Захист листів, поштових серверів і програм повинен відповідати ступеню важливості інформації, яка передається по мережі. Тобто, має здійснюватися централізоване управління сервісами електронної пошти. Повинна бути розроблена політика, в якій вказувався б потрібний рівень захисту. Для вирішення задач із забезпечення безпеки інформації, що надсилається через електрону пошту в усьому світі все активніше застосовуються технології криптографічного захисту з використанням відкритих ключів.

Список літературних джерел.

5. Волокита А., Мухін В., Стешин В..Специфіка інформаційних систем на основі технології cloud computing. URL: http://archive.nbuv.gov.ua/ portal/natural/vcndtu/ 2011_53/29.htm.
6. Інформаційна безпека при роботі у мережі Інтернет. URL: https://khm.gov.ua/uk/content/informaciyna-bezpeka-pry-roboti-u-merezhi-internet.
7. Гутман Б., Бегвілл Р. Політика безпеки при роботі в Інтернеті. URL: http://citforum.ru/internet/security_guide/glava8.shtml#8_7.

УДК 316.772.5:[004.056:351.86](043.2)

Македонський Б. О. студент 3 курсу спеціальності 125 «Кібербезпека»
Зелінська О.В. доцент, доцент кафедри інформаційних технологій

СОЦІАЛЬНИЙ ФАКТОР У ПРОБЛЕМІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ І КІБЕРБЕЗПЕКИ

Донецький національний університет імені Василя Стуса, м. Вінниця

Одним із основних методів протизаконного отримання інформації є соціальна інженерія. Соціальна інженерія – метод отримання необхідного доступу до інформації, що ґрунтується на особливостях психології людей. Основною метою соціальної інженерії є отримання доступу до конфіденційної інформації, паролів, банківських даних та інших захищених систем. Хоча термін соціальної інженерії виник недавно, такий спосіб отримання інформації використовується досить довго [1]. Кожен із нас стикається з таким майже щомісяця, коли через телефонні дзвінки повідомляють, що із вашої картки списуються грошові суми і просять продиктувати данні картки. Це підтверджує, що саме ви є її власником і блокує рахунок. І все, усі данні уже відправлені зловмисникам, особисто власником карти. Їм залишається лише забрати гроші жертви. Це один із найпримітивніших методів використання соціальної інженерії. Для такого не потрібні ніякі технічні знання, знання програмування, потрібно лише знати психологію людини, і вміти правильно говорити.

Набагато важче викрасти інформацію, уже у декількох людей, або у великої компанії зі своєю структурою і налагодженою системою безпеки. Так, але багато чого залежить саме від людей, не дарма кажуть, що людина є найслабшою ланкою системи безпеки. Прикладом може бути крадіжка у компанії The Ubiquiti Networks 40 мільйонів доларів у 2015 році. Ніхто не зламував операційні системи та не крав дані, тому що правила безпеки порушили самі працівники. Шахраї надіслали електронного листа від імені топ-менеджера компанії та попросили, щоб фінансисти перевели велику суму грошей на вказаний банківський рахунок [2]. Це лише один із прикладів, коли таким чином викрадають інформацію. Також гарним прикладом соціальної інженерії є фільм «Хто я» (Who am I).

Технічного захисту від подібних атак немає, тому потрібно працювати з людьми.

Потрібно навчитись виконувати певні дії:

- **Перевіряти джерело** (замисліться на хвилину про те, звідки надходить повідомлення, не довіряйте йому. Перевірити джерело неважко. Наприклад, подивитися на заголовок електронного листа та порівняти його з іншими листами того ж відправника. Перевірте, куди ведуть посилання, підроблені гіперпосилання легко виявити, просто навівши на них курсор (тільки не натискайте!)).
- **Що їм відомо?** (Чи знає той, хто вам дзвонить чи пише, всю відповідну інформацію – наприклад, ваше повне ім'я? Співробітник банку повинен мати перед очима всі ваші дані і обов'язково запитає кодове слово, перш ніж дозволить вам вносити зміни в свій рахунок).
- **Зупиніться та подумайте** (Соціальні інженери часто використовують ілюзію терміновості для того, щоб жертва не замислювалася про те, що відбувається. Усього хвилина роздумів може допомогти вам виявити та запобігти атаці).
- **Вимагайте дані, що засвідчують особу** (Соціальному інженеру найпростіше проникнути в будівлю, що охороняється, несучи в руках коробку або стос папок. Хтось обов'язково притримає для нього двері. Не потрібно вірити такому, завжди вимагайте посвідчення особи) [3].

Список літературних джерел:

1. Социальная инженерия – как не стать жертвой URL: https://efsol.ru/articles/social-engineering.html (Дата звернення: 20.11.2021)
2. Осторожно, это ловушка: что такое социальная инженерия URL: https://www.reg.ru/blog/chto-takoe-sotsialnaya-inzheneriya/ (Дата звернення: 20.11.2021)
3. Как избежать атаки с использованием социальной инженерии URL: ttps://www.kaspersky.ru/resource-center/threats/how-to-avoid-social-engineering-attacks (Дата звернення: 20.11.2021)