DOI https://doi.org/10.30525/978-9934-26-686-7-3

ОСНОВИ ПРОЦЕСУ ФІКСАЦІЇ КІБЕРПРАВОПОРУШЕНЬ, ЩО ВПЛИВАЮТЬ НА ЗМІНУ ПСИХІЧНОГО СТАНУ ОПЕРАТОРІВ ЕОМ

Гавриленко Є. В., Саханчук А. Д., Саханчук Т. І.

ВСТУП

Розвиток комунікаційних технологій зумовив багато перетворень у галузі спілкування мільйонів людей. Завдяки широкому та якісному розвитку комп'ютерних технологій людство все більше присвячує свій час життя роботі в соціальних мережах[1]. Серед соціуму виділяється група фахівців системи кібербезпеки, які забезпечують комфорт та безпеку спілкування в ланцюжках інформаційної взаємодії: «людина – комп'ютер – інформаційна мережа – комп'ютер – людина».

Як і багато століть тому, – створювана, збирана, збережена та передана інформація піддається порушенням конфіденційності, цілісності, доступності сукупність яких названі в керівних документах «тріадою CIA»[2].

Правопорушники, які раніше використовували для своїх корисливих цілей матеріально-речові інформаційні канали, з розвитком технологій також перемістили акценти свого негативного впливу на електронну область носіїв інформації. Чим досконаліше розвиваються інформаційні системи, тим витонченішими діють правопорушники.

Перелікам загроз для інформації і її захисту присвячено сотні документів нормативно-правової бази, серед яких закони, постанови Кабінету Міністрів України, галузеві нормативні документи відповідних державних установ, підприємств та організацій, стандарти, кодекси, й ін., як профілактичного, так і «виховного» характеру[3].

Кіберправопорушення є основним деструктивним фактором, що формує сучасні загрози інформаційній безпеці. Їхня «роль» полягає у систематичному та навмисному порушенні властивостей інформації, тобто порушенні її конфіденційності, цілісності та доступності.

Передові країни змушені створювати міжнародні організації задля забезпечення кібербезпеки. Дії користувачів, працівників, програмістів та адміністраторів різного рівня спрямовані на профілактику та протидію кіберправопорушенням.

---

[1] How much time do we spend on social media? Mediakix. 2016. URL: http://mediakix.com/2016/12/how-much-time-is-spent-on-social-media-lifetime/#gs.rPNYGG8

[2] Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР

[3] Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР; Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII; Про інформацію : Закон України від 02.10.1992 № 2657-XII; Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX.

Список злочинних комп'ютерних технологій впливу на інформацію дуже великий. Він містить багато певних загроз, які можуть призвести не тільки до небажаних втрат, що визнані реалізацією тріади CIA, а й впливати на стан операторів ЕОМ, створюючи умови для реалізації негативних наслідків кіберправопорушень. Чому й присвячена дана наукова робота.

1. Виникнення передумов проблеми та формулювання проблеми

Комп'ютерні технології для роботи з інформацією дозволяють кіберправопорушникам створювати певні загрози, класифікація яких наведена на Рис.1[4].

Рис. 1. Класифікація кіберзагроз інформації

2. Вплив кіберзагроз на операторів ЕОМ

Звісно, що кібератака – це злочин який здійснюється проти широкого спектра цілей – від викрадення даних, для отримання фінансової вигоди, шпигунства або дестабілізації роботи як державних структур, інфраструктури, так й психічного стану окремих громадян.

Європейське дослідження за участю майже тисячі осіб показало: кібератаки спроможні погіршити ментальне здоров'я тих, хто зіткнувся з випадками реалізованих кіберзагроз. Зокрема, йдеться про підвищену тривожність, стрес, гнітюче почуття провини, сором і гнів.

[4] Козюра В. Д., Хорошко В. О., Шелест М. Є., Ткач Ю. М., Усов Я. Ю. Комплексні системи захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. Ніжин : ФОП Лук'яненко В. В. ; ТПК «Орхідея», 2019. с. 128.

Яка саме емоційна реакція може накрити жертву – залежить від типу кібератаки.

Крадіжка CVV-коду картки, злом додатку банку або витік фінансових даних викликають тривогу. Злом акаунта в соціальних мережах з усіма листуваннями і «нюансами» – гнів і відчуття безпорадності. Той, хто повівся на фейкові листи від знайомих (наприклад, «начальник» наказав скинути внутрішні документи компанії), відчуває сором і провину – в першу чергу через ризик нашкодити іншим.

Найгостріші реакції викликають кіберзлочини, пов'язані з чутливою приватною інформацією, – наприклад, крадіжка медичних даних. Жертви таких атак відчувають сильний стрес і втрату контролю над власним життям.

Такі наслідки цілком можна порівняти з емоційними реакціями жертв фізичних злочинів. Коли хтось вривається в приватний інтернет-простір, це мало чим відрізняється від злому і розграбування квартири.

Почуття вразливості і хронічна тривожність після пережитої кібератаки посилюються нездатністю людей ефективно впоратися з її наслідками – багатьом для цього просто не вистачає знань.

Кіберзлочинність має глибокий та багатогранний вплив на психічне здоров'я людини, що класифікується фахівцями як значна публічна загроза. Результати впливу варіюються від легкого стресу до важких клінічних станів.

На основі досліджень, що висвітлюються у контексті цифрової безпеки та ментального здоров'я (зокрема за даними інституцій, що співпрацюють з ВООЗ, наприклад, INTERPOL та UNODC), можна виділити такі основні наслідки: психологічні та емоційні наслідки:

- психологічна травма та симптоми, схожі на посттравматичний стресовий розлад;
- тривога та депресія;
- сором та почуття провини;
- гнів та самоізоляція.

Слід особливо зупинитись на вплив кіберзагроз на стан підлітків та, в цілому, молоді.

Кібербулінг (кіберзалякування) – це систематичне цькування, приниження або залякування людини з використанням цифрових технологій: соціальних мереж, месенджерів, ігрових платформ чи мобільних телефонів. Це умисні дії, спрямовані на створення психологічного тиску, які можуть включати погрози, наклепи, поширення особистих даних, інтимних фото або самозванство.

Дослідження показують, що підлітки, які зазнали кібербулінгу, в 4 рази частіше схильні до самоушкодження або суїцидальних думок, ніж інші.

Більше 45% підлітків, що зазнали кібербулінгу, відчувають безпорадність, а близько 30% – повну самотність.

Зв'язок із загальним станом здоров'я, ВООЗ та партнери наголошують, що кібератаки на медичні заклади (наприклад, лікарні) не лише ставлять під загрозу конфіденційність пацієнтів, але можуть призвести до затримок у лікуванні, створюючи пряму загрозу життю та здоров'ю.

Аналізуючи сказане вище, ми говоримо про наслідки, які потерпілі особи почали відчувати і переживати, як прямий, наочний, видимий негативний

вплив отриманої аудіо та відео інформації з екрана монітора на їхнє психічне здоров'я і, в цілому, на організм, тобто це видимі наслідки, які встановлені.

Однак, кіберзагрози можуть впливати на психіку людину та її поведінку таким чином, що особа не помічає, або не одразу помічає, шкідливий вплив на неї, а також на ті дії чи бездіяльність, які вона буде вчинювати, будучи під негативним, злочинним впливом кіберправопорушника, який може використовувати спеціальні, приховані (непомітні) канали впливу на психіку та поведінку операторів ЕОМ.

В результаті впливу загроз може бути не тільки реалізована тріада CIA, але й змінений стан операторів ЕОМ. При цьому можуть бути створені програмні завади, що «не лише дезінформують операторів, але і й змінюють їх психофізіологічний стан за рахунок потайної дії на них спеціальних оптичних і звукових сигналів»[5]. У більшості випадків, умовно кажучи – звичайно, дія загроз спрямована на напрями, що висвітлені у XVI розділі Кримінального кодексу України (ККУ) як «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку»[6].

Щоб не перевантажувати цей матеріал назвами та змістом статей ККУ поставимо питання – «чи містить ККУ інформацію, яка описує покарання кіберправонарушника за злочинний вплив відтворюваної монітором інформації на психофізіологічний стан оператора ЕОМ?».

Відповідь: «Конкретно – ні. АЛЕ, побічно, для вирішення цього питання можна рекомендувати застосування низки статей ККУ».

Конкретизуємо питання: «Чи є злочином навмисний злочинний вплив зображення монітора на оператора ЕОМ»?

Відповідь: «Станом на лютий 2026 року, навмисний вплив зображення монітора на оператора ЕОМ може кваліфікуватися як злочин залежно від наслідків та способу здійснення такого впливу».

Прямої статті з таким формулюванням у Кримінальному кодексі України (ККУ) немає, проте подібні дії підпадають під наступні норми:

1.Кіберзлочини (Розділ XVI ККУ), якщо вплив здійснюється через несанкціоноване втручання в роботу комп'ютера (наприклад, хакерський злам для виведення шкідливого контенту), це порушує Статтю 361 ККУ.

2.Злочини проти життя та здоров'я:

- якщо візуальний вплив (наприклад, стробоскопічні ефекти для виклику епілептичного нападу) спричинив шкоду здоров'ю, дії можуть бути кваліфіковані за статтями про умисне нанесення тілесних ушкоджень (Ст. 121, 122, 125 ККУ);

- у разі доведення до самогубства через психологічний тиск за допомогою зображень – Стаття 120 ККУ;

---

[5] Козюра В. Д., Хорошко В. О., Шелест М. Є., Ткач Ю. М., Усов Я. Ю. Комплексні системи захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. Ніжин : ФОП Лук'яненко В. В. ; ТПК «Орхідея», 2019. с. 129.

[6] Кримінальний кодекс України : Закон України від 05.04.2001 № 2341-III. *Відомості Верховної Ради України*. 2001. № 25–26. Ст. 131.

- терористичний акт (Стаття 258 ККУ), якщо такі дії мають на меті залякування населення або вплив на прийняття рішень органами влади, вони можуть розглядатися як форма кібертероризму.

Подальший аналіз Кримінального Кодексу України може показати, що в ньому не має прямих статтей, які можливі до застосування по відношенню до кіберправопорушника, який вчинив навмисний, злочинний вплив на оператора ЕОМ, застосовуючи специфічний (прихований) сигнал чи групу різних сигналів через системи інформаційних технологій на потерпілого та його психологічний стан.

Є статті 142, 356 КК України, де перша це незаконне проведення медико-біологічних, психологічних або інших дослідів над людиною, якщо це створювало небезпеку для її життя чи здоров'я, а друга це самоправство, тобто самовільне, всупереч установленому законом порядку, вчинення будь-яких дій, правомірність яких оспорюється окремим громадянином або підприємством, установою чи організацією, якщо такими діями була заподіяна значна шкода інтересам громадянина, державним чи громадським інтересам або інтересам власника.

Що у першому, що у другому випадку із вказаними вище статтями ККУ, вони не містять згадки та можливості впливу на потерпілого за допомогою інформаційних технологій, що унеможливлює її до застосування у разі використання таких технологій на психологічний стан особи.

Окрім того, за відсутності прямої статті в ККУ за протиправні дії кіберправопорушника, які розглядаються в цій роботі, виникають питання щодо збору, фіксації належних та допустимих доказів, які повинні повно, об'єктивно та всебічно вказати на застосування кіберправопорушником злочинного впливу на оператора ОЕМ.

Ще, окрім кримінальної відповідальності, існують суворі гігієнічні вимоги до роботи з моніторами, порушення яких роботодавцем може тягнути адміністративну відповідальність.

Ретельний аналіз змісту статей ККУ 121, 122, 125, 120, 142, 258(1-6), 356 напряму не підпадає під випадки, коли оператор ЕОМ під зовнішнім оптичним впливом починає порушувати правила роботи з комп'ютерними програмними продуктами, робити помилки та порушувати роботу комп'ютерної системи. Тоді, може й не існує негативний вплив зображення на моніторі на роботу оператора ЕОМ?

Для знаходження відповіді по даному питанню, дослідимо напрямки роботи передових колективів комп'ютерних лабораторій світового рівня. При цьому, застосуємо процес спілкування з системами штучного інтелекту.

3. Перелік і зміст роботи світових комп'ютерних лабораторій, які вивчають Penetration testing

Penetration testing (тестування на проникнення) – це санкціонована, контрольована імітація кібератак на ІТ-інфраструктуру, мережі чи програми.

При здійсненні пошуку інформації виявилося, що багато комп'ютерних спеціалістів у світових лабораторіях вже доволі давно та ретельно займаються вивченням ступеню впливу акустичних та оптичних сигналів, що передані по комп'ютерних мережах і відтворені моніторами та акустичними системами на робочих місцях операторів ЕОМ.

У цьому напрямку найбільший розвиток і опис досліджень отримали психолінгвістичні онлайн-експерименти.

Методи дослідження мовленнєвої діяльності сприйняття, засвоєння та вироблення мови, вчені проводять дистанційно через інтернет за допомогою веббраузерів, спеціалізованих платформ або онлайн-форм. Вони дозволяють науковцям збирати дані про роботу мозку при обробці мови («мовні» процеси), часто вимірюючи реакцію респондентів з точністю до мілісекунд.

Про експерименти з оптичним впливом зображень на стан операторів ЕОМ в інтернеті інформація оказалася дуже скудною і обмеженою. Однак, порівняння отриманої «фірмової» інформації зі «сторонньою» інформацію про експерименти в одних і тих же лабораторіях з високим ступенем вірогідності дозволяють спеціалістам (що працюють з ІзОД) зробити висновок, що ця інформація носить закритий характер.

Існують різноманітні типи лінгвістичних та оптичних психічних онлайн-експериментів:

1. Асоціативний експеримент, – виявлення асоціацій, що сформовані попереднім досвідом (наприклад, назвати перше слово, що спадає на думку у відповідь на стимул).

2. Завдання на лексичне рішення (Lexical Decision Task), – учасник на екрані монітора бачить набір букв і має швидко визначити, чи це реальне слово, чи вигадане.

3. Оцінка прийнятності (Acceptability/Grammaticality Judgment), – респонденти оцінюють, чи є речення граматично правильним або природним.

4. Самокероване читання (Self-paced Reading) – учасник читає текст, натискаючи клавішу, щоб побачити кожне наступне слово або фразу, що дозволяє виміряти час обробки кожного елемента.

5. Називання зображень (Picture-naming Task), – учасники бачать зображення і повинні швидко його назвати.

Онлайн-експерименти стали стандартом у дослідженнях мови, особливо після 2020 року, дозволяючи збирати великі масиви даних за допомогою веббраузерів (jsPsych, Labvanced, Gorilla).

4. Провідні дослідницькі центри вивчення дистанційного впливу на психіку оператора ЕОМ

LAELabs – Psycholinguistics Lab (**University of Hawaii**), – спеціалізується на віртуальних дослідженнях того, як мова виробляється, сприймається, розуміється та засвоюється.

Psycholinguistics@York (**University of York, Великобританія**), – проводить широкий спектр поведінкових онлайн-експериментів, у тому числі з використанням методів **eye-tracking** (!) у реальному часі.

Language & Cognitive Neuroscience Lab (**University of Wisconsin-Madison**), – досліджує статистичне навчання, вплив вироблення мови на розуміння та вплив соціолінгвістичних варіацій.

Psycholinguistics Lab (**University of Strathclyde, Великобританія**), – вивчає когнітивні механізми тобто сукупність психічних процесів (сприйняття, пам'ять, мислення, увага), за допомогою яких мозок отримує, обробляє, зберігає та використовує інформацію.

University of Edinburgh (**School of Philosophy, Psychology and Language Sciences**), – дослідники (наприклад, проф. Кенні Сміт) розробляють онлайн-методи (lexical decision tasks, mouse clicks) та навчають проведенню онлайн-експериментів.

University of Cambridge (**Language Sciences**), – активно займається психолінгвістичними дослідженнями, включаючи онлайн-платформи для мовних тестів.

The ELL Psycholinguistics Lab (**University of Wisconsin-Madison**), – використовує онлайн-інструменти для перехресних лінгвістичних досліджень (наприклад, Lexical Decision Task).

Дуже показовим є те, що дані експерименти відносяться до:

1. Когнітивної психології – вивчають, як люди отримують, обробляють, зберігають та використовують інформацію.

2. Психофізіології – вивчають фізіологічні механізми психічних процесів (емоцій, станів, сприйняття).

3.Психодіагностики – якщо це спрямовано на вимірювання та зміну психічного стану.

Ці процеси разом утворюють внутрішній світ людини або її психічну діяльність.

Мультимедійні дослідження дозволяють використовувати звук, **зображення та відео для стимуляції**.

Дуже цікавою є платформа Experiment Builder, що розроблена компанією SR Research Ltd., штаб-квартира якої розташована в Канаді.

Офіси та виробничі потужності компанії знаходяться в Оттава (Канада): головний офіс компанії, Міссісога (Онтаріо, Канада): місце реєстрації та розробки програмного забезпечення, що зазвичай вказується у правилах цитування софту.

Experiment Builder – це **візуальне середовище для створення психологічних та нейрофізіологічних експериментів**, яке найчастіше використовується разом з айтрекерами серії EyeLink, що також виробляються в Канаді. Також існує хмарний інструмент з подібною назвою – Gorilla Experiment Builder, який розроблений компанією Cauldron Science у Великій Британії (Кембридж), – відкіля отримати службову інформацію дуже важко, бо вона знаходиться під зміцненим контролем .

5. Створення та застосування тестерів, що фіксуюсь оптичний вплив на оператора ЕОМ для фіксації цифрових доказів кіберправопорушення

Нагадаємо, що цифрові докази є невід'ємною частиною кримінальних проваджень сьогодення, зокрема у справах, які стосуються сучасних технологій та кіберзлочинів. Ці докази включають цифрову інформацію, залишену на таких приладах як комп'ютери, мобільні пристрої, мережеві журнали та інші ресурси, які здатні відобразити дії суб'єкта або механізми, які можуть вплинути на середовище оператора ЕОМ.

У науковій літературі цифрові докази описуються як електронна інформація, отримана та закріплена таким чином, що її можна легально представити у кримінальному процесі для підтвердження певних обставин справи[7].

Процесуальні вимоги до доказів, у тому числі електронних, формуються під впливом норм Кримінального процесуального кодексу України, які вимагають суворого забезпечення їх належності та достовірності. Саме тому технічно правильне вилучення інформації напряму впливає на можливість її використання у суді.

Правильне трактування цифрових доказів у кримінальному провадженні вимагає глибокого розуміння їх правового статусу та допустимості. У національній практиці тривають дискусії щодо допустимих меж втручання у приватне життя, порядку отримання інформації з віддалених сервісів, а також щодо можливості використання копій замість оригінальних джерел[8].

Як приклад оптичного впливу візуальних образів, з якими може зустрітися людина у житті, можна назвати лікувальний (або кримінальний…) гіпнотичний вплив на поведінку людини частини візуальних елементів такої науки як «Нейро-Лінгвістичне Програмування» (NLP), що є набором психологічних технік, які дозволяють впливати на думки і поведінку людей, змінюючи її не тільки тут та зараз, а й на майбутні моменти життя.

NLP це дистанційно-контактне програмування підсвідомості для зміни поведінки людини за допомогою мови та вербальних сигналів (в оптичному диапазоні): жестів, міміки… . Зрозуміло, що керуючі сигнали кожна людина по-своєму отримує і розуміє інформацію з каналу звуку та каналу зору. І тут очі є не тільки першим «функціональним блоком» на шляху прийому відео-інформації, але й дуже якісним індикатором зовнішнього впливу, що дозволяє контролювати і програмувати стан підсвідомості людини.

Ремарка 1. Таким чином, проміжним висновком є першим функціональним елементом, що дозволяє контролювати психологічний стан підсвідомості оператора ЕОМ, фіксуючи звичайну швидкість та напрями рухів патерн очей («очних яблук») оператора. Як було наведено раніше, для цього можуть бути застосовані:

---

[7] Електронне наукове видання «Аналітично-порівняльне правознавство». URL: http://journal-app.uzhnu.edu.ua/article/view/334687

[8] Сутність цифрових доказів і проблеми їх використання у кримінальному провадженні. URL: https://dspace.nlu.edu.ua/handle/123456789/20503

1. Стаціонарні айтрекери що розміщуються під монітором комп'ютера.

2. Айтрекери-окуляри (мобільні).

3. Веб-камери. Вони дозволяють проводити масові дистанційні дослідження, але з нижчою точністю.

В схожій науці дистанційного нейрокольороводинамічного програмування **(NCDP)** підсвідомості людини – в основу покладено наявність нейрон-фізіологічного зв'язку між впливом (причиною) навколишнього фону (наприклад, – непомітна зміна динаміки та кольорового змісту зображення на екрані комп'ютерного монітору) на підсвідомій зміні поведінки (дій) та/або стані людини.

Безліч психологічних характеристик сигналів для дистанційного програмування поведінки людей описуються по-різному. Далі ми торкнемося такої спектральної характеристиці сигналів, як довжина хвилі світла, що попадає на сітківку очей людини. Звісно, що диференціальні компоненти кольору джерела світла впливають на очі людини. Причому, на відміну від роботи Gabriel Kreiman, що спирається у своїх міркуваннях на відбите від предметів світло, а саме: «…Світло потрапляє на сітківку після того, як відбивається об'єктами довкілля…»[9], – ми звернемо увагу на інше джерело, яке на нашу думку має здібність дистанційно впливати та змінювати поведінку людини. Реально, – це групи фотонів з екранів моніторів, світлодіодних матриць, різноманітних сканерів, проекторів та й т. ін., що безпосередньо «породжуються» самим джерелом випромінювання і «відсвітлюють» предмети оточуючого середовища.

Наприклад, колір екрану монітору комп'ютера, з яким ми працюємо кожен день , звичай має більш сотні відтінків – від білого, світло-сірого до темного. І на тлі тих кольорів ми бачимо малюнки, тексти і багато чого іншого (Рис. 2). І всі ті відтінки на Рис. 2 визначені зазвичай як – «білий, світлий».

Світлова інформація досягає ока через лінзу кришталика (Рис. 3). Коли світло досягає фокальної площини, що збігається з положенням сітківки, зображення перевертається (на 180°). Сітківка є частиною центральної нервової системи: вона походить з тих же ембріональних структур, які дають початок решті мозку, і вона має гематоенцефалічний бар'єр, аналогічний такому ж як у решти мозку.

Світло проходить через безліч клітин ока і потрапляє на фоторецептори: палички та колбочки. Загалом у людини близько 10^{8} паличок та 10^{7} колбочок.

Палички дуже чутливі до світла та призначені для уловлювання фотонів в умовах низького освітлення. Нічне бачення залежить від паличок. Палички можуть захоплювати одиночний фотон видимої частини спектру, енергія якого становить лише близько 10^{-19} Дж, і передавати його енергію далі. Доказано, що люди можуть реєструвати одиночні фотони[10].

[9] Крейман Г. Біологічний та комп'ютерний зір / пер. з англ. И. Л. Люско ; під ред. Т. Б. Кіселевої. Москва : ДМК Пресс, 2022. 314 с.

[10] Там само.

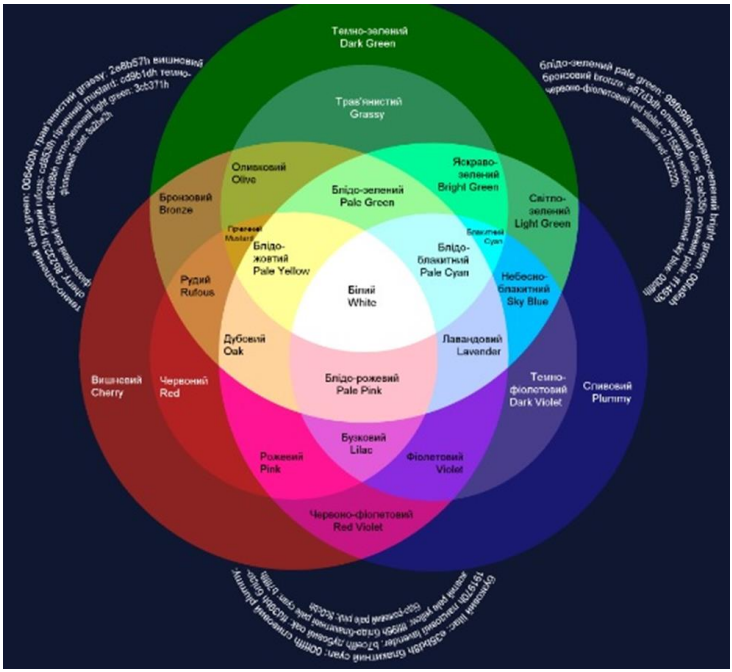


Рис. 2. Біла пляма в центрі, є інтегральним результатом реакції мозку на стимуляцію нейронів фотонами різних довжин хвиль [поширено в Інтернеті]

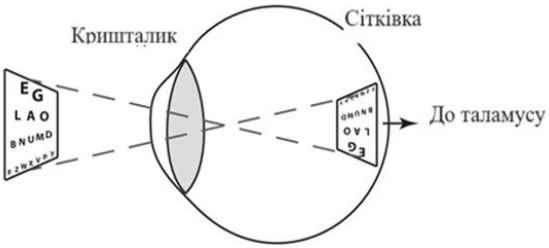


Рис. 3. Деякі функціональні елементи ока людини

У більшості людей є три типи колбочок: – довгохвильові, чутливі до довжини хвилі світла з максимумом 560 нм (жовто-зелений колір); – середньохвильові, чутливі до діапазону з максимумом 530 нм (зелений колір); – короткохвильові, чутливі до діапазону з максимумом 420 нм (фіолетовий колір). Колірний зір залежить від активності колбочок[11]».

Розуміючи схожість нейрофізіологічних зв'язків **NLP** та **NCDP** має сенс показати схожості у вигляді функціоналів, як це наведено на Рис. 4.

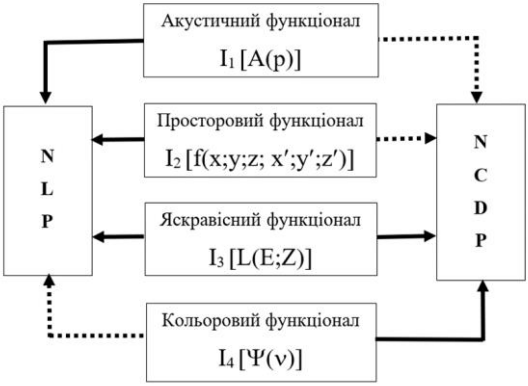


Рис. 4. Задіяність функціоналів в NLP та NCDP

Зорові нейрони тримають під контролем певну область поля зору, в якій, як доказує експеримент, вони **реагують ще на щось крім зміни візерунків**, руху предметів, та їх яскравості. Як ми розуміємо, це реакція нейронів на будь-які зміни у спектральному складі світлового потоку, що впливає на них, тобто йдеться про реакцію на динаміку змін у спектральному складі випромінювання що впливає на нейрони сітківки.

Таким чином, ретельно вивчаючи роботу Gabriel Kreiman, можна виявити, що зір людини працює не тільки на стимулюючи елементи впливу в NLP.

Зафіксовано, що нейрони головного мозку, гангліозні клітини сітківки, під час експерименту з фіксацією активності нейронів «ніби так» видають у мозок якісь сигнали, які при незнанні подразника можна класифікувати як випадкові. Ці «безпричинні» сигнали виробляються настільки часто, що їх стали ігнорувати, розмовляючи про випадкові імпульси від збудника (подразника) невідомого походження.

Іншими словами, «якщо порівняти нейрон з пороговим пристроєм, його спрацьовування не обов'язково відсутнє за відсутності зорової просторової стимуляції в межах рецептивного поля…»[12].

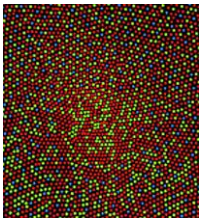
[11] Крейман Г. Біологічний та комп'ютерний зір / пер. з англ. И. Л. Люско ; під ред. Т. Б. Кіселевої. Москва : ДМК Пресс, 2022. 314 с.

[12] Там само.

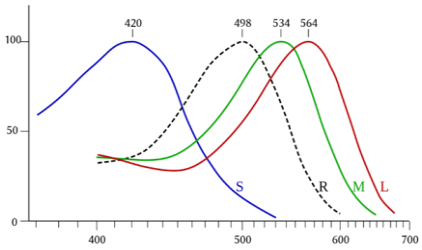
На превеликий жаль, сучасні технології дозволяють одночасно реєструвати діяльність лише кількох сотень вихідних нейронів сітківки, але й така кількість підконтрольних нейронів доказує реальну можливість здійснення **NCDP**.

6. Вплив компонентів білого кольору на психічний стан оператора ЕОМ через підсвідомість мозку

Таким чином знаючи, що, колбочки відповідальні за кольоровий зір, звернемо увагу на їх розташування на сітківці здорової людини (Рис. 5)[13].



а) Розташування в фоторецепторних клітин



б) Чутливість фоторецепторних клітин

Рис. 5. Розподіл колбочкових клітин у центральній ямці сітківки ока людини з нормальним колірним зором

Основна небезпека для людини зберігається у суміші кольорів що надають оператору ЕОМ відчуття білого екрана на тлі якого розміщують інформацію різного конфіденційного змісту – тексти, таблиці та ін. (Рис. 6).

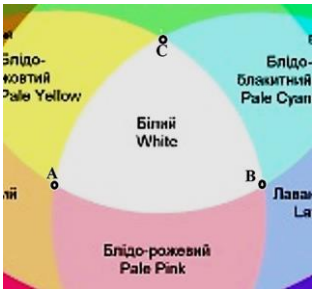


Рис. 6. «Вирізка» білої ділянки з Рис. 2

Якщо в процесі роботи правопорушник отримає можливість (а таких місць на протязі комп'ютерної мережі мінімум чотири) навмисно змінювати насиченість білої ділянки ABC, варіюючи кількість та розташування на екрані монітору

[13] Сітківка. Вікіпедія. URL: https://uk.wikipedia.org/wiki/сітківка

кольорових компонентів білого «кольору», то незалежно від бажання оператора ЕОМ та його психічного настрою, нейрони будуть постачати оператору у головний мозок інформацію, як мінімум, – о насиченості білої ділянки червоним, синім та зеленим світлом, бо в інтегральному ракурсі ця біла пляма (фон екрана) має непримітне для очей «мерехтіння». Оператор ЕОМ підсвідомо буде знаходитись під впливом комп'ютерних зображень фону екрана.

Ремарка 2. Доволі ефективні та корисні прилади застосовує в цьому напрямі фірма Optopol[14], що вивчає та лікує зір людини. Сучасний автоматичний комп`ютерний «периметрометр» використовується офтальмологом для визначення полів зору і перевірки порогової чутливості сітківки ока. Периметрія – це інструментальний метод діагностики в офтальмології, який дозволяє визначати межі полів зору і найменше їх відхилення від встановлених норм на самих ранніх стадіях, а також зафіксувати результати у вигляді діаграм, графіків та трьохвимірного зображення. Образи, що створюються на апаратурі фірми Optopol, застосовують об`єкти різного розміру та яскравості, тобто застосовується тільки просторовий і яскравісний функціонали **NCDP**.

ВИСНОВКИ

Проведене дослідження показало наступне.

1. У Кримінальному Кодексі України покарання кіберправопорушників за дії що спрямовані на негативний дистанційний вплив загроз на персонал, – оператора ЕОМ, адміністраторів та ін. – розглядаються лише побічно.
2. Прилади щодо фіксації та збору цифрових доказів такого роду кіберправопорушень знаходяться в стані розробки багатьма ведучими фірмами в системи кібербезпеки і охороняються та зберігаються на рівні ІзОД.
3. Кіберправопорушник має можливість не тільки змінювати фон в інтегральному розумінні цього процесу, але в диференціальному ракурсі має можливість створювати непомітні для зору, але-ж суттєві для підсвідомості, динамічні образи (і відео-елементи, які можуть бути корельованими з конкретними життєвими «сюжетами» оператора), що дозволяє дистанційно впливати на поведінкові реакції персоналу ЕОМ.
4. Створення тестерів для проведення тестінгу на проникнення одночасно з функціями виявлення, фіксації та збору цифрових доказів кіберправопорушень є актуальною задачею професіоналів системи кібербезпеки.

АНОТАЦІЯ

У статті досліджуються механізми прихованого дистанційного впливу на психофізіологічний стан оператора ЕОМ через оптичні та акустичні сигнали. Проаналізовано стан сучасної нормативно-правової бази України щодо кваліфікації таких дій як кіберзлочини та визначено відсутність прямих норм, які б могли описати покарання за навмисний візуальний вплив на здоров'я людини.

Розглядається концепція дистанційного нейрокольороводинамічного програмування (NDCP) підсвідомості, що базується на нейрофізіологічному

[14] Optopol Technology. URL: https://optopol.com/

зв'язку між спектральним складом випромінювання екрана та зміною поведінкових реакцій людини. Описано роль фоторецепторів сітківки у сприйнятті поодиноких фотонів та динамічних змін фону екрана, які можуть бути непомітними для свідомості, але суттєвими для підсвідомості.

Окрему роль приділено світовому досвіду проведення психолінгвістичних експериментів та використанню технологій eye-tracking для фіксації змін у стані оператора. Обґрунтовано актуальність створення спеціалізованих тестерів для виявлення та збору цифрових доказів таких правопорушень у системах кібербезпеки.

ABSTRACT

The article explores the mechanisms of covert remote influence on the psychophysiological state of a computer operator through optical and acoustic signals. The current state of Ukraine's regulatory and legal framework regarding the classification of such actions as cybercrimes is analyzed, identifying a lack of direct norms that could describe the punishment for intentional visual impact on human health.

The concept of remote Neuro-Color-Dynamic Programming (NCDP) of the subconscious is examined, based on the neurophysiological connection between the spectral composition of screen radiation and changes in human behavioral reactions. The role of retinal photoreceptors in perceiving single photons and dynamic changes in the screen background, which may be invisible to the conscious mind but significant for the subconscious, is described.

Special attention is paid to global experience in conducting psycholinguistic experiments and the use of eye-tracking technologies to record changes in the operator's state. The urgency of creating specialized testers for detecting and collecting digital evidence of such offenses within cybersecurity systems is justified.

Література

1. How much time do we spend on social media? *Mediakix*. 2016. URL: http://mediakix.com/2016/12/how-much-time-is-spent-on-social-media-lifetime/ #gs.rPNYGG8.

2. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР.

3. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII.

4. Про інформацію : Закон України від 02.10.1992 № 2657-XII.

5. Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX.

6. Козюра В. Д., Хорошко В. О., Шелест М. Є., Ткач Ю. М., Усов Я. Ю. Комплексні системи захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. Ніжин : ФОП Лук'яненко В. В. ; ТПК «Орхідея», 2019. 144 с.

7. Кримінальний кодекс України : Закон України від 05.04.2001 № 2341-III. *Відомості Верховної Ради України.* 2001. № 25–26. Ст. 131.

8. Електронне наукове видання «Аналітично-порівняльне правознавство». URL: http://journal-app.uzhnu.edu.ua/article/view/334687.

9. Сутність цифрових доказів і проблеми їх використання у кримінальному провадженні. URL: https://dspace.nlu.edu.ua/handle/123456789/20503.
10. Крейман Г. Біологічний та комп'ютерний зір / пер. з англ. И. Л. Люско ; під ред. Т. Б. Кіселевої. Москва : ДМК Пресс, 2022. 314 с..
11. Сітківка. Вікіпедія. URL: https://uk.wikipedia.org/wiki/сітківка.
12. Optopol Technology. URL: https://optopol.com/.
13. Гавриленко Є. В. NCDP – neurocolordynamic programming. Ricerche scientifiche e metodi della loro realizzazione: esperienza mondiale e realtà domestiche : raccolta di articoli scientifici «ΛΌΓΟΣ» con gli atti della VIII Conferenza scientifica e pratica internazionale (Bologna, 19 Dec. 2025). Bologna ; Vinnytsia, 2025. С. 138–146. DOI: 10.36074/logos-19.12.2025.025.

Information about the authors:
Gavrylenko Yeva Vladyslavivna,
Software Engineer – Bachelor's Degree of the Educational and Research Institute Computer Sciences and Artificial Intelligence of Department of Security of Information Systems, Networks & Technologies,
V.N. Karazin Kharkiv National University
6, Svobody Sq., Kharkiv, 61022, Ukraine

Sakhanchuk Andrii Dmytrovych,
Attorney in criminal law and procedure
Chairman of the Law Firm, Kyiv, Ukraine

Sakhanchuk Tetiana Ihoryvna,
Attorney at law, Kyiv, Ukraine