навч. посібник / Ю. О. Кулаков, І. А. Жуков ; за ред. Ю. О. Кулакова. – Київ : НАУ, 2009. – 392 с.
36. Макаренко С. И. Информационная безопасность : учебное пособие для студентов вузов / С. И. Макаренко. – Ставрополь : СФ МГГУ им. М. А. Шолохова, 2009. – 372 с.
37. Маруних А. В. Захист інформації як основна складова економічної безпеки підприємства / А. В. Маруних // Управління розвитком. – 2014. – № 14. – С. 130–132.
38. Нємцева О. О. Поняття інформаційно-психологічного впливу / О. О. Нємцева // Соціальні комунікації: теорія і практика. – Київ : МЦД СК «Комтека», 2015. – С. 55–66.
39. Остапов С. Е. Технології захисту інформації: навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Харків : Вид-во ХНЕУ, 2013. – 476 с.
40. Офіційний сайт газети «Львівська пошта»: Небезпека соціальних мереж [Електронний ресурс]. – Режим доступу : http://www.lvivpost.net/suspilstvo/n/24110.
41. Павлов В. Г. Структурна організація та архітектура комп'ютерних систем : конспект лекцій / В. Г. Павлов, І. І. Михальчук. – Київ : НАУ, 2010. – 64 с.
42. Kali Linux. Тестирование на проникновение и безопасность / Парасрам Шива та ін. – Санкт-Петербург : Питер, 2020. – 448 с.
43. Петрик В. Небезпеки інформаційного простору для особистості / В. Петрик // Українські підручники. – [Електронний ресурс]. – Режим доступу : http: // pidruchniki.ws/18990227/politologiya/nebe zpeki_informatsiynogo_prostoru_dlya_osobistost.
44. Почепцов Г. Г. Інформаційна політика : навч. посіб. / Г. Г. Почепцов, С. А. Чукут. – 2-ге вид., стер. – Київ : Знання, 2008. – 663 с.

45. Пярин В. А. Безопасность электронного бизнеса / В. А. Пярин, А. С. Кузьмин, С. К. Смирнов. – Москва : Гелиос АРВ, 2002. – 256 с.
46. Рибальський О. В. Основи інформаційної безпеки та технічного захисту інформації : посібник для курсантів ВНЗ МВС України / О. В. Рибальський, В. Г. Хахановський, В. А. Кудінов. – Київ : Вид-во Національної академії внутріш. справ, 2012. – 104 с.
47. Світова гібридна війна: український фронт / за заг. ред. В. П. Горбуліна ; Національний інститут стратегічних досліджень. – Київ : НІСД, 2017. – 496 с.
48. Сериков А. Информационные технологии социального хакерства [Электронный ресурс]. – Режим доступа : http:// nefact.com/blog/metody-socialnoj-inzhenerii.
49. Соціальні мережі – реальні загрози віртуального світу. [Електронний ресурс]. – Режим доступу : http://ogo.ua/ articles/view/011–02–23/26490.htm.
50. Соціальна мережа (Інтернет) [Електронний ресурс]. – Режим доступу : https://uk.wikipedia.or/wiki/ Соціальна_мережа_(Інтернет).
51. Технические средства и методы защиты информации : учебное пособие для вузов / А. П. Зайцев и др. ; под ред. А. П. Зайцева и А. А. Шелупанова. – 4-е изд., испр. и доп. Москва : Горячая линия-Телеком, 2009. – 616 с.
52. Торокин А. А. Инженерно-техническая защита информации : учеб. пособие для студентов, обучающихся по специальностям в обл. информ. безопасности / А. А. Торокин. – Москва : Гелиос АРВ, 2005. – 960 с.
53. Філіпова Л. Я. Інформаційна парадигма соціальної комунікації (огляд наукових підходів і концепцій) / Л. Я. Філіпова // Вісник Харківської державної академії культури. – 2013. – Вип. 39. – С. 79–86.
54. Хорошко В. О. Основи інформаційної безпеки / В. О. Хорошко, В. С. Чередниченко, М. Є. Шелест ; за ред. проф. В. О. Хорошка. – Київ : ДУІКТ, 2008. – 186 с.

55. Шевченко Г. П. Духовна безпека: духовна культура і духовні цінності сучасної людини / Г. П. Шевченко // Духовність особистості: методологія, теорія і практика. – 2017. – Вип. 3. – С. 361–373.
56. Шпига П. С. Основні технології та закономірності інформаційної війни / П. С. Шпига, Р. М. Рудник // Проблеми міжнародних відносин. – 2014. – Вип. 8. – С. 326–339.
57. Юрчук В. Тенденції соціальної інженерії / В. Юрчук // Інформація, комунікація, суспільство : матеріали І Міжнародної наукової конференції ІКС–2012, 25–28 квітня 2012 року / Національний університет «Львівська політехніка». – Львів : Видавництво Львівської політехніки, 2021. – С. 128–129.
58. Яковенко В. С. Консолідація даних у бізнес-аналізі діяльності підприємств / В. С. Яковенко, Н. В. Зайцева // Глобальні та національні проблеми економіки. – 2015. – № 8. – С. 1222–1227.
59. Ясенев В. Н. Информационная безопасность в экономических системах : учеб. пособ. [Электронный ресурс] / В. Н. Ясенев. – Нижний Новгород : Изд-во ННГУ, 2006. – Режим доступа : http://ebib.pp.ua/informatsionnaya-bezopasnost-ekonomicheskih88.html.
60. Porter B. Principles of External Auditing / B. Porter, D. Hatherly, Jon Simon. – 3rd edition. – Wiley, 2008. – 816 p.

Навчальне видання

Кушнерьов Олександр Сергійович

БЕЗПЕКА ІНФОРМАЦІЇ

Конспект лекцій
для студентів усіх спеціальностей
денної форми навчання

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

Підписано до друку 27.10.2021, поз. 129.
Формат 60×84/16. Ум. друк. арк. 5,81. Обл.-вид. арк. 5,57. 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.