6. Агресор поширює різні чутки не лише про бійців, а й про військово-політичне керівництво. Довіряти ворогу не можна.
7. Інформація на приватних акаунтах може не відповідати дійсності. Не діліться нею.
8. Агресор поширюватиме наклепи та «зраду» через свої офіційні чи підконтрольні канали. Перевіряйте патріотичні на вигляд, але сумнівні повідомлення та заклики.
9. Зберігайте єдність та підтримуйте одне одного
10. Якщо перервався Інтернет-зв'язок або сторінки державних органів були зламані, звертайтесь до Суспільного мовлення. Якщо не працює телебачення – вмикайте абонентську радіоточку.

На останок варто наголосити, що наш мозок потребує перепочинку. Тому не варто забувати хоча б два-три рази на день давати своєму фізичному та емоційному станові відпочивати від новин. І саме головне, не поширюйте фейки, не довіряйте сумнівним джерелам таким чином ви допомагаєте здолати ворога на інфораційному полі бою.

Список використаних джерел

1. *Халамендик В.Б. Інформаційна гігієна к фактор збереження психічного здоров'я людини. Гуманітарний вісник Запорізької державної інженерної академії. Київ, 2016. 9 с.*
2. *54% українців не дотримуються інформаційної гігієни в Facebook – дослідження. URL: https://cutt.ly/dN5oqGv (дата звернення:08.11.2022)*
3. *Інформаційна гігієна, або як Facebook став джерелом №1 брехні для українців. URL: https://cutt.ly/dN5odWf (дата звернення:08.11.2022)*
4. *Інформаційна гігієна або як розпізнати неправдиві новини в інтернеті? Видавництво «Простір», Львів, 2019. 7 с.*
5. *У разі надзвичайної ситуації або війни. Міністерство культури та інформаційної політики України. Київ, 2022. 14 с.*

УДК 004.056:[164:658.8](043.2)

Македонський Б. О., здобувач 4 курсу спеціальності 125 «Кібербезпека»
Потапова Н. А., к.е.н., доцент, доцент кафедри інформаційних технологій

ПРОБЛЕМА КІБЕРБЕЗПЕКИ У СФЕРІ ЛОГІСТИКИ

Донецький національний університет імені Василя Стуса, м. Вінниця

З розвитком інформаційних технологій розвиваються і методи кібератак на компанії в тому числі і логістичні. Не всі хакери мають на меті отримати користь або матеріальні ресурси в результаті інциденту, багато з них проводять атаки з

однією метою – перевірити свої можливості. Що може бути гірше ніж атака з метою наживи. Саме це і потенційні втрати від можливих інцидентів потребують покращення інформаційної безпеки в сфері логістики.

Слід зауважити, що логістика один із тих напрямів діяльності, робота в межах якого здатна генерувати синергетичний ефект витрат на засадах поєднання використання елементів менеджменту та інформаційних технологій. На сьогодні, більшість логістичних ланцюгів представлені у вигляді віртуального цифрового образу, що супроводжує матеріальний потік ресурсів. Тому, саме логістичні ланцюги нас сьогодні мають бути кіберзахищеними, а їх кібербезпека повинна стати невід'ємною складовою інформаційної політики.

Нещодавно Центр аналізу загроз компанії Microsoft виявив запуск програм вимагачів на логістичні компанії із Польщі та України. Вторгнення було виявлено 11 жовтня, але скільки часу вірус був у системі та на скільки комп'ютерів перейшов поки не відомо, але збитки були задані не малі[1]

З втратами у 300 мільйонів доларів США, у 2017 році, було запущено атаку програм-вимагачів на ПК компанії AP Moller – Maersk, однієї із найбільших логістичних компаній світу, що також вплинуло на світову логістику. Зупинилось 76 портових терміналів по всьому світу, хоча відновлення було швидким але навіть це змусило і інші компанії по всьому світу зупинити перевезення.[2] Це була атака світового масштабу, але навіть такі збитки не змусили компанії збільшити фінансування сектору кібербезпеки аби уникати таких витрат.

За результатами опитування The State of Logistics Technology Report: 2019 компанії Eyefortransport результати не втішні:

- Тільки 35% постачальників рішень / послуг з перевезення вантажів мають у своєму штаті керівника з інформаційної безпеки (Chief Information Security Officer – CISO);
- Тільки 43% судноплавних компаній мають CISO;
- Тільки 21% компаній, які надають логістичні послуги, вважають, що їм потрібен CISO.

Цифри малі як для світових компаній з великим капіталом. Хоча компанії почали більше вкладати в інформаційну грамотність своїх співробітників, приблизно 55% респондентів відповіли що вони погано підготовлені до виявлення та усунення потенційних загроз кібербезпеки під час організації міжнародних вантажних перевезень. Підводячи підсумки, дослідники винесли рішуче звинувачення: «Індустрія логістики все ще не розглядає безпеку як основну частину ділових операцій». За оцінками мультинаціональної консалтинг і аутсорсинг компанії Accenture, число кібератак в компаніях в США зростає приблизно на 27% в рік. Невеликі компанії є особливо уразливими. У звіті про розслідування порушень даних, опублікованому Verizon в 2017 році, встановлено, що 61% жертв – це компанії, в яких працює менше 1000 чоловік. [3] Саме тому компаніям потрібно відповідальніше ставитись до своєї інформаційної безпеки та кібер-грамотності працівників.

Список використаних джерел

1.New "Prestige" ransomware impacts organizations in Ukraine and Poland, 2022, URL: https://www.microsoft.com/en-us/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-in-ukraine-and-poland/ (Дата звернення 03.11.2022)
2.Maersk Line: Surviving from a cyber attack, 2018 URL: https://safety4sea.com/cm-maersk-line-surviving-from-a-cyber-attack/ (Дата звернення 03.11.2022)
3.The problem of cybersecurity in the field of logistics, URL: https://dsl-ua.com/en/2019/10/10/problema-kiberbezpeki-u-sferi-logistiki/ (Дата звернення 03.11.2022)
4.Потапова Н.А. Логістика онлайн-торгівлі в контексті проявів глобалізації цифрової економіки. Економіка. Фінанси. Менеджмент: актуальні питання науки і практики. № 3. 2019. С. 62 – 77.

УДК 519.87:343.98

Матвійчук Р.Д. здобувачка
Січко Т.В., к.т.н., доцент, доцент
кафедри інформаційних технологій

ЗАСТОСУВАННЯ МАТЕМАТИЧНОГО МОДЕЛЮВАННЯ У КРИМІНАЛІСТИЦІ

Донецький національний університет імені Василя Стуса, Вінниця

Математичне моделювання у криміналістиці використовується давно. Перший крок було зроблено французьким кримінологом А. Бертільоном завдяки апарату метрології (науки про виміри) та теорії ймовірностей. У подальшому математичне моделювання було корисним при аналізі доказів, фактів, визначення обставин злочину. Прикладом фізичного моделювання у слідстві є відтворення обставин та подій, у процесі якого не лише підтверджується якась гіпотеза, але й виробляється нова. Прикладом аналітичного моделювання є опис процесу за допомогою спеціальних диференціальних рівнянь тощо [1].

Наразі багато проблем криміналістики відійшли на задній план завдяки інноваціям, а саме впровадженні технологій розпізнавання відбитків пальців та обличь. Відомо, що візерунки людського пальця для кожного особливі, але, коли це з'ясувалося вперше, то дало неймовірний поштовх для криміналістики. Подальші наукові дослідження запропонували різні алгоритми: HMFA (Hybrid Mutation-Base Firefly Algorithm) (алгоритм розпізнавання відбитків пальців із розподілом гістограми та медіанною фільтрацією), алгоритм на основі фільтрів Гауса для мінімізації шуму на зображенні, що підлягає обробці. Інші дослідження були зосереджені на вдосконаленні швидкості фази порівняння відбитків пальців для прискорення автентифікації [2].