4. Baset S., Schulzrinne H. An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol. Department of Computer Science Columbia University, New York 2004.

5. Does Skype use encryption? [Електронний ресурс]. URL: https://support.Skype.com/en/faq/FA31/does-Skype-use-encryption?q=security (дата звернення: 01.12.2021).

6. LoopbackAudioDriver. [Електронний ресурс] URL: https://github.com/02strich/LoopbackAudioDriver (дата звернення: 01.12.2021).

7. Microsoft Virtual Audio Device Driver Sample. [Електронний ресурс] URL: https://code.msdn.microsoft.com/windowshardware/virtual-audio-device-3d4e6150 (дата звернення: 01.12.2021).

УДК 004.056.53

С.І. Войцех[1], О.Є. Веріго[1]
[1]Національний технічний університет «Дніпровська політехніка», Дніпро, Україна

ПРОТИДІЯ АТАКАМ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

Анотація. Розглянуті атаки соціальної інженерії які зростають за інтенсивністю та кількістю і спричиняють фінансові та іміджеві збитки користувачам і організаціям.

***Ключові слова**: політика безпеки підприємств, атаки соціальної інженерії.*

Вступ. Досягнення цифрових технологій зробили комунікацію між людьми доступною та простішою. Але через це особиста та конфіденційна інформація може бути доступною в Інтернеті через соціальні мережі та онлайн-сервіси, які не мають чітких алгоритмів та методів захисту цієї інформації. Соціальна інженерія є однією з найбільших інформаційних проблем стосовно безпеки у мережі, оскільки використовує природну схильність людини до довіри. Атаки соціальної інженерії спрямовані на введення в оману осіб для виконання дій, які приносять зловмисникам користь, надання їм конфіденційних даних, наприклад, медичних записів, паролів або ж банківських даних жертв їх атак.

Основний матеріал. Атаки соціальної інженерії розповсюджуються в сучасних мережах і є слабким місцем кіберзахисту підприємств та людей. Вони спрямовані на маніпулювання людьми і підприємствами з метою розголошування конфіденційних даних в інтересах кіберзлочинців. Соціальна інженерія ставить під загрозу безпеку усіх мереж, незалежно від надійності брандмауерів, методів криптографії, систем виявлення вторгнень і антивірусного програмного забезпечення [1]. Люди більше довіряють іншим людям, в порівнянні з комп'ютерами або технологіями, тому саме людина є

найслабкішою ланкою в ланцюзі безпеки на даний момент. Шкідлива діяльність, здійснювана через комунікаційну взаємодію, психологічно впливає на людину таким чином, що вона може розголосити конфіденційну інформацію або порушити існуючі процедури безпеки. Саме завдяки такому впливу через взаємодію між людьми, атаки соціальної інженерії є складно контрольованими, що погрожують усім системам і мережам. За допомогою програмних або апаратних рішень запобігти цим атакам неможливо, доки користувачі не будуть навчені протидіяти їм самостійно. Кіберзлочинці обирають такі атаки, у випадках, коли немає можливості зламати систему захисту через відсутність у ній технічних вразливостей.

В наш час компанії інвестують великі суми грошей і ресурсів для створення ефективних методів протидії атакам соціальної інженерії. Однак існуючі методи виявлення таких атак мають фундаментальні обмеження через неефективність контрзаходів в умовах постійно зростаючої кількості атак соціальної інженерії [2]. Технологічні методи також обмежені, оскільки технологічні вразливості можуть бути використані у поєднанні з атаками соціальної інженерії. Соціальні інженери стають все більш кваліфікованими, а атаки соціальної інженерії – менш очевидними. Це обумовлює велику потребу в ефективних методах виявлення, протидії таким атакам та мінімізації втрат від них.

Висновок. На жаль, атаки соціальної інженерії неможливо зупинити лише за допомогою технологій та надійної системи безпеки. Соціальні інженери можуть легко обійти такі комплексні системи захисту завдяки використанню фізіологічних вразливостей та психології людини. Атаки соціальної інженерії зростають за інтенсивністю та кількістю і спричиняють фінансові та іміджеві збитки користувачам і організаціям. Саме тому наразі є потреба в розробці нових ефективних методів протидії соціальним інженерам на різних рівнях, а саме підвищенню особистої відповідальності людей, вдосконаленню політик безпеки підприємств, а на рівні держави – розробці нових стандартів, законодавчих актів, які би чітко визначали відповідальність за злочини у цій сфері.

ПЕРЕЛІК ПОСИЛАНЬ

1. Alksnis G. Applied Computer Systems / G. Alksnis, J. Purins. // Riga Technical University. – 2017. – С. 38–45.

2. Киберугроза №1 [Електронний ресурс] – Режим доступу до ресурсу: https://www.securitylab.ru/analytics/500877.php.