Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(освітній рівень)

на тему: *«Дослідження вразливостей нейроінтерфейсів»*

Виконав: студент (ка) *VI* курсу, групи *СБм-61*
Спеціальності:
125 «Кібербезпека»
(шифр і назва напряму підготовки, спеціальності)
Мокрицький М.В.
підпис (прізвище та ініціали)

Керівник *Скоренький Ю.Л.*
підпис (прізвище та ініціали)

Нормоконтроль
підпис (прізвище та ініціали)

Рецензент
підпис (прізвище та ініціали)

м. Тернопіль – 2022

АНОТАЦІЯ

Дослідження вразливостей нейроінтерфейсів // Кваліфікаційна робота освітньоого рівня «Магістр» // Мокрицький Микола Васильович // Тернопільський національний технічний університет, факультет комп`ютерно-інформаційних систем і програмної інженерії , кафедра кібербезпеки, група СБм61 // Тернопіль, 2022. // С. – 56, рис. – 14, та додат. – 3, бібліогр. – 19.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА, НЕЙРОІНТЕРФЕЙС, ВРАЗЛИВОСТІ.

Метою кваліфікаційної роботи є дослідження ризиків при використанні нейроінтерфейсів у сучасному світі.

В процесі дослідження використано загальнонаукові методи пізнання: порівняння, системний аналіз, моделювання. Також були проведені експериментальні вимірювання та здійснено математичне опрацювання з метою отримання кількісної оцінки стану інформаційної безпеки.

Розвиток мікроелектроніки та інформаційних технологій забезпечив умови для створення інерфейсів для безпосередньої взаємодії між нервовою системою людини та комп’ютерними системами. Питання безпеки застосування нейроінтерфейсів донедавна не досліджувалися через їх малу поширеність та специфіку застосування. На сьогодні, поява відносно недорогих моделей китайського виробництва та відсутність стандартизації роблять актуальними питання безпеки конфіденційної інформації, витік якої може трапитися при використанні нейроінтерфейсів. Принцип дії нейроінтерфейсів пов’язаний з генеруванням сигналів у мозку. Згенеровані дані відображають намір користувача керування зовнішнім пристроєм. Електромагнітні хвилі, утворені електричними сигналами у мозку, реєструються електродами за допомогою різноманітних технологій, таких як

електроенцефалографія або функціональна магнітно-резонансна томографія. Неопрацьовані аналогові сигнали піддаються аналого-цифровому перетворенню, щоб забезпечити подальшу обробку даних. Однією з головних цілей цього етапу є максимізація відношення сигнал/шум, щоб виміряти вихідний сигнал в якомога точнішій формі. Обробка цифрових даних необхідна для декодування запланованої дії користувача. Після цього різні моделі (наприклад, класифікатори, предиктори, регресори) або системи на основі правил визначають заплановану дію. Програми можуть надсилати необов'язковий зворотний зв'язок користувачеві, щоб генерувати сигнали мозку та, отже, нові ітерації циклу. На кожному з етапів генерується інформація, яка відображає індивідуальні особливості користувача та є конфіденційною. Програмні компоненти нейроінтерфейсів можуть мати вразливості та зазнавати атак зловмисників.

В даній роботі представлено аналіз особливостей нейроінтерфейсів та відповідних вразливостей, які можуть суттєво вплинути на функціонування цих систем.

ANNOTATION

Study of brain-computer interfaces vulnerabilities // Qualification paper of the educational level “Master” // Mykola Mokrytskyi // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cyber Security, SBm-61 group // Ternopil, 2022 // P. 56, fig. - 14, annexes - 3, references - 19.

The purpose of the qualification work is the study of risks when using neurointerfaces in the modern world.

In the research process, general scientific methods of cognition were used: comparison, system analysis, modeling. Experimental measurements were also carried out and mathematical processing was carried out in order to obtain a quantitative assessment of the state of information security.

Key words: INFORMATION SECURITY, BRAIN-COMPUTER INTERFACE, VULNERABILITY.

The development of microelectronics and information technologies provided the conditions for creating interfaces for direct interaction between the human nervous system and computer systems [1, 2]. Security issues of the use of neurointerfaces were not investigated until recently due to their low prevalence and specificity of use. Today, the emergence of relatively inexpensive Chinese-made models and the lack of standardization make the issue of the security of confidential information, which is leaked, relevant can happen when using neurointerfaces. The principle of operation of neurointerfaces is related to the generation of signals in the brain. The generated data reflects the user's intent to control the external device. Electromagnetic waves generated by electrical signals in the brain are recorded by electrodes using a variety of technologies, such as electroencephalography or functional magnetic resonance imaging. Raw analog signals undergo analog-to-digital conversion to allow further data processing. One

of the main goals of this step is to maximize the signal-to-noise ratio in order to measure the output signal as accurately as possible. Digital data processing is necessary to decode the user's intended action. Various models (eg, classifiers, predictors, regressors) or rule-based systems then determine the intended action. Programs can send optional feedback to the user to generate brain signals and thus new loop iterations. At each of the stages, information is generated that reflects the individual characteristics of the user and is confidential. Software components of neurointerfaces can have vulnerabilities and be subject to attackers' attacks.

This work presents an analysis of the features of neurointerfaces and the corresponding vulnerabilities that can significantly affect the functioning of these systems.

.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

BCI – Brain-Computer Interface (нейроінтерфейс)

IoT – Internet of Things (шнтернет речей)

EEG – electroencephalogram (електроенцефалограма)

fMRI – functional magnetic resonance imaging (функціональна магнітно-резонансна томографія)

MEG – magneto-encephalography (магнітоенцефалографія)

NIRS – near-infrared spectroscopy (спектроскопія ближнього інфрачервоного діапазону)

ВСТУП

Розвиток електроніки та комунікаційних технологій дозволяє прогнозувати близьке впровадження нейроінтерфейсів [1, 2] не лише в медичній галузі, а також в освіті, різноманітних галузях виробництва, транспорту, креативній індустрії.

Нейроінтерфейси (Brain-Computer Interface або BCI) — це технологія, що швидко розвивається, яка створює прямий канал між мозком людини та комп'ютером, що дозволяє сигналам від мозку спрямовувати певну зовнішню діяльність. Принцип дії нейроінтерфейсів пов'язаний з генеруванням сигналів у мозку. Згенеровані дані відображають намір користувача керування зовнішнім пристроєм. Електромагнітні хвилі, утворені електричними сигналами у мозку, реєструються електродами за допомогою різноманітних технологій, таких як електроенцефалографія або функціональна магнітно-резонансна томографія. Неопрацьовані аналогові сигнали піддаються аналого-цифровому перетворенню, щоб забезпечити подальшу обробку даних. Однією з головних цілей цього етапу є максимізація відношення сигнал/шум, щоб виміряти вихідний сигнал в якомога точнішій формі. Обробка цифрових даних необхідна для декодування запланованої дії користувача. Після цього різні моделі (наприклад, класифікатори, предиктори, регресори) або системи на основі правил визначають заплановану дію. Програми можуть надсилати необов'язковий зворотний зв'язок користувачеві, щоб генерувати сигнали мозку та, отже, нові ітерації циклу. На кожному з етапів генеруєтья інформація, яка відображає індивідуальні особливості користувача та є конфіденційною. Програмні компоненти нейроінтерфейсів можуть мати вразливості та зазнавати атак зловмисників.

Отже, метою роботи є аналіз вразливостей нейроінтерфейсів а також дослідження сучасних способів і засобів для мінімізації загроз безпеці нейроінтерфейсів

Для досягнення поставленої мети, необхідно виконати низку наступних задач:

- проаналізувати предметну область,
- з’ясувати типи та характерні особливості вразливостей нейроінтерфейсів,
- проаналізувати способи запобігання загрозам нейроінтерфейсів,
- дослідити роботу та спланувати заходи захисту для простого нейроінтерфейсу,
- зробити висновки щодо можливих шляхів забезпечення безпеки даних, які поширюються через нейроінтерфейси.

Об'єкт дослідження – процес влюдино-машинної взаємодії.

Предмет дослідження – вразливості нейроінтерфейсів.

Методи дослідження: загальнонаукові методи пізнання як порівняльний та системний аналіз, експериментальний метод

Наукова новизна. В роботі проведено аналіз вразливостей інтерфейсів взаємодії людини та комп’ютера з точки зору вразливостей, притаманних простим системам типу пристроїв інтернету речей.

Апробація результатів роботи. Окремі результати роботи доповідались на X науково-технічній конференції «Інформаційні моделі, системи та технології», Тернопіль, ТНТУ, 7 – 8 грудня 2022 р.

1 ОБЛАСТЬ ЗАСТОСУВАННЯ ТА ОСНОВИ РОБОТИ НЕЙРОІНТЕРФЕЙСІВ

Нейроінтерфейсом в загальному розумінні вважають систему [1, 3], яка приймає біосигнал, виміряний від людини і прогнозує (у режимі реального часу та на основі одноразового випробування) деякі абстрактні аспекти неврологічного стану, когнітивного стану, уваги чи наміру людини (див. рисунок 1.1).

Рисунок 1.1 – Перетворення сигналу мозкової активності нейроінтерфейсом [3].

1.1 Основні застосування та етапи роботи нейроінтерфейсів

Застосування інтерфейсу мозок-машина поширюється на численні й різноманітні галузі й не обмежується лише сферою медицини. Можна знайти і прогнозувати подальший розвиток таких застосувань як розумні середовища (будинок, кампус місто) та освіту [4], керування засобами доповненої реальності [5], ігри та розваги, інформаційні технології [6]. Наа сьогодні в галузі охорони здоров’я нейроінтерфейси вже використовують для виявлення та діагностики захворювань, а також реабілітації та відновлення після важлих хвороб та травм.

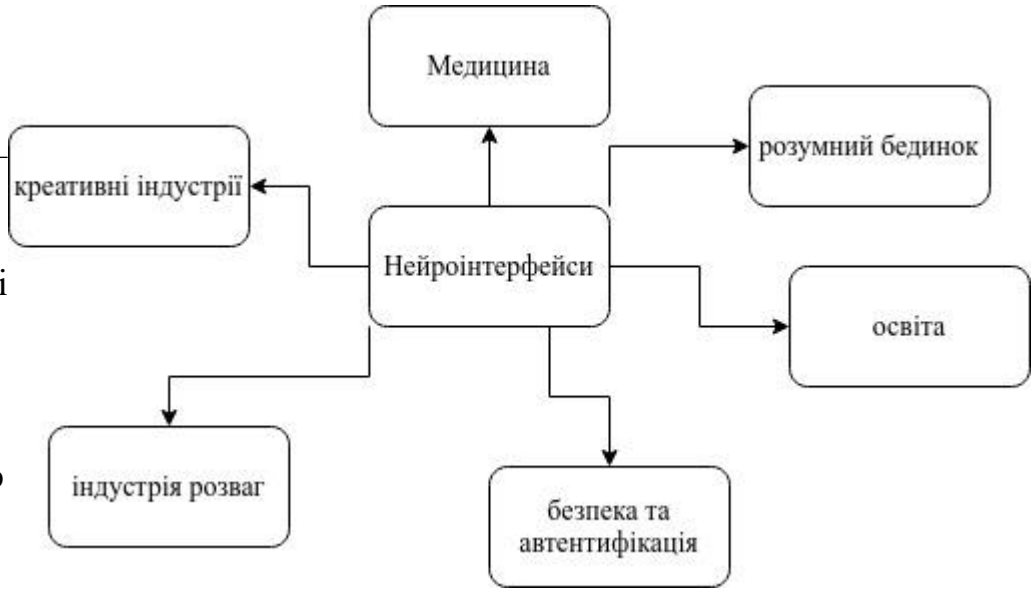

Рисунок 1.2 – Перспективні галузі застосування нейроінтерфейсів.

Інтерфейси, які безпосередньо перетворюють мозкову активність в потоки команд, мають перспективу також дати новий поштовх Інтернету речей, створюючи розумні середовища, такі як розумні будинки, транспортні засоби або робочі місця. Метою нейроінтерфейсу є виявлення та кількісна оцінка сигналів мозку, які вказують на наміри користувача, і перетворення цих функцій у режимі реального часу в команди пристрою, які виконують намір користувача. Для цього система має складатися з таких чотирьох компонентів:

1. Приймач сигналу
2. Модуль опрацювання сигналу
3. Формування керуючої команди
4. Пристрій виводу

Отримання сигналу – це процес вимірювання аналогового сигналу від мозку за допомогою різних конкретних датчиків. Отриманий сигнал потім посилюється та фільтрується, щоб видалити шум із сигналу. Нарешті, сигнал оцифровується за допомогою аналого-цифрового перетворювача і передається в блок обробки.

Опрацювання полягає в процесі вилучення унікальних характеристик із

отриманого сигналу. Ці функції повинні співвідноситися з намірами користувача та його індивідуальними особливостями.На цьому етапі індивідуальні особливості повинні відфільтровуватися системою, однак є загроза витоку конфіденційних даних про індивідуальні особлвості біологічного агента. Коли функція витягується та класифікується, вона пропускається через алгоритм перекладу функції. Основним завданням функції тут є перетворення отриманого сигналу у відповідну команду на вихідний пристрій. Вихід надається на певний пристрій виводу. Команди з алгоритму трансляції функцій керують зовнішнім пристроєм, забезпечуючи такі функції, як вибір літер, керування курсором, робота роботизованої руки тощо. Робота пристрою забезпечує зворотний зв'язок з користувачем, таким чином замикаючи контур керування.

1.2 Типи існуючих нейроінтерфейсів

Активний нейроінтерфейс отримує дані діяльності мозку, яка безпосередньо свідомо контролюється користувачем, незалежно від зовнішніх подій, для керування програмою. Реактивний нейроінтерфейс отримує свої результати від активності мозку, що виникає у відповідь на зовнішню стимуляцію, яка опосередковано модулюється користувачами для керування програмою. Пасивний або афективний тип отримує результати від спонтанної активності мозку без мети довільного контролю [8].

Інвазивні BCI

Інвазивний нейроінтерфейс потребує операції з імплантації електродів під шкіру голови для передачі сигналів мозку. Основна перевага полягає в тому, щоб забезпечити більш точне читання; однак його недолік включає побічні ефекти від операції. Після операції можуть утворитися рубцеві тканини, які можуть послабити сигнали мозку. Крім того, на думку деяких дослідників, після імплантації електродів організм може не сприймати електроди, що може спричинити медичні ускладнення.

Напівазивні BCI

Напівазивні або частково інвазивні пристрої BCI імплантуються всередину черепа, але розташовані поза межами мозку, а не всередині сірої речовини. Вони виробляють сигнали з кращою роздільною здатністю, ніж неінвазивні BCI, де кісткова тканина черепа відхиляє та деформує сигнали, і мають менший ризик утворення рубцевої тканини в мозку, ніж повністю інвазивні BCI.

Неінвазивні BCIs

Термін «неінвазивні інтерфейси мозок-комп'ютер» охоплює всю технологію, яка дозволяє стимулювати мозок-комп'ютер без необхідності проникати в нього. Більшість неінвазивних інтерфейсів мозок-комп'ютер покладаються на електроди, які розміщені на певних ділянках шкіри голови, щоб реєструвати мозкову активність. Серед основних технологій, які використовуються в процесі неінвазивних BCI, є електроенцефалограма (EEG), функціональна магнітно-резонансна томографія (фМРТ), магнітоенцефалографія (МЕГ), спектроскопія ближнього інфрачервоного діапазону (NIRS).

Методологія досліджень сигналів мозку базується на кількох критеріях [9], включаючи ризик, просторову роздільну здатність, часову роздільну здатність, співвідношення сигнал/шум, портативність, вартість і характеристику. Завдяки своїм перевагам, включаючи більш високу часову роздільну здатність, доступні ціни, зручну портативність і неінвазивність, ЕЕГ є найбільш широко використовуваним методом дослідження активності головного мозку. ЕЕГ контролює напругу, що виробляється через електричний струм у нейронах мозку. Електродами на шкірі голови тестують амплітуду сигналів ЕЕГ. Сигнали ЕЕГ мають погану роздільну здатність через обмежені електроди. Співвідношення сигнал/шум на ЕЕГ досить низьке через кількісні та емоційні причини. Фізичні причини включають навколишній шум, обструкцію кори та інших тканин кори головного мозку,

повторну нервову стимуляцію. У порівнянні з іншими мозковими імпульсами, ЕЕГ-гарнітури компактні та набагато більш доступні для більшості випадків. Сигнали ЕЕГ від будь-якого конкретного пристрою ЕЕГ містять різні частотні діапазони (альфа, бета, тета, гамма та тета), що не перекриваються, на основі надійного внутрішньосмугового зв'язку з чітким поведінковим станом.

• Дельта-ритм (0:5-4 Гц) лідирує під час глибокого сну при меншій свідомості.

• Тета-ритм (4-8 Гц) означає низьку свідомість у спокої.

• Альфа-сигнал (8-12 Гц) з'являється переважно в закритих і повністю спокійних очах, приводячи до звичайної свідомості.

• Бета-імпульс (12-30 Гц) є домінуючою частотою, коли очі відкриті та добре сприйнятливі. Бета-модель представляє майже всі щоденні завдання (їсти, рухатися, говорити).

Магнітоенцефалографія є неінвазивним методом аналізу функції нейронів мозку. MEG планує роботу мозку шляхом вимірювання магнітних полів, створюваних електричним струмом у мозку за допомогою обробки інформації. Створене магнітне поле порівняно слабке. Таким чином, MEG використовує чутливий магнітометр під назвою SQUID який встановлюються на шкіру голови для моніторингу активації нейронів (переважно тих, які знаходяться найближче до магнітометра). Подібно до магнітних полів, МЕГ має низку переваг, менше спотворень, ніж електричний струм, а також високу часову роздільну здатність і правильну просторову роздільну здатність, навіть ніж ЕЕГ. Технологія MEG є дуже дорогою.

Функціональна магнітно-резонансна томографія є неінвазивною технікою, яка використовується для вимірювання мінливості рівня кисню в крові через функцію мозку, забезпечує високу просторову роздільну здатність, що робить його придатним для визначення місцезнаходження активних ділянок мозку. Часова роздільна здатність фМРТ коливається

приблизно від 1 до 2 с. Також цей метод надає мало інформації про часову динаміку відповідей.

Великі надії пов’язують із розвитком медичної технології нейролінку (https://neuralink.com/approach/), яка є на даний час найбільш розвиненою, але недоступною незалежним дослідникам (див. рис. 1.3).

Рисунок 1.3 – Дослідний зразок нейроінтерфейсу neurolink.

Нейролінк є повністю імплантований, косметично невидимий інтерфейс мозок-комп’ютер, який дозволяє керувати комп’ютером або мобільним пристроєм. Нитки мікронного масштабу вставлені в ділянки мозку, які контролюють рух. Кожна нитка містить багато електродів і з’єднує їх з імплантатом. Коли через електрод пропускаються невеликі струми, електричне поле, що змінюється, спонукає найближчі нейрони запускати один або кілька потенціалів дії. Стимулюючи певні часові послідовності через багато електродів, можна створити моделі активності, які викликають бажане відчуття, наприклад відчуття предмета в руці або візуальне зображення. Електроди розміщують біля нейронів, щоб виявити потенціали дії. Запис від багатьох нейронів дозволяє декодувати інформацію, представлену цими клітинами. Цю інформацію потрібно декодувати, щоб

використовувати її для керування комп'ютером. Розроблено комп'ютерні алгоритми для керування віртуальною комп'ютерною мишею за допомогою активності сотень нейронів. Одна з проблем полягає в тому, щоб розробити адаптивні алгоритми, які зберігають надійну та стійку продуктивність, продовжуючи вдосконалюватися з часом. Обмін даними між імплантом та зовнішніми пристроями несе потенційну загрозу конфіденційності інформації, яка поширюється відкритими каналами.

1.3 Цикл обробки даних у системі з нейроінтерфейсом

На рис. 1.4 представлено загальне функціонування двонаправлених потоків інформації в системі з нейроінтерфейсом [1]. Потік за годинниковою стрілкою, позначений синьою стрілкою, представляє процес отримання нейронних даних, тоді як потік проти годинникової стрілки, представлений червоною стрілкою, моделює стимуляцію мозку.

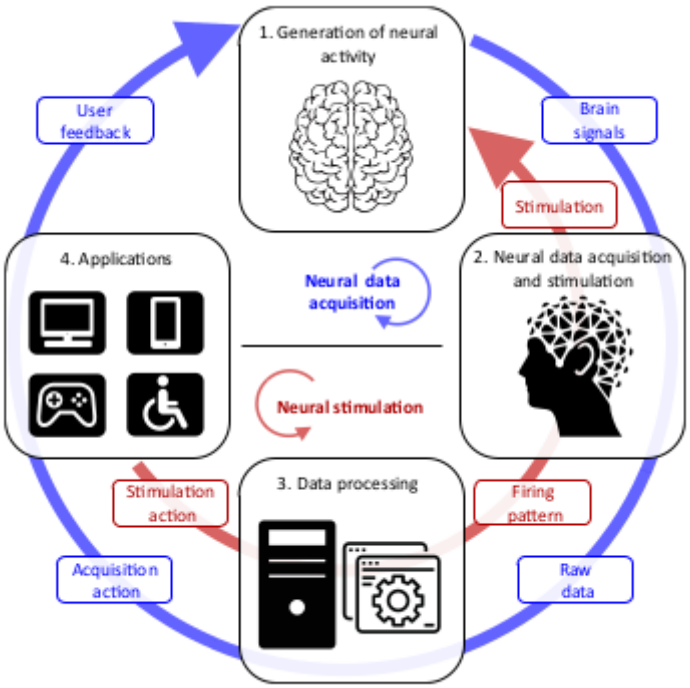

Рисунок 1.4 – Загальне функціонування двонаправлених потоків інформації в системі з нейроінтерфейсом [1]

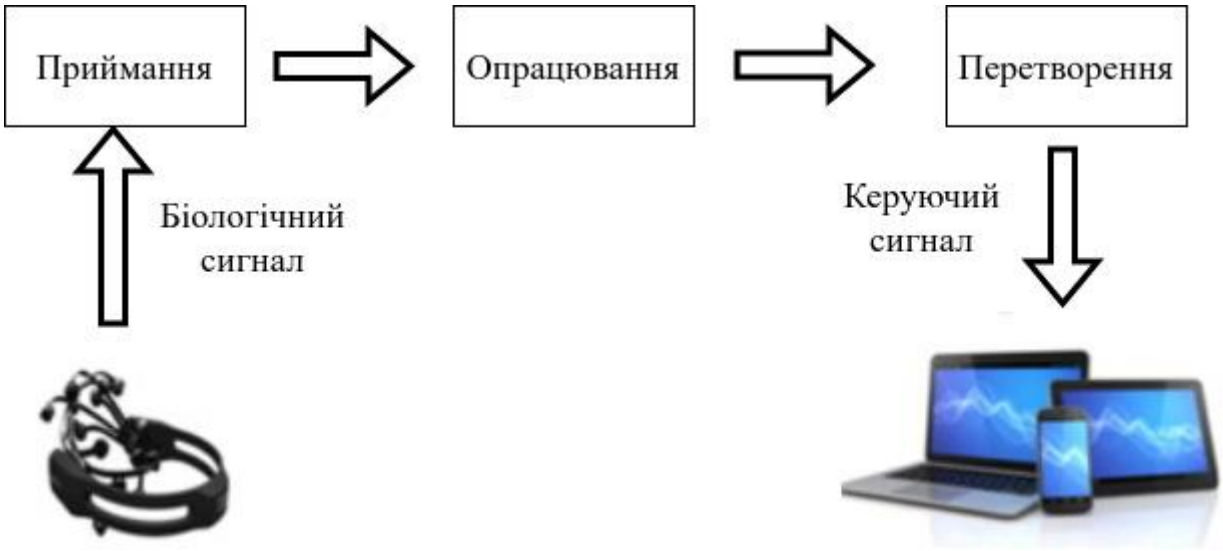

Рисунок 1.5 – Загальне функціонування двонаправлених потоків інформації в системі з нейроінтерфейсом

Опрацювання даних в системі інтерфейсу BCI відбуваєтьсяв кулька еткпів у різних пристроях, що висуває певні вимоги до захисту такої розподіленої кіберфізичної системи [11]. Активність нейронів перетворюється в сигнали, які можна обробити для виконання різних типів виведення.

1.4 Висновки до першого розділу

Принцип дії нейроінтерфейсів пов’язаний з генеруванням сигналів у мозку. Згенеровані дані відображають намір користувача керування зовнішнім пристроєм. Електромагнітні хвилі, утворені електричними сигналами у мозку, реєструються електродами за допомогою різноманітних технологій, таких як електроенцефалографія або функціональна магнітно-резонансна томографія. Неопрацьовані аналогові сигнали піддаються аналого-цифровому перетворенню, щоб забезпечити подальшу обробку даних. Однією з головних цілей цього етапу є максимізація відношення сигнал/шум, щоб виміряти вихідний сигнал в якомога точнішій формі. Обробка цифрових даних необхідна для декодування запланованої дії

користувача. Після цього різні моделі (наприклад, класифікатори, предиктори, регресори) або системи на основі правил визначають заплановану дію. Програми можуть надсилати необов’язковий зворотний зв’язок користувачеві, щоб генерувати сигнали мозку та, отже, нові ітерації циклу. На кожному з етапів генеруєтья інформація, яка відображає індивідуальні особливості користувача та є конфіденційною. Програмні компоненти нейроінтерфейсів можуть мати вразливості та зазнавати атак зловмисників.

2 ПРОБЛЕМИ БЕЗПЕКИ НЕЙРОІНТЕРФЕЙСІВ

2.1 Функції кібербезпеки та основні вразливості кіберфізичних систем

Кібербезпека та конфіденційність повинні бути реалізовані для захисту будь-якої інформаційної системи, включаючи відповідальні компоненти нейроінтерфейсів, описані в попередньому розділі. Щоб відповідати всім вимогам щодо кібербезпеки та конфіденційності, важливо дотримуватися комплексної структури, такої, як розроблена Національним інститутом стандартів і технологій (рис. 2.1). Ця структура складається з п'яти основних функцій, а саме ідентифікації, захисту, виявлення, реагування та відновлення [11].

Ідентифікація: її метою є отримати розуміня процесів та визначити ризики кібербезпеки . Це допомагає розвинути цілісне розуміння всіх аспектів, включаючи контекст, ресурси, пов’язані ризики кібербезпеки та керування ризиками.

Безпека: метою цієї функції є розробка та впровадження конкретних заходів безпеки, що допомагає мінімізувати вплив інцидентів шляхом контролю доступу, захисту даних та ін.

Функція виявлення реєструє виявлення та ідентифікує усі інциденти кібербезпеки. Це дозволяє своєчасно виявляти аномалії за допомогою постійного моніторингу.

Response: після виявлення будь-якого інциденту функція реагування (відповіді) здійснює заходи спрямовані на мінімізацію впливу інциденту кібербезпеки. Такими заходами є планування реагування, комунікаційні дії та аналіз інцидентів.

Відновлення: ця функція відповідає за розробку планів стійкості та своєчасне відновлення служб і функціональності, порушених інцидентами кібербезпеки.

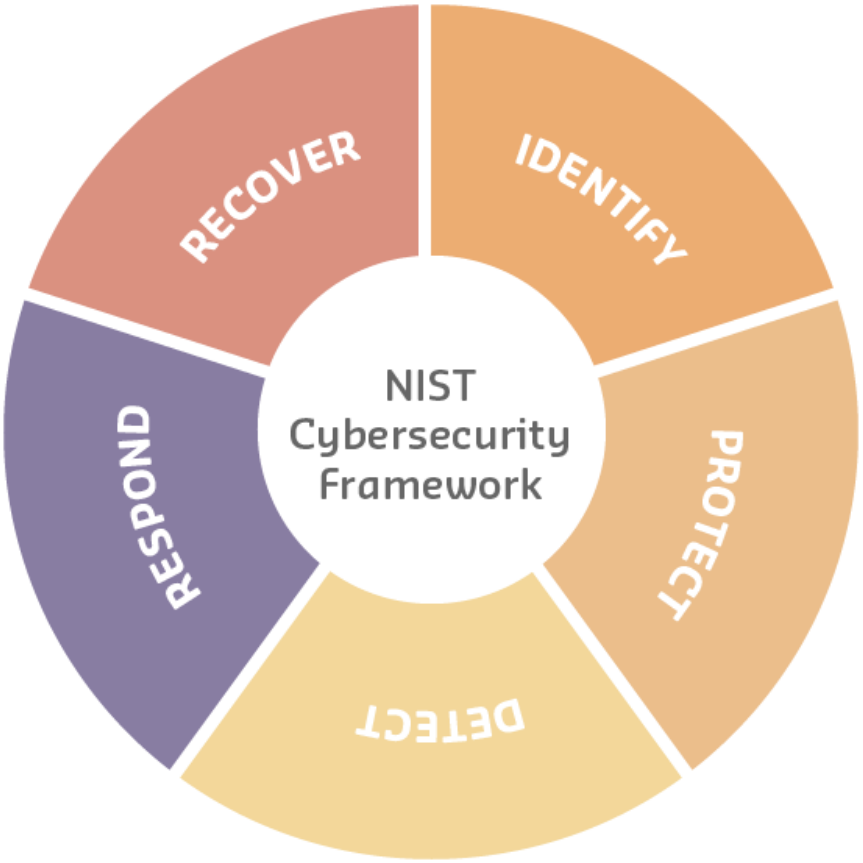

Рисунок 2.1 - Структура кібербезпеки, розроблена Національним інститутом стандартів і технологій .

Вразливість — це відома слабкість у програмному забезпеченні чи системах, якою може скористатися зловмисник. Оскільки ця проблема є відомою, на її основі можуть здійснбватися автоматизовані атаки на ресурс.

Ризик означає ймовірність втрати або пошкодженн даних, коли використана певна відома вразливість. Різні активи зловмисники по-різному оцінюють, тому ймовірність використання вразливостей буває різною.

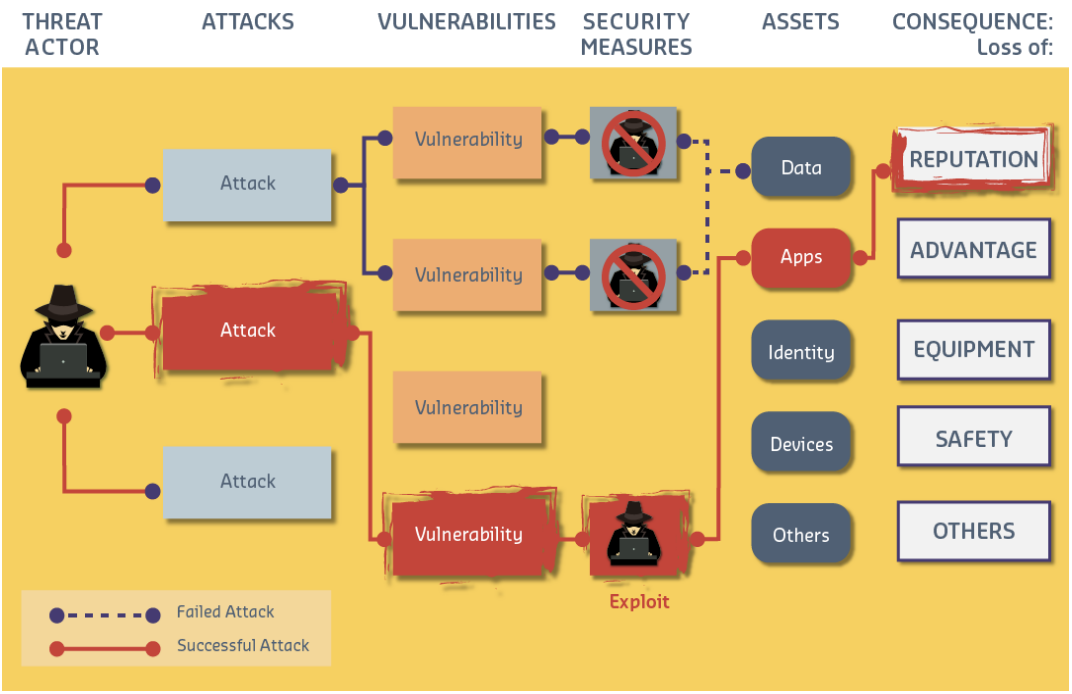

Рисунок 2.2 – Перебіг і наслідки атаки

Отже, з метою оцінки ризику необхідно провести ретельний аналіз інформації щодо загроз і вразливостей.

2.2 Розгортання нейроінтерфейсів та атаки на них

Існуючі розгортання розглядають ізольовані пристрої без стандартів для забезпечення сумісності з точки зору зв'язку та представлення даних. Це стосується комерційних брендів і пристроїв BCI, які були розроблені для вирішення конкретних проблем і несумісні між собою. Крім того, розгортання, що інтегрують зв'язок між кількома BCI, є спеціальними; тобто виробники проектують і впроваджують їх, враховуючи лише вимоги конкретного сценарію. У цьому контексті поточна тенденція BCI до таких парадигм, як IoT і хмарні обчислення, вимагатиме покращення сумісності, оскільки це важливо для забезпечення майбутнього розширення технологій BCI. Крім того, відсутність сумісності обмежує визначення глобальних систем кібербезпеки та механізмів, які можна застосовувати. У цьому сенсі поточні рішення BCI орієнтовані на пристрій і не пропонують механізмів спільної роботи проти кібератак.

Локально розгортають BCI щоб керувати процесами збору нейронних даних. Така архітектура зазвичай розгортає фази BCI між двома фізичними пристроями. Перший, ідентифікований як пристрій BCI, зосереджується на нейронних процесах отримання та стимуляції (фази 1 і 2 циклу BCI). Навпаки, додатки BCI (фаза 5) працюють у пристрої ближнього керування, ПК або смартфоні, який керує пристроєм BCI за допомогою дротового або бездротового зв'язку. 3 і 4 фази циклу можуть бути однаково реалізовані в обох пристроях, де виробники приймають остаточне рішення. Альтернативні проекти можуть виникати через специфічні вимоги до розгортань.

В дослідженні [12] ідентифікували атаки, що впливають на мікропрограмне забезпечення пристрою, впливаючи на цілісність і конфіденційність даних, а також викликаючи збої в системі. Пристрої для нейростимуляції не мають шифрування та зазвичай визначають паролі за замовчуванням, що впливає на цілісність і конфіденційність, полегшуючи несанкціонований доступ до конфіденційних даних. Зловмисники також можуть зосередитися на розрядженні батареї пристрою, що вплине як на доступність сервісу, так і на фізичну безпеку користувачів.

Нейроінтерфейси із закритим циклом використовують фізіологічні дані, отримані BCI, для покращення процедур стимуляції або доставки ліків. Однак ці конфіденційні дані можуть бути використані зловмисниками для отримання інформації про стан здоров'я пацієнта. Крім того, зловмисник може отримати конфіденційну інформацію, що зберігається на пристрої, таку як налаштування стимуляції, особисті дані або стан батареї, корисну для виконання нових атак. Було ідентифіковано [12] атаки соціальної інженерії та фішинг проти BCI, зосереджені на отриманні облікових даних користувача, що впливає на конфіденційність даних. Ці системи можуть зазнавати атак зловмисного програмного забезпечення та, зокрема, програм-вимагачів і тих, що базуються на ботнетах, що впливає на цілісність і доступність даних і програм.

Зосереджуючись на зв’язку між пристроями, в роботі [13] було досліджено безпеку комерційного рівня Emotiv Insight, який реалізував Bluetooth Low Energy (BLE) у своїй версії 4.0 для зв’язку зі смартфоном, який містить програму, запропоновану Emotiv. Було успішно здійснено атаки типу "людина посередині" через канал BLE, маючи можливість перехоплювати та змінювати інформацію, змушувати BCI виконувати небажані завдання та проводити атаки з повторенням, що, таким чином, впливає на цілісність, конфіденційність і доступність конфіденційних даних.

В якості контрзаходів слід відзначити шифрування мікропрограми, а також хеш або підпис перевірки автентичності, періодичні оновлення мікропрограми та використання механізмів авторизації для цих оновлень. Як загальні контрзаходи, може бути запрооноване регулювання нейротехнології як спосіб стандартизації її виробничих процесів. Пристрої BCI повинні зберігати журнали та отримувати доступ до подій, включаючи механізми звітування про помилки. Використання надійних криптографічних механізмів і останніх версій протоколів є визначальним для уникнення криптографічних атак, атак типу "людина посередині" та атак з перехопленням .

2.3 Висновки до розділу 2

З метою оцінки ризиків для нейроінтерфейсів необхідно проводити ретельний аналіз інформації щодо загроз і притаманних їм вразливостей. Незважаючи на незначне поширення і в зв’язку з браком комерційного інтересу, нейроінтерфейси мають відові вразливості. Слабке шифрування даних, що зберігаються на пристрої, може спричинити атаки «людина посередині». Атаки, пов’язані з даними та обліковими даними користувача, мають більший вплив, якщо системою користуються кілька користувачів.

3 ПРАКТИЧНЕ ДОСЛІДЖЕННЯ ВРАЗЛИВОСТЕЙ НЕЙРОІНТЕРФЕЙСУ

3.1 Апаратна реалізація досліджуваного нейроінтерфейсуҐ

Для практичного дослідження вразливостей було обрано доступний пристрій TGAM brainwave EEG виробництва Sichiray (КНР). Цей пристрій, так само, як і лінійка гарнітур MindTools містить технологію NeuronSky ThinkGear, яка вимірює аналогові електричні сигнали, які зазвичай називають мозковими хвилями, і обробляє їх у цифрові сигнали [14]. Потім технологія TheThinkGear робить ці вимірювання та сигнали доступними для програм.

Комплект TGAM є однією з найважливіших частин нейроінтерфейсу. В копмлект входять модуль Bluetooth, TGAM, електрод EEG? вушні кліпси, екрануючий провід, футляр для батареї.

Рисунок 3.1 – Модуль STM32 TGAM для Arduino

Набір датчиків мозкових хвиль Sichiray TGAM EEG безпечно вимірює та передає сигнали, такі як увага та медитація, альфа, бета, дельта, гамма і тета хвиль через ведений модуль Bluetooth. Набір складається з електрода ЕЕГ, двох вушних затискачів із заземлюючими електродами, модулів TGAM і Bluetooth, а також тримача батарейок 2xAAA з перемикачем. Потрібна додаткова пов'язка, щоб електрод ЕЕГ лежав на лобі над очима. Для сполучення та передачі даних потрібні наступні параметри: UART (універсальний асинхронний приймач/передавач) працює на швидкості передачі даних 1200, 9600 і 57600 біт/с; відсутність бітів парності та один стоп-біт. Приймальна частина складається з плати Arduino Uno, з'єднаної з головним модулем Bluetooth HC-05, де контакти HC-05 TXD і RXD відповідно з'єднані з контактами Arduino Uno для запуску команд AT на Модуль HC-05. Контакти HC-05 TXD і RXD відповідно з'єднані з контактами Arduino Uno RXD і TXD для передачі даних.

Було використано Brain [15] бібліотека Arduino для аналізу даних з ЕЕГ-гарнітур на базі Neurosky. Відповідний модифікований код подано в додатках. Функція getCSV() повертає рядок (char*) із переліком останніх даних про мозок у такому форматі: «сила сигналу, увага, медитація, дельта, тета, низька альфа, висока альфа, низька бета, висока бета, низька гама, висока гама. Потужність сигналу коливається від 0 до 200. Значення потужності ЕЕГ - це сильно відфільтроване представлення відносної активності на різних довжинах хвиль мозку. Через обмеженість ресурсів використаної платформи, для заходів захисту було вирішено використати спеціалізлвану платформу AWS IoT.

3.2 Планування та проведення заходів з протидії вразливостей

AWS IoT Core дозволяє налаштувати підключення пристроїв IoT до AWS Cloud та дозволяє іншим хмарним службам взаємодіяти з цим пристроєм.

Цей сервіс може обробляти повідомлення та направляти їх до AWS IoT та на сторонні пристрої.

AWS IoT Core задіює X.509 сертифікати для забезпечення доступу пристноїв до служби. Після аутентифікації, дозволені дії (підключення до брокера, отримання та надсилання повідомлень) базуються на AWS IoT політиці. Політики та ролі AWS Identity and Access Management дозволяють від імені користувача отримувати доступ до інших ресурсів AWS.

Відповідно до досліджуваної реалізації нейроінтерфейсу, мікроконтроллер задіюється для реєстрації, попереднього формування потоку даних з датчика EEG. Щоб зібрати дані, виконують такі завдання:

- Встановлення зв'язку із датчиком EEG,
- Збір та перетворення даних.

З цією метою:

- попередньо реєструють датчики у AWS з консолі IoT AWS,
- визначають ролі, політики й сертифікати за допомогою Identity&Access Management,
- налагоджують зв’язок з датчиком,
- періодично збирають дані з датчика.

Для виконання операції на платформі AWS, реєстрації та конфігурування пристроїв в цьому дослідженні використано інтегроване середовище розробки AWS Cloud9 (див рисунок 3.2), яке включає редактор програми, відлагоджувальник і термінал.

Перш за все, треба створити середовище «Sensor». Для підключення до AWS IoT Core треба кореневий сертифікат (мав би постачатися з пристроєм).

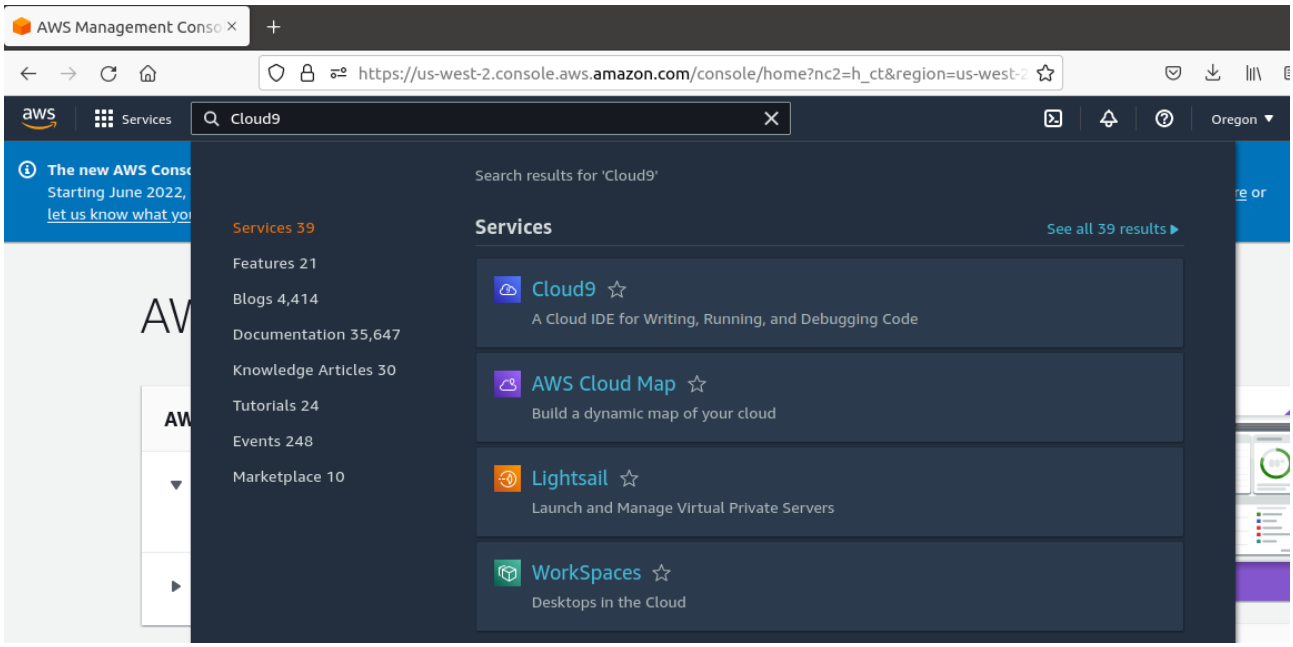

Рисунок 3.2 – Вибір середовища розробки Cloud9.

Перед алаштуванням конфігурації пристрою, маємо створити тип і річ у AWS IoT Core. Це можна здійснити через меню **IoT Core** > **Manage** > **Types.**

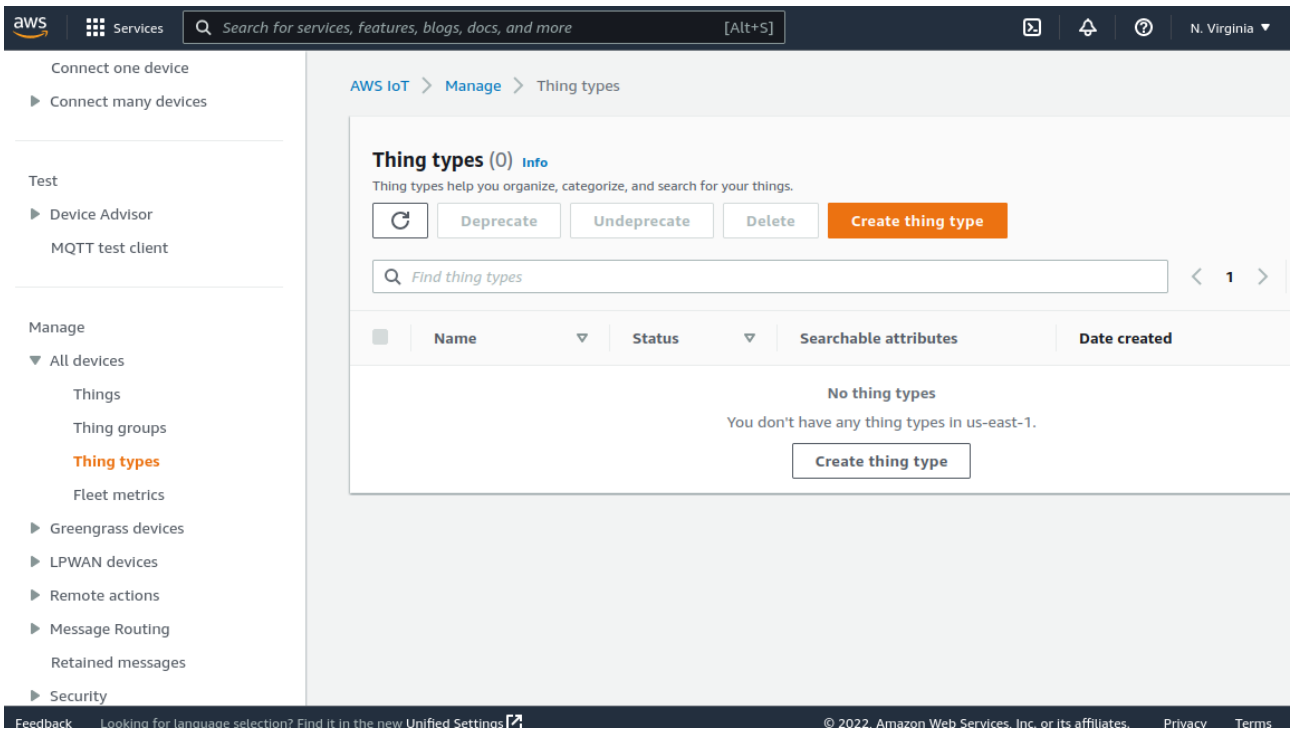

Рисунок 3.3 – Створення типу для пристрою в AWS IoT Core.

Можна також додатидовільний опис, наприклад про те що саме фіксує датчик. Кожному датчику, зареєстрованому як окрема річ, можна призначати свіої значення цих атрибутів, після чого за ними можна групувати датчики та проводити пошук.

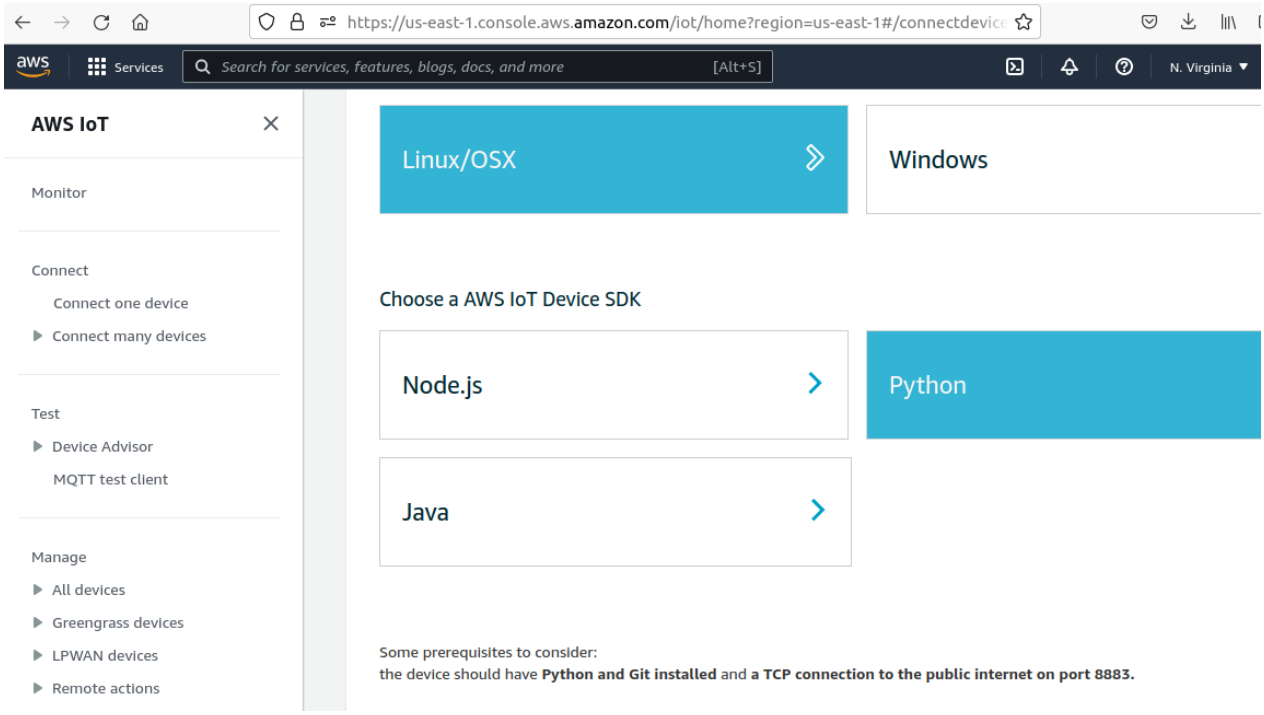

Рисунок 3.4 – Python Software Development Kit, який використовується для конфігурування.

Датчик під’єднуємо з меню **Connect device** і реєструємо як "envSensor001". Типу відповідатиме зареєстрованому екземпляру датчика.

Пакет підключення включає сертифікат пристрою, відкритий та закритий ключ, початковий сценарій для тестування підключення. Наступним кроком треба переконатися (в консолі AWS) в тому, що пристрій вдало заеєстровано та він під’єдний зі своїм ідентифікатором, отже можна його сконфігурувати відповідно до обраної політики безпеки.

Після завершення цих налаштувань для потрібного нам типу датчиків можна визначити окрему політику доступу та привілеїв пристрою (див. рис. 3.5). Базова політика надає датчику (thing)права на публікацію а також підписку на вибрані тем. Щоб дозволити пристрою публікувати виключно певні потрібні теми, необхідно змінити політику.

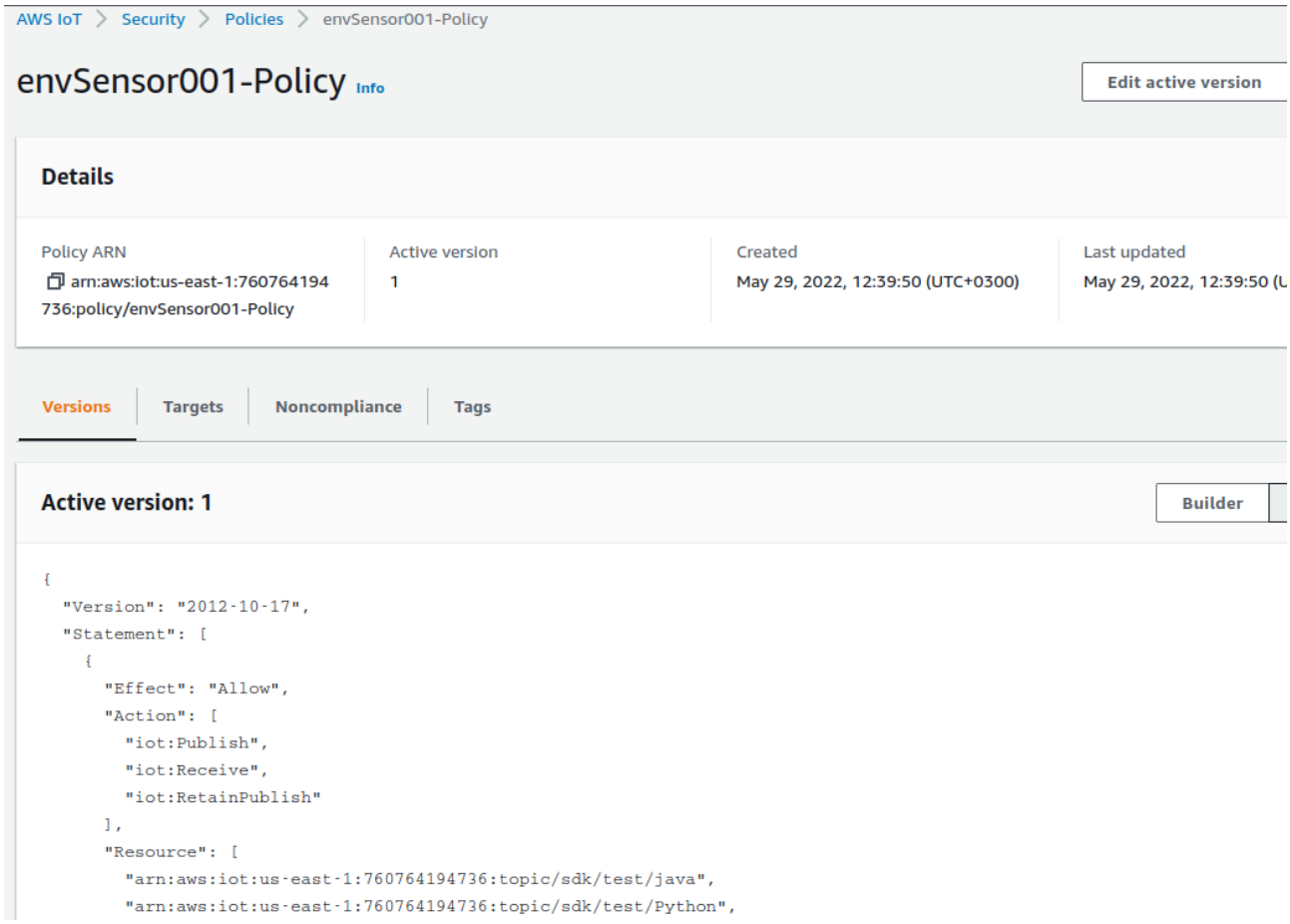

Рисунок 3.5 – Налаштування політики для датчика

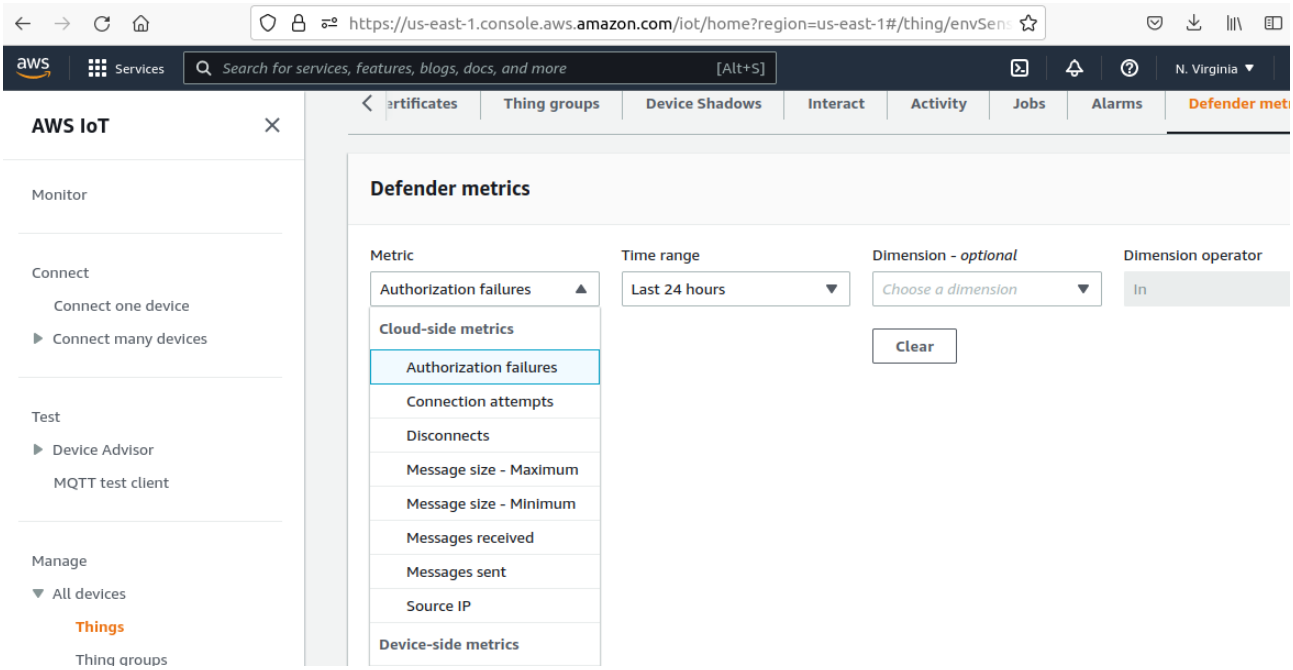

Рисунок 3.6 – Відлаштування подій, для яких відбудеться реагування і логування

Встановивши необхідні бібліотеки (рисунок 3. 7), на запит треба ввести назву сенсора, після чого дані починають надходити в хмарне сховище, ведулься системні логи, що свідчить про належне конфігурування датчика, який у нейроінтерфейсі відповідає за отримання сигналу ЕЕГ.

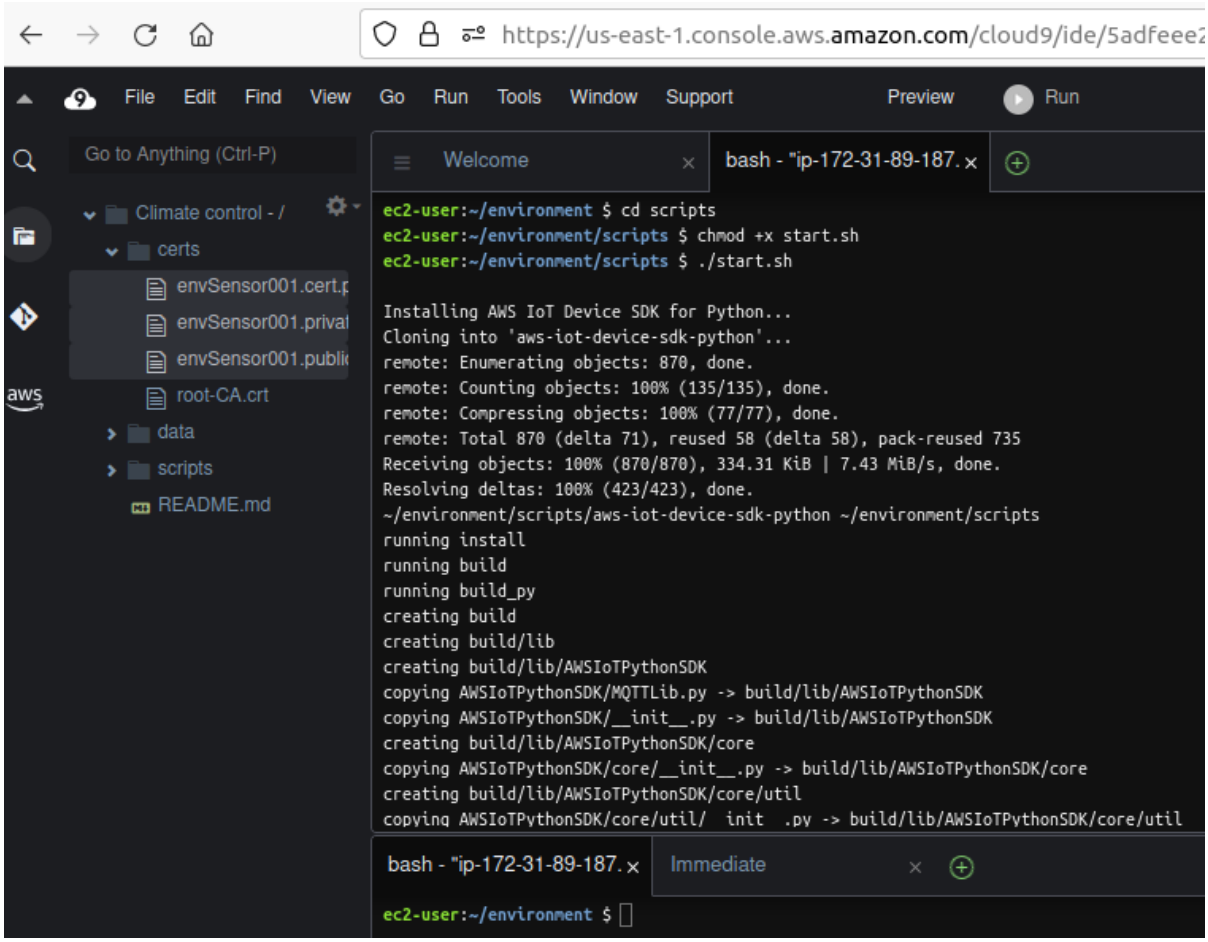

Рисунок 3.10 – Встановлення бібліотек та запуск пристрою

Аналіз наведеної вище послідовності конфігурації вказує, що пристрій повинен використовувати детальні ідентифікатори і завжди їх пов’язувати з зібраними даними. Завдяки цьому систему можна горизонтально маштабувати і за необхідності розслідувати порушення безпеки.

3.8 Висновки до розділу 3

В третьому розділі досліджено вразливості системи з нейроінтерфейсом, яка має всі атрибути та особливості пристрою IoT, за допомогою AWS IoT Core і показано, як стандартна методика конфігурування може допомогти уникнути втрати чи пошкодження чутливих конфіденційних даних.

4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Охорона праці

Тема кваліфікаційної роботи магістра присвячена дослідженню вразливостей нейроінтерфейсів. Оскільки, дана тема передбачає використання електронно-обчислювальної техніки, то важливим є дотримання вимог з охорони праці і техніки безпеки. Проаналізуємо основні правила і норми, яких необхідно дотримуватись при експлуатації комп'ютерів та периферійних пристроїв.

В загальному, поняття охорона праці в комп'ютерних системах являє собою дотримання всіх вимог і нормативів, що присутні в законодавчих актах про охорону праці. Закони цієї області спрямовані на якісну і безпечну експлуатацію робочих приладів і приміщень, дотримання санітарногігієнічних умов праці і захист від інших небезпечних чинників на підприємстві. В основних законодавчих актах про охорону праці приділяється велика увага поліпшенню умов праці в усіх галузях господарства, впровадженню сучасних засобів техніки безпеки і забезпечення санітарно-гігієнічних умов, що запобігають виробничому травматизму і професійним захворюванням.

Охорона життя і здоров'я людини є пріоритетним напрямком соціальної політики держави. В Україні прийнято закон прямої дії «Про охорону праці», який регламентує захист конституційного права працівників на безпечні умови праці. Законодавство України про охорону праці складається із загальних законів України та спеціальних законодавчих актів. Загальними законами України, що визначають основні положення з охорони праці є Конституція України, Закон України «Про охорону праці», Кодекс законів про працю (КЗпП), Закон України «Про загальнообов'язкове державне соціальне страхування від нещасного 105 випадку на виробництві та професійного захворювання, які спричинили втрату працездатності».

Одним із найважливіших нормативних документів щодо забезпечення охорони праці користувачів ПК є "Державні санітарні норми 47 і правила роботи з візуальними дисплейними терміналами (ВДТ) електронно-обчислювальних машин" ДСанПіН 3.3.2.007-98. Дотримання даних правил значно знижує наслідки несприятливої дії на працівників шкідливих та небезпечних факторів, які супроводжують роботу з 106 відеодисплейними матеріалами, зокрема можливість зорових, емоційних переживань, серцево-судинних захворювань. Виходячи з цього, роботодавець повинен забезпечити гігієнічні й ергономічні вимоги щодо організації робочих приміщень для експлуатації електроннообчислювальних машин (ЕОМ) з ВДТ, робочого середовища, робочих місць з ЕОМ, режиму праці і відпочинку при роботі з ЕОМ тощо, які викладені у нормах НПАОП 0.00-7.15- 18.

При виконанні дослідження вразливостей нейроінтерфейсів, яке передбачає використання ПК, площа та об'єм для одного робочого місця оператора визначається згідно вимог НПАОП 0.00-7.15-18 «Вимоги щодо безпеки та захисту здоров’я працівників під час роботи з екранними пристроями», зокрема площа повинна становити не менше 6,0 м², об'єм - не менше 20,0 м³, відстань робочого місця від стіни повинна складати 1м, а відстань між робочими місцями повинна становити 1,7 м.

Згідно вимог охорони праці та державних санітарних правил, стіни, стеля та підлога приміщень, в яких розміщені ЕОМ, повинні бути виготовлені з матеріалів, дозволених для оформлення приміщень органами державного санітарно-епідеміологічного нагляду.

При виборі кімнат для розміщення робочих місць ПК враховано ступінь відбиття світла на екранах дисплеїв, яке проходить через вікна і яке може викликати значне осліплення в тих, хто сидить перед ними, особливо влітку та в сонячні дні. Тому, ПК і оргтехніка розміщені біля стін, які не знаходяться біля вікон або навпроти них.

Оскільки, при незадовільному освітленні знижується продуктивність праці користувачів ПК, і можливі негативні впливи на здоров'я такі, як 48 короткозорість, швидка втомленість, тому всі приміщення, які облаштовані робочими місцями з ПК, мають природне і штучне освітлення. Не допускається розташування робочих місць з ПК в підвальних приміщеннях.

Штучне освітлення у приміщеннях повинно бути виконано у вигляді комбінованої системи освітлення з використанням люмінесцентних джерел світла у світильниках загального освітлення, які розташовувати над робочими поверхнями у рівномірно-прямокутному порядку. Штучне освітлення забезпечує на робочих місцях з ПК освітленість 300 – 500 Лк.

Для запобігання засвітленню екранів ПК прямими світловими потоками лінії світильників розташовані з достатнім бічним зміщенням відносно рядів робочих місць, а також паралельно до світлових отворів. При цьому кожне вікно повинно мати світлорозсіюючі штори з коефіцієнтом відбивання 0,7.

Отже, при розробці програмного продукту для аналізу вразливості сайту до XSS-атак, проаналізовано та враховано необхідні вимоги щодо охорони праці при використанні електронно-обчислювальної техніки і забезпечено умови для зручної та ефективної роботи працівників.

Ергономічні вимоги до робочого місця користувача персональним комп'ютером

4.2 Безпека в надзвичайних ситуаціях

Кожен має право на належні, безпечні і здорові умови праці. Це гарантує нам Конституція України (ч. 4 ст. 43).

У відповідності до вимог ст. 153 Кодексу законів про працю України на всіх підприємствах, в установах, організаціях створюються безпечні і нешкідливі умови праці. Забезпечення безпечних і нешкідливих умов праці покладається на власника або уповноважений ним орган. Умови праці на робочому місці, безпека технологічних процесів, машин, механізмів, устаткування та інших засобів виробництва, стан засобів колективного та індивідуального захисту, що використовуються працівником, а також санітарно-побутові умови повинні відповідати вимогам нормативних актів 49 про охорону праці. Власник або уповноважений ним орган повинен впроваджувати сучасні засоби техніки безпеки, які запобігають виробничому травматизму, і забезпечувати санітарно-гігієнічні умови, що запобігають виникненню професійних захворювань працівників. Стаття 158 Кодексу законів про працю України встановлює обов'язок власника або уповноваженого ним органу вживати заходів щодо полегшення і оздоровлення умов праці працівників шляхом впровадження прогресивних технологій, досягнень науки і техніки, засобів механізації та автоматизації виробництва, вимог ергономіки, позитивного досвіду з охорони праці, зниження та усунення запиленості та загазованості повітря у виробничих приміщеннях, зниження інтенсивності шуму, вібрації, випромінювання тощо. А згідно з ч. 1 ст. 13 Закону України «Про охорону праці» роботодавець зобов'язаний створити на робочому місці в кожному структурному підрозділі умови праці відповідно до нормативно-правових актів, а також забезпечити додержання вимог законодавства щодо прав працівників у галузі охорони праці.

Робочі місця офісних працівників, обладнані персональними комп'ютерами (далі – робочі місця), повинні відповідати вимогам «Правил охорони праці під час експлуатації електронно-обчислювальних машин», затверджених Наказом Державного комітету України з промислової безпеки, охорони праці та гірничого нагляду від 26.03.2010 року № 65 (Правила), та

«Державних санітарних правил і норм роботи з візуальними дисплейними терміналами електронно-обчислювальних машин», затверджених постановою Головного державного санітарного лікаря України від 10.12.98 N 7 (ДСанПіН 3.3.2-007-98). Правила поширюються на всіх суб'єктів господарювання незалежно від форм власності, які у своїй діяльності здійснюють роботу, пов'язану з персональними комп'ютерами, у тому числі на тих, які мають робочі місця, обладнані персональними комп'ютерами і периферійними пристроями. Зазначені нормативно-правові акти встановлюють санітарногігієнічні вимоги до приміщення, в якому 50 розташоване робоче місце, власне до робочого місця, освітлення, рівнів вібрації і шуму, мікроклімату в приміщенні тощо. При розміщенні робочих столів з персональними комп'ютерами слід дотримувати:

- відстань між бічними поверхнями персональних комп'ютерів 1,2 м.;

- відстань від тильної поверхні одного персонального комп'ютера до

- екрана іншого – 2,5 м.

- За потреби особливої концентрації уваги під час виконання робіт суміжні робочі місця операторів необхідно відділяти одне від одного перегородками висотою 1,5 – 2 м.

Конструкція робочого місця користувача персонального комп'ютера має забезпечити підтримання оптимальної робочої пози офісного працівника. Конструкція робочого столу має відповідати сучасним вимогам ергономіки і забезпечувати оптимальне розміщення на робочій поверхні використовуваного обладнання (дисплея, клавіатури, принтера) і документів. Висота робочої поверхні робочого столу має регулюватися в межах 680-800 мм, а ширина і глибина – забезпечувати можливість виконання операцій у зоні досяжності моторного поля (рекомендовані розміри: 600-1400 мм, глибина – 800-1000 мм). Робочий стіл повинен мати простір для ніг заввишки не менше ніж 600мм, завширшки не менше ніж 500 мм, завглибшки (на рівні

колін) не менше ніж 450 мм, на рівні простягнутої ноги не менше ніж 650 мм. Робочий стілець має бути підйомно-поворотним, регульованим за висотою, з кутом і нахилу сидіння та спинки і за відстанню від спинки до переднього краю сидіння поверхня сидіння має бути плоскою, передній край – заокругленим. Регулювання за кожним із параметрів має здійснюватися незалежно, легко і надійно фіксуватися. Шаг регулювання елементів стільця має становити: для лінійних розмірів – 15-20 мм, для кутових – 2-5 градусів. Зусилля регулювання має не перевищувати 20Н. Висота поверхні сидіння має регулюватися в межах 400-500 мм, а ширина і глибина становити не менше ніж 400 мм. Кут нахилу сидіння – до 15 градусів вперед 51 і до 5 градусів назад. Висота спинки стільця має становити (300+-20) мм, ширина – не менше ніж 380 мм, радіус кривизни горизонтальної площини – 400мм. Кут нахилу спинки має регулюватися в межах 1-30 градусів від вертикального положення. Відстань від спинки до переднього краю сидіння має регулюватися в межах 260-400 мм. Для зниження статичного напруження м’язів верхніх кінцівок слід використовувати стаціонарні або змінні підлокітники завдовжки не менше ніж 250 мм, завширшки 50-70 мм, що регулюються за висотою над сидінням у межах 230-260 мм і відстанню між підлокітниками в межах 350-500 мм. Поверхня сидіння і спинки стільця має бути напівм’якою з нековзним, повітронепроникним покриттям, що легко чиститься і не електризується. Робоче місце має бути обладнане підставкою для ніг завширшки не менше ніж 300 мм, завглибшки не менше ніж 400мм, що регулюється за висотою в межах до 150 мм і за кутом нахилу опорної поверхні підставки до 20 градусів. Підставка повинна мати рифлену поверхню і бортик по передньому краю заввишки 10 мм. Робочі місця слід розташовувати відносно світових прорізів так, щоб природне світло падало переважно з лівого боку. Монітор має розташовуватися на оптимальній відстані від очей користувача, що становить 600-700 мм, але не ближче ніж за 600 мм з урахуванням розміру літеро-цифрових знаків і символів. Розташування екрана монітору має забезпечувати зручність зорового

спостереження у вертикальній площині під кутом +30 градусів до нормальної лінії погляду працівника. Клавіатуру слід розташовувати на поверхні столу на відстані 100-300 мм від краю, звернутого до працюючого. У конструкції клавіатури має передбачатися опорний пристрій (виготовлений із матеріалу з високим коефіцієнтом тертя, що перешкоджає мимовільному її зсуву), який дає змогу змінювати кут нахилу поверхні клавіатури у межах 5-15 градусів. Висота середнього рядка клавіш має не перевищувати 30 мм. Поверхня клавіатури має бути матовою з коефіцієнтом відбиття 0,4. Розташування пристрою введення – виведення інформації має забезпечувати добру видимість монітору, зручність ручного 52 керування в зоні досяжності моторного поля і за висотою – 900-1300 мм, за шириною 400-500 мм. Під матричні принтери потрібно підкладати вібраційні килимки для гасіння вібрації та шуму. Робоче місце з персональним комп'ютером слід обладнати пюпітром для документів, що легко переміщуються. Для забезпечення захисту і досягнення нормованих рівнів комп'ютерного випромінювання необхідно застосування екранних фільтрів, локальних світлофільтрів (засобів індивідуального захисту очей) та інших засобів захисту, що пройшли випробування в акредитованих лабораторіях і мають щорічний гігієнічний сертифікат.

ВИСНОВКИ

В процесі виконання кваліфікаційної роботи було проведено літературний аналіз джерел в галузі кібербезпеки та досліджено вразливості нейроінтерфейсів. В роботі також вивчено та практично застосовано для системи Sichiray TGAM сучасні засобb для мінімізації загроз безпеці та проведено конфігурування та налаштування політик безпеки пристроїв за допомогою інструментів платформи AWS IoT Core.

Для досягнення поставленої мети було розв'язано наступні завдання:

- З’ясовано типи та характерні особливості вразливостей ytqhjsynthatqcsdй.
- Проаналізовано відомі способи запобіганням загрозам.
- Проведено порівняльний аналіз доступних засобів захисту.
- Здійснено планування та реалізовано заходи захисту для системи заданої специфікації.

Крім цього, в роботі у розділі "Безпека життєдіяльності, основи охорони праці" проведено аналіз ризику як кількісної оцінки небезпек а також дана характеристика приміщень щодо небезпеки ураження електричним струмом, пожежної небезпеки, вибухонебезпеки.

БІБЛІОГРАФІЯ

1. Bernal S.L., Celdrán A.H., Pérez G.M., Barros M.T., Balasubramaniam S. Security in Brain-Computer Interfaces: State-of-the-Art, Opportunities, and Future Challenges. ACM Comput. Surv. Vol. 54. P. 1–35.
2. Butsiy R., Lupenko S. Comparative analysis of neurointerface technologies for the problem of their reasonable choice in human-machine information systems. Scientific Journal of the Ternopil National Technical University. 2020. No. 4 (100). P. 135–148. URL: https://doi.org/10.33108/visnyk_tntu2020.04.
3. Tzyy-Ping Jung. Principles and Applications of Brain-Computer Interfaces. Center for Advanced Neurological Engineering and Swartz Center for Computational Neuroscience and University of California San Diego, USA. URL: https://cfmriweb.ucsd.edu/ttliu/be280a_12/BE280A12_BCI1.pdf
4. O. Kramar, Y. Drohobytskiy, Y. Skorenkyy, O. Rokitskyi, N. Kunanets, V. Pasichnyk, O. Matsiuk. Augmented Reality-assisted Cyber-Physical Systems of Smart University Campus. 2020 IEEE 15th International Scientific and Technical Conference on Computer Sciences and Information Technologies, CSIT 2020 - Proceedings : Institute of Electrical and Electronics Engineers Inc., Vol. 2, pp. 309-313, 2020.
5. Y. Skorenkyy, R. Kozak, N. Zagorodna, O. Kramar, I. Baran. Use of augmented reality-enabled prototyping of cyber-physical systems for improving cyber-security education. Journal of Physics: Conference Series, Vol. 1840, Issue 1, 012026, 2021.
6. A. Kharchenko, I. Halay, N. Zagorodna, I. Bodnarchuk. Optimization of software architecture selection for the system under design and reengineering. 14th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering, TCSET 2018 - Proceedings, pp. 1245–1248, 2018.
7. Abdulkader S.N., Atia A., Mostafa M.S. Brain computer interfacing: Applications and challenges // Egyptian Informatics Journal, Vol. 16, Issue 2. 2015. 213-230.URL: https://doi.org/10.1016/j.eij.2015.06.002.
8. Moore-Jackson M., Mappus R. Applications for Brain-Computer Interfaces. In: Tan, D., Nijholt, A. (eds) Brain-Computer Interfaces. Human-Computer Interaction Series. Springer, London. 2010. URL: https://doi.org/10.1007/978-1-84996-272-8_6

9. Samaa S., Dr-Hussain R., Manal J. A Systematic Review of Brain-Computer Interface Based EEG. // Iraqi Journal for Electrical And Electronic Engineering. 2020. 16. 10.37917/ijeee.16.2.9.
10. Shmatko O., Balakireva S., Vlasov A., Zagorodna N., Korol O., Milov O. Development of Methodological Foundations for Designing a Classifier of Threats to Cyber-physical Systems // Eastern-European Journal of Enterprise Technologies, 3 (105), 6-19. 2020. doi: 10.15587/1729-4061.2020.205702. URL: https://ssrn.com/abstract=3719718
11. NIST Special Publication (SP) 800-30, Revision 1, Guide for Conducting Risk Assessments. [Електронний ресурс] – Режим доступу до ресурсу: https://www.nist.gov/privacy-framework/nist-sp-800-30
12. Usieto P.B., Minguez H. Avoiding brain hacking // Challenges of cybersecurity and privacy in Brain Computer Interfaces. 2018. URL: https://www.bitbrain.com/blog/cybersecurity-brain-computer-interface
13. Sundararajan K. Privacy and security issues in Brain Computer Interface. Master's thesis. 2017. Auckland University of Technology.
14. Brainwave Computer Interface Prototype TGAM Starter Kit Soldering & Testing URL: https://www.instructables.com/TGAM-Starter-Kit-Soldering-Testing/
15. ARDUINO BRAIN LIBRARY. URL:https://github.com/kitschpatrol/Brain
16. Я.І. Бедрій Безпека життєдіяльності: Навч.посібн. – К.: Вид-во Кондор, 2009.
17. Ярошевська В.М. Безпека життєдіяльності: Навч.посібн. – Київ: Вид-во Кондор, 2004.

Додаток А

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ

М А Т Е Р І А Л И

X НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ»

7–8 грудня 2022 року

ТЕРНОПІЛЬ
2022

Computer Interfaces: State-of-the-Art, Opportunities, and Future Challenges. ACM Comput. Surv. Vol. 54. P. 1–35.

2. Butsiy R., Lupenko S. Comparative analysis of neurointerface technologies for the problem of their reasonable choice in human-machine information systems. Scientific Journal of the Ternopil National Technical University. 2020. No. 4 (100). P. 135–148. URL: https://doi.org/10.33108/visnyk_tntu2020.04.

Brain.cpp Instantiates the brain library on a hardware serial port.

```
#include "Arduino.h"

#include "Brain.h"


Brain::Brain(Stream &_brainStream) {

brainStream = &_brainStream;

init();

}


void Brain::init() {

freshPacket = false;

inPacket = false;

packetIndex = 0;

packetLength = 0;

eegPowerLength = 0;

hasPower = false;

checksum = 0;

checksumAccumulator = 0;


signalQuality = 200;

attention = 0;

meditation = 0;


clearEegPower();

}
```

```
boolean Brain::update() {

if (brainStream->available()) {

latestByte = brainStream->read();

if (inPacket) {

if (packetIndex == 0) {

packetLength = latestByte;

if (packetLength > MAX_PACKET_LENGTH) {

sprintf(latestError, "ERROR: Packet too long %i", packetLength);

inPacket = false;

}

}

else if (packetIndex <= packetLength) {

packetData[packetIndex - 1] = latestByte;

checksumAccumulator += latestByte;

}

else if (packetIndex > packetLength) {

checksum = latestByte;

checksumAccumulator = 255 - checksumAccumulator;

if (checksum == checksumAccumulator) {

boolean parseSuccess = parsePacket();


if (parseSuccess) {

freshPacket = true;

}

else {

sprintf(latestError, "ERROR: Could not parse");
```

```
}

}

else {

sprintf(latestError, "ERROR: Checksum");

}

inPacket = false;

}


packetIndex++;

}

if ((latestByte == 170) && (lastByte == 170) && !inPacket) {

inPacket = true;

packetIndex = 0;

checksumAccumulator = 0;

}

lastByte = latestByte;

}


if (freshPacket) {

freshPacket = false;

return true;

}

else {

return false;

}
```

```
}

void Brain::clearPacket() {
for (uint8_t i = 0; i < MAX_PACKET_LENGTH; i++) {
packetData[i] = 0;
}
}

void Brain::clearEegPower() {
for(uint8_t i = 0; i < EEG_POWER_BANDS; i++) {
eegPower[i] = 0;
}
}

boolean Brain::parsePacket() {
hasPower = false;
boolean parseSuccess = true;
clearEegPower(); // clear the eeg power to make sure we're honest about missing values

for (uint8_t i = 0; i < packetLength; i++) {
switch (packetData[i]) {
case 0x2:
signalQuality = packetData[++i];
break;
case 0x4:
attention = packetData[++i];
break;
```

```
case 0x5:
meditation = packetData[++i];
break;
case 0x83:
i++;
for (int j = 0; j < EEG_POWER_BANDS; j++) {
uint8_t a,b,c;
a = packetData[++i];
b = packetData[++i];
c = packetData[++i];
eegPower[j] = ((uint32_t)a << 16) | ((uint32_t)b << 8) | (uint32_t)c;
}

hasPower = true;
break;
case 0x80:
i += 3;
break;
default:
/*
Serial.print(F("parsePacket UNMATCHED data 0x"));
Serial.print(packetData[i], HEX);
Serial.print(F(" in position "));
Serial.print(i, DEC);
printPacket();
*/
```

```
parseSuccess = false;
break;
}
}
return parseSuccess;
}
void Brain::printCSV() {
brainStream->print(signalQuality, DEC);
brainStream->print(",");
brainStream->print(attention, DEC);
brainStream->print(",");
brainStream->print(meditation, DEC);
if (hasPower) {
for(int i = 0; i < EEG_POWER_BANDS; i++) {
brainStream->print(",");
brainStream->print(eegPower[i], DEC);
}
}

brainStream->println("");
}
char* Brain::readErrors() {
return latestError;
}
char* Brain::readCSV() {
if(hasPower) {
```

```
sprintf(csvBuffer,"%d,%d,%d,%lu,%lu,%lu,%lu,%lu,%lu,%lu,%lu",
signalQuality,
attention,
meditation,
eegPower[0],
eegPower[1],
eegPower[2],
eegPower[3],
eegPower[4],
eegPower[5],
eegPower[6],
eegPower[7]
);

return csvBuffer;
}
else {
sprintf(csvBuffer,"%d,%d,%d",
signalQuality,
attention,
meditation
);

return csvBuffer;
}
}
```

```
void Brain::printPacket() {
brainStream->print("[");
for (uint8_t i = 0; i < MAX_PACKET_LENGTH; i++) {
brainStream->print(packetData[i], DEC);

if (i < MAX_PACKET_LENGTH - 1) {
brainStream->print(", ");
}
}
brainStream->println("]");
}

void Brain::printDebug() {
brainStream->println("");
brainStream->println("--- Start Packet ---");
brainStream->print("Signal Quality: ");
brainStream->println(signalQuality, DEC);
brainStream->print("Attention: ");
brainStream->println(attention, DEC);
brainStream->print("Meditation: ");
brainStream->println(meditation, DEC);

if (hasPower) {
brainStream->println("");
brainStream->println("EEG POWER:");
brainStream->print("Delta: ");
```

```
brainStream->println(eegPower[0], DEC);

brainStream->print("Theta: ");

brainStream->println(eegPower[1], DEC);

brainStream->print("Low Alpha: ");

brainStream->println(eegPower[2], DEC);

brainStream->print("High Alpha: ");

brainStream->println(eegPower[3], DEC);

brainStream->print("Low Beta: ");

brainStream->println(eegPower[4], DEC);

brainStream->print("High Beta: ");

brainStream->println(eegPower[5], DEC);

brainStream->print("Low Gamma: ");

brainStream->println(eegPower[6], DEC);

brainStream->print("Mid Gamma: ");

brainStream->println(eegPower[7], DEC);

}


brainStream->println("");

brainStream->print("Checksum Calculated: ");

brainStream->println(checksumAccumulator, DEC);

brainStream->print("Checksum Expected: ");

brainStream->println(checksum, DEC);


brainStream->println("--- End Packet ---");

brainStream->println("");

}
```

```
uint8_t Brain::readSignalQuality() {

return signalQuality;

}

uint8_t Brain::readAttention() {

return attention;

}

uint8_t Brain::readMeditation() {

return meditation;

}

uint32_t* Brain::readPowerArray() {

return eegPower;

}

uint32_t Brain::readDelta() {

return eegPower[0];

}

uint32_t Brain::readTheta() {

return eegPower[1];

}

uint32_t Brain::readLowAlpha() {

return eegPower[2];

}
```

```
uint32_t Brain::readHighAlpha() {

return eegPower[3];

}


uint32_t Brain::readLowBeta() {

return eegPower[4];

}


uint32_t Brain::readHighBeta() {

return eegPower[5];

}


uint32_t Brain::readLowGamma() {

return eegPower[6];

}


uint32_t Brain::readMidGamma() {

return eegPower[7];

}
```

BrainSoftSerialTest.ino reads brain data over SoftwareSerial and prints a CSV over hardware serial.

```
#include <SoftwareSerial.h>

#include <Brain.h>

SoftwareSerial softSerial(10, 11);

Brain brain(softSerial);

void setup() {

softSerial.begin(9600);

Serial.begin(9600);

}


void loop() {

if (brain.update()) {

Serial.println(brain.readErrors());

Serial.println(brain.readCSV());

}

}
```