кібервійни, ролі кіберфронту в активних бойових діях та значення мобілізаційного потенціалу кібер фахівців в обороні держави тощо.

Список використаних джерел:

1. Richard A. Clarke and Robert K. Knake»Cyber War: The Next Threat to National Security and What to Do About It» (Harper Collins 2010). 2011. 320 p.
2. Мережко А. А. Конвенция о запрещении использования кибевойны в глобальной информационной сети информационных и вычислительных ресурсов (Интернете). Політичний менеджмент. URL: https://web.archive.org/web/20111007185753/http://www.politik.org.ua/vid/publcontent.php3?y=7&p=57.

ЛЮДСЬКИЙ ФАКТОР ЯК ОДИН ІЗ ВИДІВ ВРАЗЛИВОСТЕЙ В КІБЕРБЕЗПЕЦІ

Кравцов О.О.

студент 1-го курсу магістратури
факультету кібербезпеки та інформаційних технологій
Національного університету «Одеська юридична академія»

Питання про захист інформаційних інфраструктур, є одним з важливих питань для вирішення, як цивільними підприємствами, так і державою в цілому.

Один із аспектів надання якісного захисту інформаційній інфраструктурі являється протистояння внутрішнім загрозам. Будь-яка інформаційна інфраструктура, яка навіть має найновіші програмно-технічні засоби захисту, все ще опрацьовується людиною, що дає злочинцям, дуже велику вразливість, яку вони можуть використовувати для своїх цілей через соціальну інженерію.

Соціальна інженерія – це термін, який використовується для широкого спектру шкідливих дій, що здійснюються через взаємодію людей. Він використовує психологічні маніпуляції, щоб обманом змусити користувачів зробити помилки безпеки або роздати конфіденційну інформацію[1].

Такі вразливості можливо віднести до внутрішніх загроз до інформаційної інфраструктури. Внутрішні загрози – це загрози, що виникають через користувачів із законним доступом до інформаційної інфраструктури.

Такі користувачі використовують цей доступ зловмисно чи ненавмисно для заподіяння шкоди бізнесу. Внутрішні загрози не обов'язково трапляються через працівників підприємства, вони також можуть трапитися через колишніх співробітників, підрядників або партнерів, які мають доступ до систем або даних організації.

Можна виділити 4 внутрішні загрози:

1) Пішаки – це працівники, які маніпулюють зловмисною діяльністю, часто ненавмисно, за допомогою фішингу або соціальної інженерії. Будь то несвідомий працівник, який завантажує зловмисне на свою робочу станцію, або

користувач, який розкриває облікові дані третій стороні, що видає себе за службовця довідкової служби. Одним із прикладів є мережа Ubiquiti Networks, яка була атакована за допомогою фішингу. Електронні листи від вищих керівників змушували працівників перерахувати десятки мільйонів доларів на банківський рахунок дочірньої компанії, зареєстрованої в Гонконзі. Тоді співробітники не знали, що електронні листи підроблені, а банківський рахунок контролюється шахраями.

2) Гуфи – не діють зі зловмисними намірами, а навмисно завдають шкоди. Гуфи – це неосвічені або самовпевнені користувачі, які вважають, що вони звільнені від політики безпеки, незалежно від компетентності. У 95% організацій є працівники, які активно намагаються обійти контроль безпеки, і майже 90% внутрішніх атак спричинені недосвідченими користувачами, які не знають якої шкоди вони можуть завдати своїми діями. Прикладом махінації може бути користувач, який зберігає незашифровану особисту інформацію в обліковому записі хмарного сховища для зручного доступу на своїх пристроях, незважаючи на те, що це суперечить політиці безпеки.

3) Співучасники – це користувачі, які співпрацюють із третьою стороною, часто конкурентами. Такі користувачі використовують їхній доступ таким чином, що навмисно завдають шкоди. Співучасники, як правило, використовують свій доступ для викрадення інтелектуальної власності та інформації про клієнтів або для порушення нормальної ділової діяльності.

4) Самотні вовки повністю незалежні і діють зловмисно без зовнішнього впливу чи маніпуляцій. Такі суб'єкти особливо небезпечні, коли мають підвищений рівень привілеїв, таких як системні адміністратори або адміністратори баз даних. Класичним прикладом самотнього вовка є Едвард Сноуден, який використовував свій доступ до секретних систем для витоку інформації про кібершпигунство в Агентстві національної безпеки США [2].

Список використаних джерел:

1. Social Engineering: URL: https://www.imperva.com/learn/application-security/social-engineering-attack/
2. Andrea GilData: Security – Confidentiality, Integrity & Availability. kVA by UL. URL: https://cutt.ly/4bq5U4G

Науковий керівник: доцент Лобода Ю.Г.