Міністерство освіти і науки України
Кам’янець-Подільський національний університет імені Івана Огієнка
Фізико-математичний факультет
Кафедра комп’ютерних наук

Дипломна робота
магістра

з теми: **“РОЗРОБКА МЕТОДУ ВИЯВЛЕННЯ ДЕСТРУКТИВНОГО ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОГО ВПЛИВУ В СОЦІОТЕХНІЧНИХ СИСТЕМАХ”**

Виконала: студентка групи KN1-M22
спеціальності 122 Комп’ютерні науки
Войцехівська Олександра Віталіївна

Керівник: **Моцик Р.В.,**
доцент кафедри комп’терних наук,
кандидат педагогічних наук, доцент

Кам’янець-Подільський – 2023

ЗМІСТ

ВСТУП

В сучасному світі інформаційних технологій соціотехнічні системи стали необхідною складовою нашого повсякденного життя. Вони об'єднують технології та суспільство, створюючи екосистеми, в яких інформація та взаємодія відіграють ключову роль. Однак разом із неймовірними можливостями, які надають соціотехнічні системи, приходить і загроза деструктивного інформаційно-психологічного впливу.

Деструктивний вплив може приймати різні форми, включаючи дезінформацію, фішинг, кібератаки, маніпуляцію громадською думкою та багато інших. Він може завдавати шкоду як окремим користувачам, так і суспільству в цілому, порушуючи приватність, розкриваючи конфіденційну інформацію та психологічно впливаючи на нашу поведінку та переконання.

Саме тому розробка методу виявлення деструктивного інформаційно-психологічного впливу в соціотехнічних системах стає актуальною і важливою проблемою. Ця тема об'єднує інформаційні технології, психологію та кібербезпеку в спробі розробити ефективні методи виявлення та захисту від деструктивного впливу.

У нашому дослідженні ми ставимо за мету розкрити сутність деструктивного впливу в соціотехнічних системах, вивчити психологічні аспекти цього явища та розробити методологію та інструменти для виявлення і запобігання його наслідкам. Наша робота спрямована на створення безпечних та стійких соціотехнічних систем, де користувачі можуть вільно спілкуватися та обмінюватися інформацією без страху перед деструктивними загрозами.

Подальше дослідження цієї теми має потенціал впливати на розвиток кібербезпеки, психологічної науки та суспільства в цілому, роблячи інформаційні технології безпечнішими та надійнішими для всіх користувачів.

Тема нашого дослідження: "Розробка методу виявлення деструктивного інформаційно-психологічного впливу в соціотехнічних системах" є досить

актуальною і важливою в сучасному світі, особливо з відкриттям нових можливостей для впливу на суспільство за допомогою інформаційних технологій.

Розробка методу виявлення деструктивного інформаційно-психологічного впливу в соціотехнічних системах є актуальною темою сьогодення, оскільки вона стосується різних сфер життя і може мати велике значення для захисту інформаційної безпеки, захисту від маніпуляцій та покращення психологічного здоров'я користувачів.

Метою дослідження є розробка ефективного методу виявлення деструктивного інформаційно-психологічного впливу в соціотехнічних системах з метою захисту користувачів та суспільства від негативних наслідків цього впливу.

Завдання дослідження:

1. Аналіз основних видів деструктивного інформаційно-психологічного впливу.
2. Дослідження методології виявлення видів деструктивного інформаційно-психологічного впливу в соціотехнічних системах.
3. Аналіз алгоритмів та програмних засобів для виявлення деструктивного впливу на основі дослідженої методології.
4. Розробка методу виявлення деструктивного інформаційно-психологічного впливу в соціотехнічних системах.

Ці завдання спрямовані на досягнення загальної мети - створення ефективного методу виявлення деструктивного впливу в соціотехнічних системах і забезпечення захисту суспільства від цього впливу.

Об'єкт дослідження. Соціотехнічні системи. Соціотехнічні системи включають в себе комплекс взаємодій між технічними елементами (наприклад, інформаційні технології, платформи, соціальні мережі) і людьми, що використовують ці технології.

Предмет дослідження. Дослідження методу виявлення деструктивного інформаційно-психологічного впливу в соціотехнічних системах.

Апробація результатів дослідження. Результати дослідження були оприлюднені на звітній науковій конференції студентів та магістрів за підсумками науково дослідної роботи у 2022-2023 навчальному році та публікаціях: .

Структура роботи. Магістерська робота складається із вступу, трьох розділів, висновків, списку використаних джерел.

РОЗДІЛ 1. АНАЛІЗ ПОНЯТТЯ «ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИЙ ВПЛИВ» В СОЦІОТЕХНІЧНИХ СИСТЕМАХ

1.1. Аналіз понять «психологічний» вплив та «інформаційний вплив»

Концепція деструктивного психологічно-інформаційного впливу стала актуальною в епоху зростання використання масових комунікаційних технологій, зокрема телебачення та радіо. Одним із перших науковців, які акцентували увагу на негативних аспектах впливу масових медіа на психіку та суспільство, був Клод Шеннон, американський математик та інженер.

У 1948 році, Шеннон разом із Варреном Вівером опублікував статтю "Математична теорія зв'язку", де вони вперше формалізували ідеї зв'язку та інформації. Це дало початок теорії інформації, яка була важливою для розвитку масових комунікаційних технологій.

Інший важливий вчений, Маршалл Маклюен, в середині 20-го століття досліджував вплив технологій на суспільство та культуру. У своїй книзі "Зрозуміти медіа: Зовнішні розширення людини" (Understanding Media: The Extensions of Man), він висловлював погляди на те, як розвиток технологій, зокрема телебачення, може впливати на сприйняття світу та взаємодію людей.

Ці та інші науковці зробили важливий внесок у розуміння того, як інформація та масові комунікаційні засоби можуть мати деструктивний вплив на психіку та суспільство. Тема цього впливу продовжує розвиватися і в сучасному дослідженні медіа та інформаційних технологій.

Проаналізуємо поняття "психологічний вплив" і "інформаційний вплив". Проведемо аналіз їх впливу на мислення, поведінку та переконання людей через психологічні і інформаційні методи. Ось короткий огляд цих понять:

Психологічний вплив:

Психологічний вплив включає в себе використання психологічних прийомів та технік для зміни думок, переконань або поведінки людини. Це

може бути використано для переконування, мотивації, маніпуляції або психологічного впливу на особистість.

Приклади психологічного впливу (Рисунок 1.1) включають в себе використання емоційного впливу, авторитету, соціальної норми, психологічного тиску тощо.

Рисунок 1.1 – Структура психологічного впливу

Психологічний вплив може бути використаний в різних сферах, включаючи рекламу, політику, маркетинг, виховання тощо.

Інформаційний вплив:

Інформаційний вплив використовується для впливу на особистість або суспільство через розповсюдження певної інформації або повідомлень. Це може включати в себе поширення новин, даних, фактів, аргументів або брехні з метою вплинути на думки або переконання людей.

Приклади інформаційного впливу включають в себе пропаганду, рекламу, медіа-маніпуляції, публічні виступи, спілкування в соціальних мережах тощо. Інформаційний вплив може бути важливим інструментом для формування громадської думки, впливу на політичні процеси, зміни споживчого підходу, впливу на вибори та багато інших сфер.

Обидва ці види впливу важливі і досліджуються в багатьох галузях, включаючи психологію, комунікаційну науку, політологію, маркетинг та інші.

Розуміння їхньої природи та ефективних методів захисту від негативного впливу має важливе значення для захисту прав та інтересів людей і суспільства в цілому.

В наукових працях виділено основні психологічні аспекти впливу через інформацію, а саме:[1, ст.13-18, 7, ст. 45-50]

- емоційний вплив. Інформація може викликати емоційну реакцію у людини. Новини, фотографії, відео та інші медійні вміст можуть викликати радість, гнів, смуток, страх. Емоційний вплив інформації може вплинути на рішення та дії людини.

Когнітивний вплив —це інформація яка може впливати на когнітивні процеси людини, такі як сприйняття, пам'ять і мислення. Люди обробляють інформацію, формують переконання та роблять рішення на основі того, як вони сприймають та розуміють інформацію.

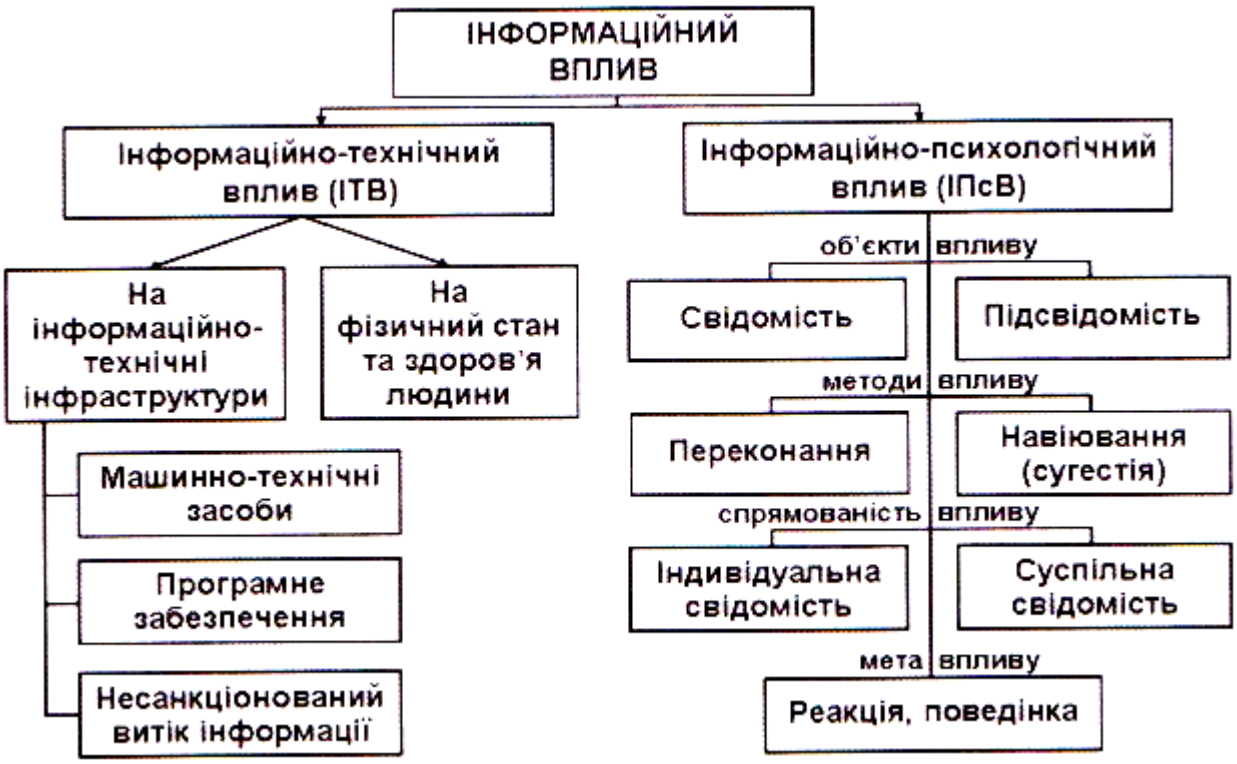
- переконання і вплив на думки. Інформація може вплинути на формування переконань та усвідомлення людиною своєї точки зору. Це може включати в себе переконувальні техніки, логічні аргументи та вплив на переконання.

- вплив на соціальну норму. Інформація може впливати на сприйняття соціальних норм та цінностей. Вона може відображати те, як інші люди реагують на певні ситуації або події і, таким чином, формувати соціальну норму.

- маніпуляція та психологічний тиск. Деякі інформаційні техніки можуть використовувати психологічний тиск та маніпуляцію для досягнення певних цілей. Це може включати в себе використання психологічних трюків для впливу на поведінку.

Психологічні аспекти впливу на людину через інформацію дуже важливі, оскільки вони впливають на сприйняття та реакцію людей на різні повідомлення, медійний контент та інші джерела інформації. Розуміння цих аспектів дозволяє аналізувати та критично ставитися до інформації, що має важливе значення в сучасному інформаційному середовищі.

Вплив на людину через інформацію має численні психологічні аспекти, оскільки інформація може впливати на мислення, емоції, поведінку та



переконання людей.

Рисунок 1.2 – Структура інформаційного впливу

Проаналізуємо механізми деструктивного впливу.

Деструктивний вплив – це вплив, спрямований на завдання шкоди, виснаження, зміни або нанесення шкоди індивіду, групі, суспільству або системі. Цей вплив може бути використаний з різних мотивів і в різних сферах життя. У публікаціях (дослідженнях, статтях з проблеми дослідження) науковців [1, ст. 36-40] [7, ст. 20-26] проводиться аналіз базових видів дезінформацій, а саме:

- дезінформація. Поширення неправдивої або маніпулятивної інформації з метою змінити думки, переконання або поведінку. Це може включати в себе фейкові новини, спекуляції, чутки та інші форми дезінформації.
- маніпуляція емоціями. Використання інформації для виклику певних емоцій, таких як страх, гнів або обурення, для маніпуляції поведінкою або думками людей.
- психологічний тиск. Використання психологічного тиску, наприклад, шантажу, інтимного впливу або психологічних методів впливу для досягнення певних цілей.
- соціальний вплив. Використання соціального статусу, авторитету або відомостей про соціальні зв'язки для нанесення шкоди або впливу на інших.
- психологічний тиску групи. Використання групового тиску, стигматизації або виключення з групи для впливу на інших членів групи.
- використання інформаційних технологій. Використання інформаційних технологій, таких як соціальні мережі, для поширення деструктивної інформації або для кібербулінгу.
- психологічне та фізичне насильство. Використання психологічного або фізичного насильства для досягнення певних цілей або для завдання шкоди іншим.

- психологічна маніпуляція. Використання психологічних технік для зміни переконань, ставлення або поведінки інших без їхньої належної свідомості.

Механізми деструктивного впливу можуть виявлятися в різних ситуаціях і сферах життя, і їх розуміння важливо для захисту від негативних наслідків такого впливу та для підвищення свідомості про можливі загрози.

1.2. Соціотехнічні системи їх сутність та взаємодія

Дослідження соціотехнічних систем виникли в контексті розвитку інформаційних технологій та їх впливу на суспільство. Один із піонерів у цій області - Ендрю Філдінг (Andrew Fielding) - був англійським інженером та соціологом.

У 1956 році Філдінг опублікував статтю "Соціотехнічні системи", в якій він розглядав взаємодію між технічними та соціальними аспектами систем. Він аналізував, як технічні засоби і системи впливають на людей та їх соціальне оточення, а також як соціальні чинники можуть впливати на розвиток технічних систем.

Спроби розуміти соціотехнічні аспекти виникали також в інших областях. Наприклад, в рамках кібернетики та системного підходу до управління, де науковці досліджували взаємодію між технічними та соціальними системами.

Спеціальна область досліджень, присвячена соціотехнічним системам, розвивалася далі, і сучасні дослідження у цьому напрямку включають в себе аспекти якісного та кількісного аналізу взаємодії між технічними та соціальними елементами в різних контекстах, таких як розробка технологій, використання інформаційних систем та інші соціально-технічні аспекти.

Соціотехнічні системи мають таку назву, оскільки вони поєднують в собі як соціальні, так і технічні аспекти. Такі системи включають в себе технології, які взаємодіють з користувачами та впливають на їхню поведінку, а також

соціальні структури та взаємодії, що розвиваються в цьому технологічному контексті.

З кількох причин соціальнотехнічні системи називають "соціо", а саме:

- Інтеграція технології та суспільства. Соціотехнічні системи об'єднують технологію та суспільство, і вони взаємозалежні. Технологія впливає на спосіб, як суспільство взаємодіє та функціонує, і навпаки.
- Робота з користувачами. У соціотехнічних системах важливо розуміти, як користувачі взаємодіють з технологією та як технологія впливає на їхню поведінку та переконання. Це враховує соціальний аспект.
- Врахування соціальних наслідків. Створення та використання технологій має соціальні наслідки, такі як приватність, безпека, власність, етика та інші аспекти, які потребують соціального аналізу та регулювання.
- Комунікація та взаємодія. Соціотехнічні системи включають в себе комунікаційні процеси та взаємодії між людьми, користувачами та технологіями.
- Вплив на суспільство. Технології та соціотехнічні системи можуть мати значний вплив на суспільство, змінюючи спосіб життя, роботу, культуру та взаємовідносини між людьми.

У підсумку, термін "соціотехнічні системи" відображає важливу взаємодію між соціальними та технічними аспектами систем, що виникають при розвитку і використанні інформаційних технологій.

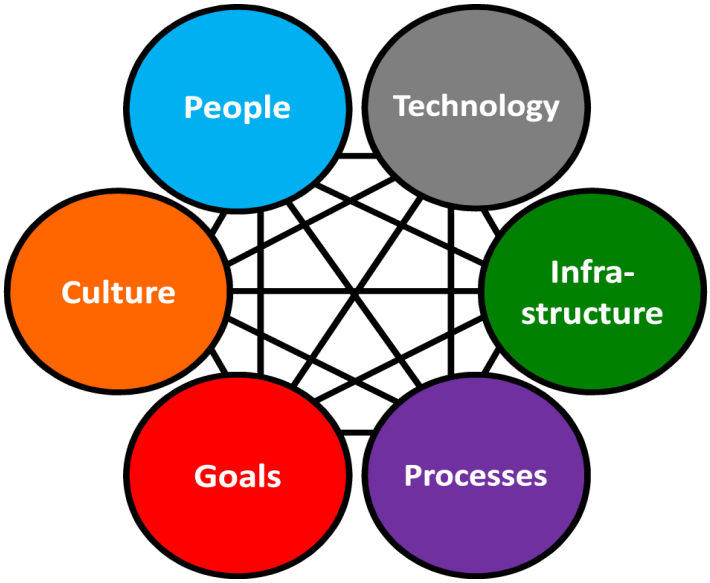


Рисунок 1.3– Структура соціотехнічних систем

Соціотехнічні системи - це складні системи, які об'єднують технічні та соціальні аспекти. Вони включають в себе взаємодію між технічними елементами (наприклад, комп'ютери, програмне забезпечення, технології) і людьми, які використовують ці технічні рішення. Сутність соціотехнічних систем розглянуто фахівцями в багатьох статтях. [2, ст. 3] [6, ст. 5]

Соціотехнічні системи можуть бути знайдені в різних сферах життя, включаючи бізнес, організації, освіту, медицину, технології та інші галузі. Розуміння їх сутності важливо для розробки та використання ефективних технологій та систем, які відповідають потребам користувачів і суспільства в цілому.

1.3. Роль і вплив інформації в соціотехнічних системах

Сьогодні багато сфер суспільства та технологій залежить від інформації.

Зрозуміння ролі та впливу інформації в соціотехнічних системах допомагає суспільству та фахівцям в галузі інформаційних технологій ефективно використовувати ці ресурси для поліпшення життя та розвитку суспільства.

Роль і вплив інформації в соціотехнічних системах надзвичайно важливі і впливають на сучасне життя. Ось деякі основні елементи, які відіграють важливу роль у соціотехнічних системах на думку науковців [2, ст. 4] [6, ст. 2]

- засіб комунікації. Інформація служить як засіб комунікації між людьми в соціотехнічних системах. Інформаційні технології, такі як соціальні мережі, електронна пошта, месенджери, дозволяють спілкуватися та обмінюватися даними.
- формування думок та переконань. Інформація впливає на формування думок, переконань і ставлення людей до різних питань. Медійний

контент, новини, реклама та інші джерела інформації можуть впливати на сприйняття світу та прийняття рішень.

- психологічний вплив. Інформація може викликати емоційну реакцію у людини. Різні види інформації можуть викликати радість, гнів, страх, смуток або інші емоції.
- вплив на поведінку. Інформація може впливати на поведінку людей. Наприклад, реклама може спонукати до покупки продукту, а соціальні мережі можуть впливати на активність користувачів.
- вплив на соціальні норми. Інформація може сприяти зміні соціальних норм та цінностей. Вона може відображати те, як інші люди реагують на певні ситуації або події, і, таким чином, впливати на соціальну норму.
- важливість прийняття рішень. Інформація є ключовим фактором для прийняття рішень в різних сферах життя, від бізнесу і освіти до медицини і політики.
- використання в різних галузях. Інформація використовується в різних галузях, таких як бізнес, наука, медицина, освіта, розваги та інші. Вона є основою для розвитку нових технологій, інновацій та розв'язання різних завдань.
- важливість захисту інформації. З огляду на важливість інформації, її захист є критичним аспектом в соціотехнічних системах. Це включає в себе заходи для забезпечення конфіденційності, цілісності та доступності даних.

Загалом, інформація відіграє ключову роль в соціотех нічних системах і має великий вплив на сучасне суспільство. Вона формує спосіб, яким ми сприймаємо світ, взаємодіємо один з одним та приймаємо рішення. Розуміння ролі та впливу інформації допомагає ефективно використовувати технології та системи, а також розробляти заходи для захисту прав та інтересів людей у цифровому віці

Проте важливо також бути обережними та критичними щодо інформації, яку ми споживаємо, оскільки інформація може бути використана для маніпуляції, дезінформації або навіть для завдання шкоди. Здатність критично оцінювати інформацію та розрізняти достовірність важлива для збереження інформаційної грамотності та цифрової безпеки.

Фахівці з цифрової безпеки надають рекомендації до соціотехнічних систем. Рекомендації для соціотехнічних систем, які мають справу з детектуванням деструктивних інформаційно-психологічних впливів [7, ст. 45]

1) Розробка методології дослідження. Розробіть методологію, яка дозволить аналізувати і виявляти деструктивний вплив в соціотехнічних системах. Визначте ключові показники та критерії для оцінки такого впливу;

2) Розвинення алгоритмів та моделей. Розробіть алгоритми та моделі, які дозволять виявляти аномалії в інформаційних потоках та поведінці користувачів, які можуть свідчити про деструктивний вплив;

3) Моніторинг та аналіз. Забезпечте постійний моніторинг і аналіз інформаційних потоків та даних, щоб вчасно виявляти загрози та аномалії;

4) Розробка систем попередження. Розробіть системи попередження та реагування на деструктивний вплив, які дозволять вживати заходи щодо обмеження шкоди та відновлення системи.

5) Психологічна підготовка та підтримка. Забезпечте психологічну підготовку та підтримку для персоналу, який працює з інформаційними системами та може бути вразливим до деструктивного впливу.

6) Взаємодія з користувачами. Залучайте користувачів до процесу виявлення та реагування на деструктивний вплив, створюючи механізми зворотного зв'язку та звітування;

7) Етичні стандарти. Розробіть і впровадьте етичні стандарти для обробки інформації та впливу на користувачів, зокрема враховуючи психологічні аспекти.

8) Законодавча відповідність. Дотримуйтесь відповідних законодавчих норм та вимог щодо захисту приватності та інформаційної безпеки.

9) Дослідження та аналітика. Проводьте наукові дослідження та аналіз впливу на соціотехнічні системи, щоб постійно вдосконалювати методи виявлення та захисту;

10) Глобальний підхід. Розглядайте деструктивний вплив як глобальний виклик, який вимагає співпраці та координації на різних рівнях та в різних галузях

Ці поради зможуть ефективно захистити соціотехнічних системи від деструктивних факторів, підвищивши їхню безпеку та стійкість.

1.4. Деструктивний психологічний інформаційних вплив

Питання деструктивного психологічного інформаційного впливу досліджувалося в різні періоди часу та контексти різними дослідниками. Однак важливо відзначити, що деякі аспекти цієї проблематики досліджувалися ще до появи терміну "деструктивний психологічний інформаційний вплив".

Фахівці з інформаційної безпеки дослідили в своїх працях основні аспекти цієї проблеми, а саме: [3, ст. 34-41] [4, ст. 12-15]

– пропаганда військових конфліктів. У різні часи історії деструктивний психологічний вплив досліджувався у контексті військових конфліктів, де пропаганда використовувалася для маніпулювання масовою свідомістю та створення негативних стереотипів.

– теорія масового сприйняття. Класичні дослідження в галузі комунікацій, такі як теорія масового сприйняття, вивчали, як повідомлення впливають на психологічні аспекти індивіда та суспільства.

– дослідження соціальної психології. Соціальні психологи вивчають вплив соціальних чинників на психіку людини, включаючи вплив інформації на ставлення, переконання та поведінку.

– дослідження в області медіакомунікацій. Дослідження в області медіакомунікацій вивчають вплив різних типів інформації, включаючи масові медіа, на сприйняття та психічний стан споживачів.

– інтернет та соціальні мережі. Останнім часом вивчається вплив деструктивної інформації в онлайн-середовищі, зокрема у контексті фейків, дезінформації та кібербулінгу.

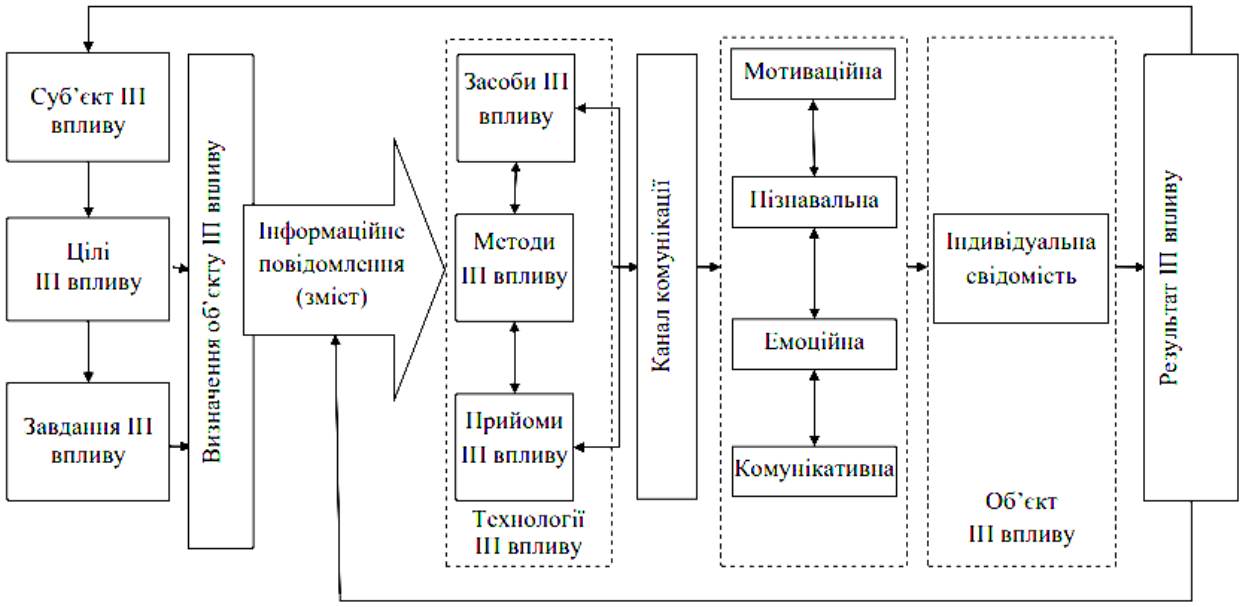


Рисунок 1.4 – Структурно-функціональна схема деструктивного інформаційно-психологічного впливу

Фахівці з інформаційної безпеки виділили основні види та форми деструктивного впливу в інформаційних системах, а саме: [5, ст. 14]

– кібератаки включають в себе різні види кібератак, такі як деніал-сервіс атаки, віруси, троянські коні, розповсюдження шкідливого програмного забезпечення тощо. Ці атаки можуть спричинити втрату даних, завдати шкоди інформаційній інфраструктурі, а також знизити доступність систем.

– фішинг - це вид атаки, при якому атакувач намагається обдурити користувачів, надсилаючи їм лукаві повідомлення або веб-сторінки, які виглядають як легітимні, але призначені для крадіжки особистої інформації, такої як паролі або номери кредитних карт.

– соціальна інженерія, цей вид атак включає в себе маніпуляцію індивідами або групами з метою отримання конфіденційної інформації або надання доступу до об'єктів.

– кібершантаж включає в себе загрози, шантаж або вимагання, які надходять через інтернет або інші інформаційні засоби.

– розповсюдження дезінформації включає в себе поширення неправдивої або маніпулятивної інформації з метою зміни громадської думки або спричинення паніки.

– кібершпигунство, атаки на інформаційні системи з метою видалення чутливої інформації, що може бути використана в політичних, комерційних або злочинних цілях.

– кібертероризм - це використання кібератак для спричинення паніки, збитку та надання підтримки терористичним цілям.

– кібербулінг, зловживання інформаційними технологіями для психологічної або емоційної атаки на індивідів, зокрема через соціальні мережі і онлайн-платформи.

Це лише декілька прикладів видів деструктивного впливу в інформаційних системах. Ці атаки можуть мати серйозні наслідки, включаючи фінансові втрати, порушення приватності, втрату даних і навіть загрозу громадській безпеці. Захист від цих видів деструктивного впливу вимагає комплексного підходу, включаючи застосування технічних, організаційних та етичних заходів.

Деструктивний вплив в інформаційних системах може мати серйозні психологічні наслідки для жертв та спільноти в цілому.

Психологами викладено в своїх працях види психологічних наслідків деструктивного впливу. [8, ст. 3-7]

Люди, які стали жертвами деструктивного впливу, можуть відчувати страх і тривогу щодо своєї безпеки та приватності. Вони можуть стурбовано переживати можливу втрату даних, фінансову шкоду або інші наслідки атаки.

Деякі форми деструктивного впливу, такі як кібербулінг чи публічне розголошення конфіденційних даних, можуть призвести до страху перед соціальним виключенням та негативним ставленням оточуючих.

Деструктивний вплив може викликати стрес та депресію в жертв. Вони можуть відчувати себе безпомічними та враженими, що може призвести до погіршення психічного здоров'я.

Жертви деструктивного впливу можуть втрачати довіру до інших індивідів та онлайн-середовища загалом. Можуть відчувати втрату самоповаги через негативні коментарі, оцінки або критику, які можуть супроводжувати деструктивний вплив.

Деструктивний вплив може надавати враження втрати контролю над власним життям та інформацією, що може викликати почуття безпомічності та втрати особистої свободи.

Стан тривоги та стресу може призвести до порушення сну та нездатності до концентрації, що може вплинути на робочу продуктивність та якість життя жертв.

Ці психологічні наслідки можуть бути дуже серйозними і вимагають підтримки та допомоги для жертв. Заходи до захисту від деструктивного впливу та розвинення інформаційної грамотності можуть допомогти зменшити ці наслідки і підвищити свідомість про цю проблему.

1.5. Методи захисту від деструктивного впливу

Володіння інформацією є надважливою потребою особистості, без неї неможливе формування та існування її індивідуальної свідомості. Вона допомагає людині правильно оцінити ситуації, в яких знаходиться, спрогнозувати розвиток подій, розробити варіанти дій та прийняти обмірковане правильне рішення. Досить низька якість отриманої інформації призводить до руйнівних змін психіки людини, що виявляються в тривожності, напруженості та дезадаптації. У такий спосіб простежується неможливість отримання соціально значущих даних серед потоку інформації. Подібні речі значною

мірою прослідковуються в ситуаціях умисного використання інформації в маніпуляційних цілях. В наукових статтях розглянуто методи та стратегії захисту від деструктивного впливу в інформаційних системах. [9, ст. 32-56]

Кіберзахист — це використання антивірусного програмного забезпечення, брандмауерів, систем виявлення вторгнень та інших кіберзасобів для захисту інформаційних систем від кібератак.

Застосування шифрування для захисту конфіденційної інформації від несанкціонованого доступу під час зберігання та передачі даних.

Встановлення механізмів аутентифікації (перевірки ідентифікації користувачів) та авторизації (надання дозволу на доступ до ресурсів) для контролю доступу до інформації.

Вимога до користувачів використовувати сильні паролі та змінювати їх періодично, а також застосування методів двофакторної аутентифікації.

Постійне встановлення патчів і оновлень для операційних систем, програмного забезпечення та апаратних пристроїв для закриття вразливостей.

Забезпечення інформаційної грамотності користувачів та персоналу щодо кібербезпеки, включаючи ідентифікацію фішингу та інших шахраївських атак.

Використання систем моніторингу та аналізу подій для виявлення надзвичайних подій та потенційних загроз безпеці інформаційних систем.

Регулярне створення резервних копій даних і інформаційних систем для відновлення інформації у випадку втрати чи пошкодження.

Розроблення та впровадження політик та процедур щодо конфіденційності і безпеки інформації для персоналу та користувачів.

Використання глобального підходу до кібербезпеки, який включає в себе захист на всіх рівнях та в галузях, від користувачів до мереж і систем.

Також розглянуто *технічні засоби захисту:*[9, ст. 25-30]

– антивірусне програмне забезпечення. Захищає комп'ютери від шкідливих програм та вірусів, перевіряючи та блокуючи їх.

– брандмауери. Контролюють трафік мережі та фільтрують небажаний або шкідливий трафік, забезпечуючи безпеку мережі.

– інтрузійні виявлення та системи інтрузії. Виявляють аномалії та вторгнення в мережу та систему та сповіщають про них.

– шифрування. Застосування шифрування для захисту даних під час передачі та зберігання, забезпечуючи конфіденційність.

– парольні політики. Встановлення правил для складності та періодичної зміни паролів.

– системи ідентифікації та аутентифікації. Вимагають ідентифікації користувачів та надають доступ лише після аутентифікації.

– системи резервного копіювання. Забезпечують створення резервних копій даних для відновлення інформації в разі втрати чи пошкодження.

– системи моніторингу та аналізу подій. Виявляють аномалії та події, що вказують на можливі загрози безпеці.

Розглянуто *психологічні засоби захисту:*[9,ст. 60-64]

– навчання та інформаційна грамотність. Підвищення свідомості користувачів та персоналу щодо загроз і методів захисту.

– соціальна інженерія. Навчання користувачів розпізнавати спроби маніпуляції та обману з боку атакувальників.

– захист від стресу. Психологічний тренінг для працівників, щоб допомогти їм реагувати на стресові ситуації, пов'язані з кібератаками.

– співпраця та комунікація. Встановлення ефективних зв'язків та комунікації між різними частинами організації для виявлення та відповіді на загрози.

– соціальний і психологічний супровід. Забезпечення психологічної підтримки для жертв деструктивного впливу.

Це лише декілька прикладів методів захисту від деструктивного впливу. Захист від кіберзагроз вимагає постійної уваги, моніторингу і адаптації до змінюючихся загроз та технологій. Технічні та психологічні засоби захисту

доповнюють один одного та сприяють створенню комплексної стратегії захисту від деструктивного впливу.

Різні фахівці з інформаційної безпеки надають рекомендації до соціотехнічних систем. [8, ст. 10-15]

Розробляти методологію, яка дозволить аналізувати і виявляти деструктивний вплив в соціотехнічних системах. Визначте ключові показники та критерії для оцінки такого впливу.

Розробляти алгоритми та моделі, які дозволять виявляти аномалії в інформаційних потоках та поведінці користувачів, які можуть свідчити про деструктивний вплив.

Забезпечувати постійний моніторинг і аналіз інформаційних потоків та даних, щоб вчасно виявляти загрози та аномалії.

Розробляти системи попередження та реагування на деструктивний вплив, які дозволять вживати заходи щодо обмеження шкоди та відновлення системи.

Забезпечити психологічну підготовку та підтримку для персоналу, який працює з інформаційними системами та може бути вразливим до деструктивного впливу.

Залучати користувачів до процесу виявлення та реагування на деструктивний вплив, створюючи механізми зворотного зв'язку та звітування.

Розробляти і впроваджувати етичні стандарти для обробки інформації та впливу на користувачів, зокрема враховуючи психологічні аспекти.

Дотримуйтесь відповідних законодавчих норм та вимог щодо захисту приватності та інформаційної безпеки.

Проводити наукові дослідження та аналіз впливу на соціотехнічні системи, щоб постійно вдосконалювати методи виявлення та захисту.

Розглядати деструктивний вплив як глобальний виклик, який вимагає співпраці та координації на різних рівнях та в різних галузях.

Ці рекомендації допоможуть забезпечити ефективний захист соціотехнічних систем від деструктивного впливу та підвищити рівень безпеки та стійкості цих систем.

Висновки до першого розділу

У першому розділі ми провели аналіз основних визначень нашого дослідження, а саме:

1. Розробка та впровадження детекторів та алгоритмів для виявлення деструктивного впливу в соціотехнічних системах є важливою для забезпечення безпеки та стійкості цих систем.
2. Висвітлення психологічних аспектів деструктивного впливу, зокрема впливу на психіку та поведінку користувачів, може допомогти краще розуміти механізми атак та розвивати ефективні методи захисту.
3. Важливо розвивати механізми взаємодії з користувачами та співпрацю з ними для виявлення та реагування на деструктивний вплив.
4. Врахування законодавчих норм і етичних стандартів є важливим для регулювання інформаційного впливу та захисту прав користувачів.
5. Деструктивний вплив є глобальним викликом, і вимагає спільних зусиль на різних рівнях і в різних сферах.

РОЗДІЛ 2. ДОСЛІДЖЕННЯ ІСНУЮЧИХ МЕТОДІВ АНАЛІЗУ ІНФОРМАЦІЙНИХ РЕСУРСІВ ЩОДО НАЯВНОСТІ ДЕСТРУКЦІЙ

2.1 Дослідження методів аналізу інформаційних технологій для виявлення деструктивних впливів

Аналіз публікацій з проблем забезпечення інформаційної безпеки свідчить, що на даний час достатньо добре досліджено [2-7, 10]:

– джерела та причини інформаційних загроз;
– компоненти, форми інформаційної боротьби;
– методи та засоби інформаційної боротьби;
– види реалізації інформаційно-психологічних впливів.

Більшість наукових праць зосереджені на проблемах забезпечення інформаційної безпеки у таких геополітичному та технологічному аспектах. Разом з тим, самі інформаційні технології та засоби ведення інформаційно-психологічного протиборства або мають обмеження на відкрите використання, або досліджені на недостатньому рівні.

Головний інтерес тут стосується ключового компонента інформаційних технологій забезпечення інформаційно-психологічної безпеки особистості, а саме методів аналізу та виявлення (детектування) інформаційних деструкцій в електронних документах. Отже необхідно розглянути ті інструменти ІТ, що використовуються для моніторингу засобів масової інформації. Таких технологій на даний час розроблено близько сотні. Але основні їх функціональні можливості, як правило, стосуються: організації зберігання середніх або великих обсягів інформації; забезпечення простих пошукових можливостей та / або тематичні рубрикатори. При цьому не підтримується жодного механізму якісного аналізу ІР.

Всі існуючі інформаційні технології та методу в залежності від глибини аналізу текстової інформації можна розглядати за трьома класами, а саме:

1. До першого класу відносяться технології та методи, які забезпечують аналіз IP за ключовими словами. Відповідно такі методи дозволяють з одного боку створювати, а з іншого боку виявляти інформаційні атаки *першого покоління*.

2. Інформаційні технології та методи, які додатково дозволяють аналізувати семантичний контент електронних TIP створюють другий клас. Відповідно такі технологічні рішення забезпечують умови для здійснення та виявлення інформаційно-психологічних атак *другого покоління*. Саме такі інформаційно-психологічні атаки здійснюють вплив на свідомість особистості.

3. Третій клас інформаційних технологій та методів формують такі технологічні рішення, які додатково дозволяють збільшити глибину аналізу текстової інформації до рівня врахування психологічно-емоційної та внутрішньо-установочної складової особистості. Такі інформаційно-технологічні рішення створюють потенційні можливості з одного боку для проведення, а з іншого – для детектування сугестивних інформаційно-психологічних впливів на підсвідомість особистості. Саме такі інформаційно-психологічні операції є найбільш значущими з позиції нанесення шкоди та найбільш непомітними для смислового аналізу. Отже такі впливи відносяться до атак третього покоління – найбільш перспективних та складних інформаційно-психологічних атак.

Функціональні характеристики доступних технологічних рішень обробки, аналізу текстової інформації для створення умов протидії інформаційно-психологічним атакам першого та другого поколінь представлено в табл. 2.1. Найбільш відомою з них є інформаційна технологія, що базується на комплексному смисловому аналізаторі електронного тексту *Text Analyst* [12, 14]. В створі задоволення потребам інформаційно-психологічних операцій така технологія відноситься до *другого покоління*.

Аналізатор тексту Text Analyst – інтелектуальне програмне забезпечення для аналізу змісту електронних текстів, смислового пошуку інформації та формування електронних архівів [12, 14].

Процедури обробки інформації в системі включають:

1. Попередній аналіз текстової інформації (виділення в тексті понять, які входять в базові словники).

2. Статистичний аналіз тексту – визначення частот зустрічальності в тексті слів і словосполучень (важливість поняття оцінюється за частотою його використання в тексті).

3. За результатами частотного аналізу формування семантичної мережі для аналізованого тексту, що відбиває зв'язки між поняттями і об'єднуючою їх в єдину смислову картину (перед побудовою семантичної мережі встановлюється поріг значимості для понять і зв'язків між ними).

4. На основі семантичної мережі побудова тематичної структури тексту у вигляді дерева або лісу понять (кожній темі відповідає своє дерево понять).

5. Автоматичне реферування тексту на основі його тематичної структури.

6. Формування гіпертекстової розмітки;

5. Смисловий пошук інформації.

Таблиця 2.1

Огляд програмних реалізацій технологій обробки електронної текстової інформації

Назва системи	**Основне призначення**
Астарта	Інструмент автоматизації аналітичних досліджень. Експертний рубрикатор, призначений для збору, зберігання і семантичного аналізу текстових матеріалів. Під аналізом тут розуміється автоматичне створення рубрик і угруповання, а також інтелектуальна вибірка інформації по заданій темі
Галактика–Zoom	Програмний комплекс призначений для аналітичної обробки текстових неструктурованих документів. Здійснює швидкий пошук і контент-аналіз відібраної інформації. Побудований за принципом роботи з тематичним рубрикатором
Медиалогия	Інформаційно-аналітична система здійснює моніторинг понад 24 000 об'єктів, фіксуючи статистичну та аналітичну інформацію з тисячі джерел (центральна і регіональна паперова преса, інформаційні агентства, транскрипти та оригінали телерадіопередач, Інтернет-джерела). На обробці повідомлень задіяно кілька сотень кваліфікованих операторів, безупинно переглядають до десяти тисяч повідомлень на добу. Система дозволяє класифікувати публікації за значимістю, визначати ставлення ЗМІ до об'єктів, аналізувати характеристики PR–кампаній, встановлювати відображені в ЗМІ зв'язку між об'єктами і т. д
Hummingbird	Інформація автоматично рубрикується, а потім піддається OLAP–аналізу. Є засоби, за допомогою яких користувачі можуть самі створювати нові або настроювати наявні дерева рубрик. Вибірка документів проводиться за допомогою, як контекстного пошуку, так і OLAP–аналізу
TextAnalyst	Інструмент для аналізу змісту текстів, смислового пошуку інформації, формування електронних архівів. Здатна будувати семантичні дерева, але не за об'єктами, а за окремими статтями, в результаті чого створюється смисловий портрет кожного тексту на основі кількості згадувань і близькості зустрічання різних значущих, на думку програми, слів. Є модуль, що генерує реферат текстового документу

Основні функціональні принципи, що реалізовані в технологічному продукті Text Analyst включають до себе наступне. По-перше, принцип асоціативності, який полягає у використанні такої моделі представлення тексту, при якій його фрагменти вказують на місця їх зберігання. Якщо фрагменти збігаються, то вони вказують на одне і те ж місце, де записується частота їх зустрічальності. По-друге побудову структури понять, що представляє текст, відповідно до їх важливості і взаємозв'язків. По-третє формування тематичної структури тексту у вигляді багаторівневої ієрархії тем, і розкриваючих їх підтем.

Технологію Text Analyst розроблено з використанням об'єктно-орієнтованого підходу і COM–технології. На їх основі реалізовані два програмних об'єкта, а саме: лінгвістичний процесор і алгоритмічне ядро.

Концепція Text Analyst передбачає наявність двох базових словників: для української та англійської мов. Для них передбачені 4 підсловника: словник видаляємих слів; словник загальних слів; словник слів-уподобань користувача (предметних понять); словник слів-винятків з правил нормальної словозміни.

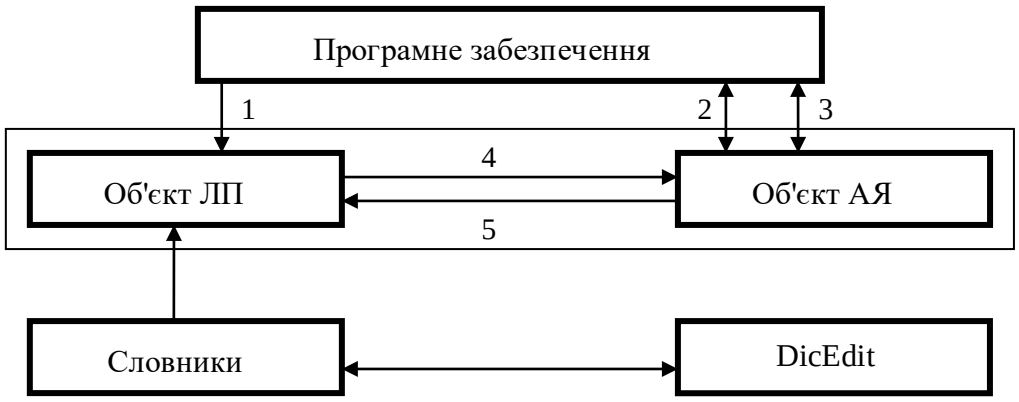


Рисунок 2.1 – Схема побудови Text Analyst

Додаток DicEdit дозволяє настроювати словники на програмне забезпечення аналізованих текстів чи створювати власні словники.

Основними функціями модуля лінгвістичного процесора є:

– виділення з тексту послідовності слів;

– виключення з цієї послідовності елементів словника видаляємих слів; (він містить малозначущі і неінформативні слова);

– маркування слів атрибутами, визначаючими їх типи;

– приведення словоформ до базової граматичної форми.

Таким чином, на вхід лінгвістичного процесора надходить рядок тексту. Відповідно на його виході формується послідовність слів, маркованих атрибутами, визначаючими їх типи. Словник лінгвістичного процесора встановлює набір слів, що видаляються з тексту, і атрибути слів у вихідний послідовності. Лінгвістичний процесор створює базу даних (БД), в яку заносить всю лінгвістичну інформацію про аналізований текст. Надалі робота відбувається з цією БД, а не з вихідним текстом, що значно спрощує обробку і збільшує її продуктивність.

На вхід модуля алгоритмічного ядра надходить послідовність слів з атрибутами, визначеними лінгвістичним процесором. Даний модуль виконує такі основні функції:

1) статистичний аналіз вхідних послідовностей слів і виділення понять, під якими в Text Analyst розуміються слова і словосполучення, зустрічальність яких у тексті не нижче встановленого порога;

2) визначення смислових зв'язків між поняттями;

3) завдання посилань на пропозиції, в які входять виділені поняття.

На виході алгоритмічного ядра формуються компоненти БД, що представляють зміст тексту. Основою цих компонентів служить семантична мережа, тобто безліч слів і словосполучень, пов'язаних між собою по граничному атрибуту (частоті). Побудована таким способом семантична мережа передає зміст текстів, значно скорочуючи при цьому обсяг вихідної інформації (за рахунок виключення несуттєвих деталей). Вона являє собою індекс аналізованого тексту, який може бути ефективно використаний для

реалізації різних методів доступу до тексту, в тому числі асоціативного (смислового) пошуку.

Вершинами семантичної мережі є слова і словосполучення, що несуть у тексті основне смислове навантаження. Вони виділяються по частоті в тексті. Порогове значення цього параметра може задаватися користувачем. У формованої семантичної мережі кожне поняття, багаторазово згадане в тексті, представляється єдиним елементом, приведеним до базової граматичної форми. Зв'язки між вершинами відображають спільне використання понять в тексті. Крім того, вершина співвідноситься зі списком пропозицій, в яких вжито відповідне їй поняття. Таким чином, в "смисловому портреті" тексту інтегрується інформація, що відноситься до понять.

Кожне поняття, яке увійшло в семантичну мережу, представляє деяку тему тексту і характеризується числовий оцінкою – смисловим вагою. Ця ж оцінка приписується і зв'язків між поняттями. Значення смислового ваги лежить в інтервалі від 1 до 100 і відображає важливість поняття по відношенню до сенсу всього тексту. Чим воно більше, тим важливіше поняття. Поняття з максимальними значеннями (рівними або близькими до 100) є ключовими і являють найважливіші теми тексту.

Високе значення ваги зв'язку першого поняття з другим вказує на те, що більша частина інформації в тексті, що відноситься до першого поняття, відноситься і до другого. Проте зв'язок першого поняття з другим не завжди має ту ж вагу, що і зв'язок другого поняття з першим.

Користувач може настроювати засоби візуалізації семантичної мережі, встановлюючи порогові ваги відображуваних понять і зв'язків, а також спосіб їх сортування.

В області автоматизації побудови Text Analyst дозволяє автоматично перетворити мегабайтний масив текстової інформації в гіпертекст, виділивши істотні смислові взаємозв'язки між його фрагментами. Основою для формування гіпертексту служить семантична мережа. Її проекція на

вихідні тексти трансформує їх у гіпертекст. У текстах виділяються кольором поняття семантичної мережі, що рекомендуються як гіперпосилань, які ведуть до фрагментів, що містить або ці поняття, або інші поняття, пов'язані за змістом з вихідними. В результаті виникає можливість циклічного руху по ланцюжку : обраний фрагмент тексту – поняття семантичної мережі – вибрана гіперпосилання – фрагмент тексту.

Однак, такі технологічні рішення не передбачають оцінку таких складових інформаційно-психологічних аспектів, як емоції, загрози, характер відносин між об'єктами та ін. Отже існуючі доступні інформаційні технології першого та другого класу не забезпечують якісний глибинний аналіз текстових інформаційних ресурсів.

З одного боку таке становище обумовлено тим, що сучасні теоретичні положення визнають явища існуючими лише тоді, коли вони або безпосередньо спостерігається, або відтворено проявляє себе в експериментах, або строго обчислюється. Причому в будь-якому випадку останнє слово залишається за практикою: потрібно, щоб явище спостерігаємо функціонувало або виявлялися б сліди його дії. Але, з іншого боку, там, де мова йде про психологічний стан особистості, все виглядає інакше.

Ця область науково-прикладних досліджень завіюється на недостатньому рівні. Наслідком чого є те, що не створено адекватних математичних інструментів для опису інформаційно-психологічних взаємозв’язків та їх впливу на моральне-психологічний стан особистості та зміни внутрішніх установок.

2.2. Обґрунтування підходу відносно детектування сугестивних інформаційно-психологічних деструкцій в електронних текстових ресурсах в умовах інформаційного протиборства

Психологічні явища найчастіше безпосередньо не спостерігаються, в експериментах, тобто: або проявляються, або ні; обчисленню піддаються погано; сліди їх функціонування невизначені або нерегулярні.

Особливо критичний стан спостерігається для спроб встановлення інформаційно-психологічних залежностей в області підсвідомості.

Отже, оскільки природна мова є одним з найсильніших засобів впливу на особистість, наприклад, психологічні теорії розглядають його як ефективний засіб програмування людей. Тому для ефективного інформаційно-психологічного впливу на соціум та особистість важливі не тільки і не стільки логічність і аргументованість мови (синтаксичне, морфологічне та семантичне представлення текстової інформації), *скільки емоційний і підсвідомий інформаційний вплив на слухача* (особистість).

Саме такий тип деструктивних інформаційно-психологічного інформаційно-психологічних атак складає найбільш перспективне *третє покоління* інформаційних операцій. Для нього характерно:

1) скритність (тому що не підлягає виявленню класичними технологіями аналізу тестової інформації);

2) низький рівень протидії та контролю (тому що його дія стосується саме підсвідомості особистості, що дуже складно контролювати).

В теж час, незважаючи на це, існують спроби створити методики, які в тій чи іншій мірі (обмеженій мірі) можуть визначити інформаційно-психологічний вплив на підсвідомість особистості, шляхом аналізу інформації, яка людиною сприймається. Функціональні компоненти цих методик, які засновано на багаторазових експериментах, проведених з різними соціальними групами, не мають належного математичного обґрунтування. Однак, достатня кількість експериментів показує, що відповідні результати інформаційно-психологічного впливу хоч і мають відхилення, але більшість випробовувань показують приблизно однакові

результати. Отже саме ці середні показники залежностей інформаційно-психологічного впливу і були закладені в методиках для аналізу ТІР.

В загальному випадку виявлення та створення інформаційно-психологічного неусвідомленого (сугестивного) впливу на підсвідомість може використовуватись для:

1) безпосереднього деструктивного інформаційно-психологічного впливу на особистість з боку протиборчої сторони;

2) забезпечення протидії шляхом нанесенні інформаційної атаки на противника в наших інтересах;

3) здійснення інформаційної пропаганди в інтересах ідейно-моральної політики держави та соціуму;

4) проведення конструктивних інформаційних впливів для оздоровлення морально-психологічного стану особистості

5) просунення комерційних інтересів, наприклад підготовка відповідних рекламних інформаційних блоків. Простим прикладом цього можна навести рекламу, мета якої не просто розповісти про новий продукт, як багато хто вважає, а змусити людину купити цей продукт. Дивлячись рекламу, у людини в підсвідомості може скластися думка про те, що товар йому дійсно потрібний або ж він віддасть йому перевагу при виборі серед інших. Такий вплив може бути закладено саме завдяки методикам неусвідомленого впливу на підсвідомість.

Представником третього класу інформаційних технологій є "***Психолінгвістична експертна система ВААЛ-2000***" [13]. Згідно відкритих публікацій [13-16] така технологія дозволяє в автоматизованому режимі проводити обробку великої кількості текстової інформації, виявити глибинні мотиви психолінгвістичного впливу слів і фраз на слухачів та забезпечити апарат для створення відповідних деструктивних інформаційно-психологічних атак третього покоління. Треба відмити, що це технологічне рішення є закритим продуктом. Інформація стосовно її структурно-

функціональних складових та тактико-технічних характеристик у відкритих публікаціях є обмеженою.

Дослідження побудови системи ВААЛ для аналізу сугестивних впливів на підсвідомість людини текстів .

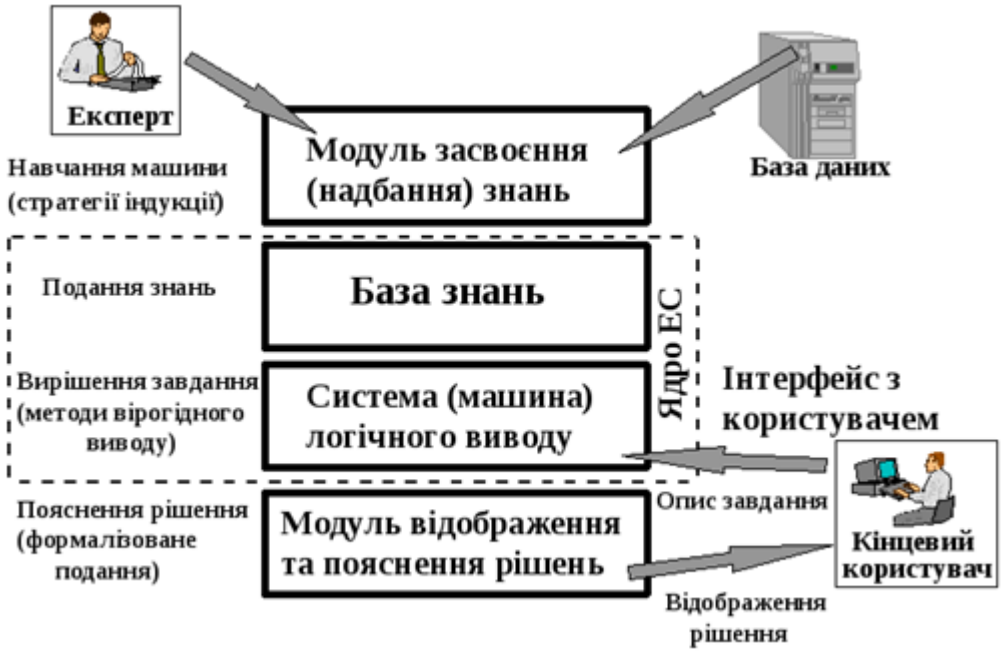


Рисунок 2.1 – Схема побудови ВААЛ 2000

Експертна система "ВААЛ" компанії "Тривола" призначена для психолінгвістичного аналізу текстів з прогнозуванням емоційних несвідомих реакцій аудиторії (слухачів, читачів) і, при необхідності, подальшим психологічним редагуванням тексту – ітераційним процесом його зміни в бажаному напрямку [13,16].

Фактично система являє собою проблемно-орієнтований аналізатор текстів, реалізований у вигляді шаблону з макросами для текстового процесора MS Word з додатковими DLL – бібліотеками словників. Тому працює система тільки в сімействі операційних систем ОС Windows з встановленим програмним забезпеченням MS Word.

З відкритих джерел відомо, що в даний час система ВААЛ широко використовується у великих рекламних і PR-компаніях, консалтингових

центрах, банках, видавництвах, вона з успіхом застосовується в передвиборних кампаніях [17]. Технологію ВААЛ також використовують в дослідницьких центрах психологи, психотерапевти, лінгвісти та практики нейролінгвістичного програмування.

Система володіє наступними можливостями:

- оцінювання неусвідомлюваного емоційного впливу фонетичної; структури текстів та окремих слів на підсвідомість людини;

– генерування слів із заданими фоносемантичними характеристиками;

– завдання характеристики бажаного впливу і цілеспрямоване редагування текстів для досягнення зазначених характеристик;

– коригування тексту за обраними параметрами з використанням словника синонімів на 5 тис. синонімічних рядів з 25 тис. слів;

– настроювання на різні соціальні та професійні групи людей, які можуть бути виділені по використовуваної ними лексиці;

– оцінювання звуко-колірної характеристики текстів;

– введення додаткових нових фоносемантичних шкал користувачем, розширюючи систему в потрібному для нього напрямку;

– факторний аналіз даних з подальшою візуалізацією результатів;

– повноцінний контент-аналіз тексту за великим числом спеціально складених вбудованих і користувальницьких категорій;

– емоційно-лексичний аналіз текстів;

– контекстний контент-аналіз текстів;

– автоматична категоризація текстів.

В основі оцінки емоційного впливу фонетики слова і тексту лежить фоносемантичний аналіз і методи нейролінгвістичного програмування (визначення навантаження на основні сенсорних каналів сприйняття людини, мета-програми та ін.). Для оцінки фоносемантичного впливу слова або словосполучення в системі ВААЛ можна використовувати 24 біполярних

шкали. Всім звукам за цими шкалами зіставлені оцінки. Спеціальні формули дозволяють на основі цих оцінок зіставити оцінки окремим словам, словосполученням, фразам і текстам. І хоча ці оцінки не усвідомлюються людьми, але, як показали експерименти, відбувається досить сильний вплив на підсвідомість.

Експертна система ВААЛ дозволяє проводити автоматизований аналіз тексту з декількох різних по суті, але додаткових до один одного за змістом, позицій. Користувач системи може сам визначити, які з можливих критеріїв варто використовувати для вирішення поставлених перед ним завдань. Безумовно, для ефективного використання того чи іншого блоку технології ВААЛ потрібна згода з вихідними припущеннями авторів і розуміння використовуваної термінології тільки в тому сенсі, в якому його використовують автори.

При реалізації проекту ВААЛ були використані наступні припущення :

1) вибір людиною лексичних та граматичних варіантів з можливих у його рідній мові залежить від його психологічних особливостей. Відповідно, психологічні особливості знаходять своє вираження в його усній і письмовій мові. Аналізуючи усну або письмову мову людини можна реконструювати його картину світу і здійснити атрибутування його картини світу і / або індивідуальності на основі тієї чи іншої системи класифікації;

2) у ситуації вільного вибору людина вибирає і / або краще сприймає тексти (усні чи письмові), відповідні його картині світу і схильний ігнорувати інші варіанти опису;

3) комунікативна ефективність тексту залежить від слабо- або неусвідомлюваних ефектів, створюваних окремими значущими для окремої людини або в культурі в цілому словами (різні форми лексичного символізму), нелінгвістичними характеристиками тексту (наприклад, фоно- та кольоро- ассоціації) і невербальними характеристиками процесу комунікації;

4) текст, включаючи його зміст і контекст, для автора і сприймаючого можуть значити більше, ніж може виявити будь-яка специфічна система опису тексту;

5) різні блоки аналізу текстів в системі ВААЛ є специфічними і незалежними один від одного системами класифікацій лексичних та граматичних форм. Спільна інтерпретація категорій з різних блоків аналізу авторами не передбачалося, але не відкидається, технічна можливість надана і залишається особистою прерогативою кожного легального користувача.

В системі ВААЛ-2000 користувач може сконструювати свої власні або скористатися наступними блоками критеріїв аналізу тексту: психіатричний аналіз; психоаналітичний аналіз; мотиваційний аналіз; емоційно-лексичний аналіз; діагностика мета-програм; фоно- та кольорово-семантичний аналіз.

Вибір блоків аналізу для вирішення конкретних завдань визначається згодою з теоретичними передумовами і методикою реалізації аналізу в ВААЛ, особистими перевагами, рівнем підготовки і завданнями дослідника.

Категорії «*Психіатричного аналізу*» атрибутують текст (як ціле) по відповідності текстам осіб з тією чи іншою акцентуацією. У технології ВААЛ реалізована діагностика паранояльний, демонстративної, депресивної, збудливої і гіпертермічної акцентуацій.

Категорії «*Психоаналітичного аналізу*» оцінюють вираженість в тексті слів, що відносяться до сексуальної символіки (за З.Фрейду), архетипів (за К.Юнгом) і вираженню агресивності.

Категорії «*Мотиваційного аналізу*» визначають вираженість в тексті предикатів мотивації у відповідності з традиційними категоріями мотиваційних властивостей (потреба, мотив, валентність, інструментальна діяльність) з угрупованням по чотирьох групах мотивів: фізіологічні, досягнення, влади та афіляції.

Категорії «*Емоційно-лексичної оцінки*» дозволяють виявити емоційну насиченість і структуру оцінки за 15 емоційно – оціночними критеріями, виділеним і найбільш значущим в культурі.

Категорії «*Діагностики мета-програм*» включають в себе оцінку вираженості каналів репрезентації ; суб'єктивну організацію простору, часу і руху: категорії порівняння; логічних операцій; причинно-наслідковий і "свійчужий" атрибуцію ; визначення "центру уваги".

Фоно- та *кольорово-семантичний* аналіз тексту дозволяє оцінити неусвідомлювані емоційні компоненти тексту і слова, згенерувати штучні слова з високою комунікативною ефективністю.

При необхідності користувач може створити власні лексичні та фонетичні категорії аналізу і використовувати їх окремо або спільно з категоріями, пропонованими концепцією ВААЛ.

Концептуально ВААЛ можна використовувати для забезпечення:

1) системи інформаційно-технологічної підтримки щодо створення деструктивних скритих інформаційно-психологічних атак; 2) протидії відповідним інформаційно-психологічним атакам; 2) комерційних інтересів.

Для цього існує можливість, щодо:

– складання текстів виступів і документів з наперед заданими характеристиками впливу на потенційну аудиторію;

– проектування емоційної складової іміджу політичного діяча або організації та активного формування емоційного ставлення до них різних соціальних груп;

– створення емоційно забарвлених рекламних матеріалів і пошуку найбільш вдалих назв і торгових марок;

– неявний експрес-діагностики та психологічного тестування, психо- і гіпнотерапії;

– створення легких в засвоєнні навчальних матеріалів.

Можливе застосування системи в журналістиці, освіті, інформаційному протиборстві та інших областях діяльності людей, де словесний вплив на той чи інший сегмент соціуму є одним з визначальних факторів.

На сьогоднішній день істотним обмеженням системи є її висока вартість і жорстка прив'язка до стороннього програмного забезпечення. Також сама система є повністю закритою, що робить неможливим її подальший розвиток сторонніми розробниками або ж доповненням її необхідними мовними засобами для аналізу.

Отже з одного боку сугестивні деструктивні інформаційно-психологічні атаки є найбільш актуальними та значимими з позиції швидкого та неконтрольованого нанесення шкоди, а з іншого боку інформаційні технології та методи щодо протидії такими впливам не мають належного чина науково-прикладних розробок. Це збільшую актуальність таких інформаційно-психологічних впливів та рівень шкоди від їх застосування.

Таким чином, по зробленому дослідженню можна зробити такі висновки:

1. Інформаційні технології, які відносяться до першого і другого класів, та базуються на методах пошуку, аналізу, складання та формування текстів (інформації) представлені дуже широко. Однак, такі технології: з одного боку враховують лише аналіз текстової інформації за ключовими словами, або додатково за семантикою контенту; з іншого боку не враховується сугестивна складова інформаційно-психологічного впливу, а саме психологічно-емоційні та внутрішньо-установочні характеристики особистості.

Тому такі технологічні рішення не забезпечують виявлення сугестивних (скритих) деструктивних інформаційно-психологічних атак на підсвідомість особистості, тобто вони в сучасній інформаційній війні не придатні для ведення інформаційно- психологічного протиборства та забезпечення національної безпеки держави.

Висновки до другого розділу

1. Інформаційні технології, які відносяться до першого і другого класів, та базуються на методах пошуку, аналізу, складання та формування текстів (інформації) представлені дуже широко. Однак, такі технологічні рішення не забезпечують виявлення сугестивних (скритих) деструктивних ІП атак на підсвідомість особистості, тобто вони в сучасній інформаційній війні не придатні для ведення ІП протиборства та забезпечення національної безпеки держави.

2. Інформаційні технології, які дозволяють проведення більш глибинного аналізу ІР, а саме враховують можливість виявлення сугестивного впливу на підсвідомість, характеризуються тим, що: у відкритих джерелах відсутній опис їх математичної бази та функціональні зв'язки ІП взаємозалежності їх базових складових; існує жорстка заборона урядів більшості держав на експорт даних продуктів в повному обсязі.

3. Відсутність вітчизняних розробок в області інформаційних технологій забезпечення протидії сугестивним деструктивним ІП атакам (ІП операціям третього покоління) на підсвідомість особистості створює критичний рівень загроз порушення національної безпеки держави. Отже існує необхідність в розробці комплексних методів виявлення (детектування) сугестивних деструктивних ІП впливів на підсвідомість особистості з врахуванням сучасних технологічних аспектів (особливостей) створення інформаційних деструкцій протиборчою стороною.

РОЗДІЛ 3. РОЗРОБКА МОДЕЛІ МЕТОДУ ВИЯВЛЕННЯ ДЕСТРУКТИВНОГО ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОГО ВПЛИВУ В СОЦІОТЕХНІЧНИХ СИСТЕМАХ

3.1. Розробка моделі загроз інформаційно-психологічної безпеки з врахуванням прихованого інформаційного деструктивного впливу на суспільство

Для оцінки стану забезпечення інформаційної безпеки суспільства в інфокомунікаційному просторі в умовах ведення інформаційної боротьби (інформаційної протидії) необхідно виконати аналіз загроз, викликаних проведенням деструктивного інформаційно-психологічного впливу з побудовою узагальненої моделі загроз інформаційній безпеці суспільства.

Під загрозою ***інформаційно-психологічної безпеки суспільства*** інфокомунікаційному (соціотехнічному) просторі розуміється множина $\psi_{зіб}$ можливих порушень морально-психологічного стану, його внутрішніх установок [12, 13, 11, 8]. ***Джерелом загроз*** (суб'єкт інформаційного протиборства) інформаційно-психологічної безпеки є безліч $\psi_{дзіб}$ носіїв загрози безпеки, дії яких можуть призвести до порушення здоров’я людей [12, 13, 11, 8]. Суб'єктами інформаційного протиборства виступають спеціальні центри протидіє протиборчої сторони, спецслужби іноземних держав, терористичні організації, політизовані радикальні угруповання, кримінальні структури, транснаціональні корпорації та інші формальні й неформальні учасники сучасних міжнародно-правових відносин. Під ***вразливістю суспільства*** розуміється множина $\psi_{вібо}$ причин, що призводять до втрати інформаційно-психологічної безпеки суспільства, і, як наслідок, до деградації його морально-психологічного стану і здоров'я, тобто.

$$\psi_{вібо} = \{\psi_{вібо/ву}; \psi_{вібо/вп}; \psi_{вібо/рп}; \psi_{вібо/взв}; \psi_{вібо/вс}\}.$$

Уразливості можуть бути обумовлені причинами наступного характеру [2, 3, 8]:

1. рівнем внутрішніх установок (множина причин $\psi_{\text{вібо/ву}}$), включаючи особливості менталітету, спадкові ознаки, генотип;

2. рівнем виховання людини (множина причин $\psi_{\text{вібо/вп}}$);

3. рівнем розвитку людини (множина причин $\psi_{\text{вібо/рп}}$), включаючи морально-психологічний, інтелектуальний, психіки та ін.;

4. рівнем сприйнятливості до зовнішніх впливу (множина причин $\psi_{\text{вібо}/\text{взв}}$), в тому числі рівень критичного осмислення одержуваної інформації;

5. рівень взаємодії в соціумі (множина причин $\psi_{\text{вібо}/\text{вс}}$).

У загальному випадку виділяються такі основні уразливості як: несформований і нестійкий до цього віку морально-психологічний стан людини; особливості менталітету і навколишнього соціального середовища, спадкові ознаки;; слабка нервова система і нестійка психіка; слабкий фізичний розвиток; недостатній рівень критичного осмислення інформації; недостатньо сформована інтелектуальна організованість; схильність до впливу ближньої і дальньої соціальної, соціотехнічного і інформаційного середовища. Атака (інформаційно-психологічний вплив) це множина $\psi_{\text{атк /іп}}$ дій з боку множини $\psi_{\text{дзіб}}$ джерел загроз, що реалізує множину $\psi_{\text{вібо}}$ вразливостей інформаційно-психологічної безпеки особистості. Відповідно безліч інформаційно-психологічних атак (впливів) задається як:

$$\Psi_{\text{атк / іп}} \psi \{\psi_{\text{дзіб}} ; \psi_{\text{вібо}} \}.$$

Наслідки порушення інформаційно-психологічної безпеки особистості це можлива множина $\psi_{\text{зіб}}$ реалізацій загроз множиною $\psi_{\text{дзіб}}$ джерел загроз через наявну множину $\psi_{\text{вібо}}$ вразливостей, спрямованих на нанесення множини $\psi_{\text{шк}}$ збитків як з позиції розвитку людини, так і з позиції їх інформаційно-психологічної безпеки. Це записується таким виразом:

$$\psi_{зіб} : \{\psi_{дзіб} ; \psi_{вібо}\} \rightarrow \psi_{шк} \qquad (3.1)$$

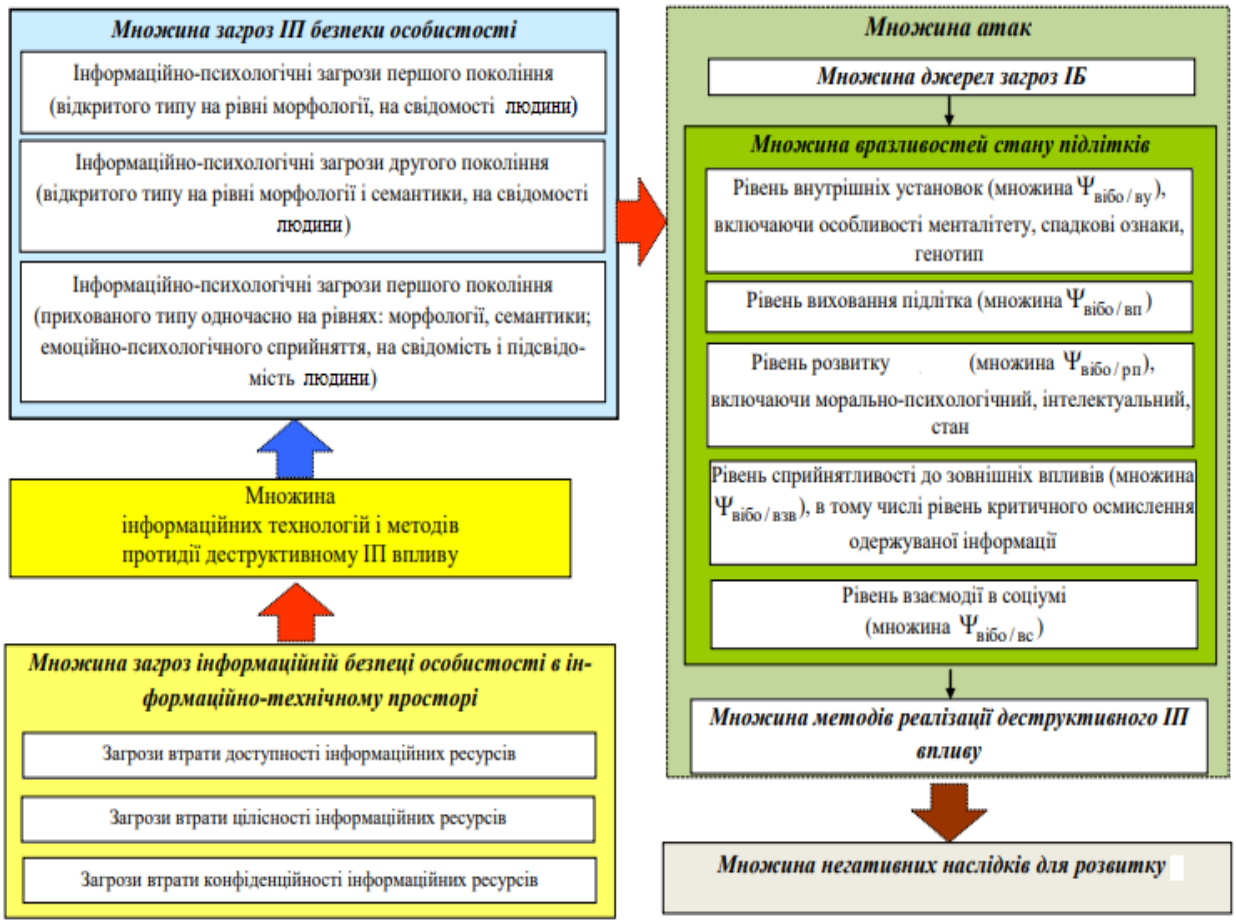
Для оцінки і формування підходів підвищення протидії деструктивним інформаційно-психологічним впливам потрібно провести аналіз безлічі можливих порушень інформаційно-психологічної безпеки суспільства з обов'язковою ідентифікацією багатьох джерел загроз, множини $\psi_{дф}$ дестабілізуючих факторів, що сприяють їх прояву і множини вразливостей [2, 3, 5, 8]. Такий аналіз загроз інформаційно-психологічної безпеки суспільства є одним з найважливіших етапів при оцінці реального стану забезпечення протидії деструктивним інформаційно-психологічним атакам у відкритому інфокомунікаційному просторі в умовах проведення політики демократизації суспільства, свободи слова та інтеграції в світовий інформаційний простір. Його основою є розробка моделі загроз [2, 3, 8].

На підставі моделі загроз формується політика безпеки, тобто протидія деструктивним інформаційно-психологічним атакам з урахуванням їх актуальності і значущості. Для цього виконується моделювання та класифікація безлічі джерел загроз і безлічі їх проявів. Тут, як правило, використовується аналіз взаємодії наступного логічного ланцюжка: "безліч загроз в інформаційно-психологічному просторі – безліч джерел загроз – безліч методів реалізації деструктивного інформаційно-психологічного впливу – безліч вразливостей стану людини – безліч негативних наслідків для розвитку і здоров'я людини" (рис. 3.1). Вихідними даними для побудови моделі загроз і класифікації джерел загроз ІПБ особистості є [2, 3, 6, 8]:

Рисунок 3.1 – Загальна модель реалізації загроз інформаційно-психологічної безпеки особистості

Структурна схема системи забезпечення інформаційно-психологічної безпеки суспільства у відкритому інфокомунікаційному просторі в умовах, коли з одного боку необхідно забезпечити концепцію демократизації суспільства, а з іншого боку, коли ведеться інформаційна війна, представлена на рис. 3.2. Як показано на рис. 3.2. прикладом зв'язки, представленої на рис. 3.1. для інформаційної безпеки суспільства може бути наступний варіант. Протиборча сторона (джерело загроз) - низька здатність щодо критичного аналізу інформації (вразливість обумовлена сприйнятливість до зовнішніх впливів) - дезінформація або деструктивний інформаційно-психологічний вплив на усвідомленому рівні сприйняття інформації людною (атака) - модифікація стану людини, його цільової мотивації і емоційних установок (результат, наслідки), в тому числі підтримка і участь в деструктивних рухах спротиву, формування антипатріотичних настроїв.

Проведений аналіз процесів деструктивних впливів соціальному і



соціотехничному (інфокомунікаційному) просторах в умовах: з одного боку ведення інформаційної протидії, а з іншого боку проведення політики демократизації суспільства, його інформатизації, дозволяє зробити таку класифікацію загроз інформаційній безпеці суспільства, а саме (рис. 3.3):

Рисунок 3.2 — Структурна схема системи забезпечення інформаційно-психологічної безпеки людини у відкритому інфокомунікаційному просторі в умовах демократизації суспільства та інформаційної війни

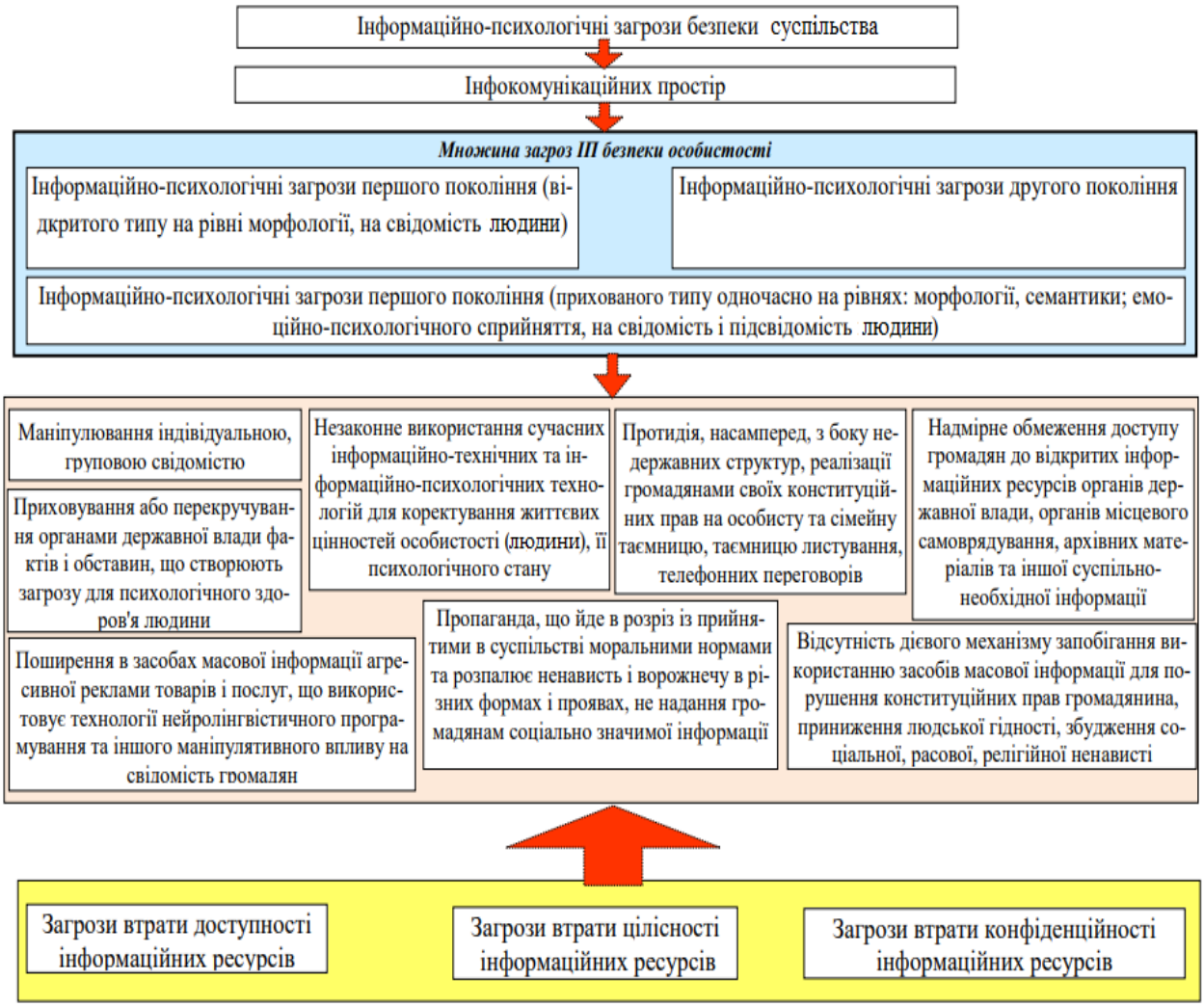


Рисунок 3.3 — Модель загроз інформаційно-психологічної безпеки особистості в інфокомунікаційному просторі

1. Безліч загроз в інформаційно-психологічному просторі. Тут в залежності від глибини використання інформаційних деструкцій розрізняють такі види загроз (деструктивних інформаційно-психологічних атак):

1) до першого виду відносяться загрози (інформаційно-психологічної загрози *першого покоління)*, які обумовлені відкритими інформаційно-психологічними атаками на свідомість, які застосовують інформаційні деструкції на рівні морфологічного опису електронних текстових документів, тобто на рівні окремих слів;

2) інформаційно-психологічні загрози, які додатково використовують інформаційні деструкції на рівні семантичного опису

інформаційних ресурсів (електронних текстових документів) створюють другий вид (загрози, які обумовлені відкритими інформаційно-психологічними атаками *другого покоління* на свідомість);

3) третій вид інформаційно-психологічних загроз це загрози які пов’язані з сугестивними (скритими) деструктивними інформаційно-психологічними атаками на підсвідомість людей, з додатковим використанням інформаційних деструкцій текстових інформаційних ресурсів на рівні врахування психологічно-емоційної та внутрішньо-установочної складової особистості. Такі загрози відносяться до *третього покоління*.

2. Безліч загроз в IT просторі. Даний вид загроз пов'язаний з втратою інформаційної безпеки за такими категоріями як доступність, цілісність і конфіденційність. Розгляд таких загроз в єдиному ***мережоцентричному*** просторі щодо інформаційної безпеки особистості пов'язано з наявністю певного взаємозв'язку між загрозами в інформаційно-психологічних та IT просторах. Наявність взаємозв'язку обумовлено наступними причинами:

- деструктивні модифікації можуть організовуватися на базі інформаційних потоків, які відповідають сервісам реального часу. Сервіси такого типу мають жорсткі вимоги по характеристикам доступності, своєчасності, цілісності отриманої інформації;
- дії, пов'язані із здійсненням протидії деструктивним інформаційно-психологічним атакам супроводжуються необхідністю обчислювальних та інформаційних витрат, тобто формуються додаткові затримки на обробку інформаційних ресурсів (виникають ризики для втрати доступності інформації), можуть виникати загрози втрати цілісності в процесі обробки інформації;
- аналіз інформаційних ресурсів на наявність деструктивних трансформацій може стосуватися інформаційних сегментів інфотелекомунікаційної системи, інформації з обмеженим доступом в інтересах особистості (персональні дані), соціуму і держави. Тут відповідно

виникають загрози втрати конфіденційності інформаційних ресурсів. Такі загрози можна трактувати як загрозу втрати інформаційної безпеки особистості з позиції порушення категорій доступності та цілісності інформаційного ресурсу, тобто загрози в ІТ просторі, які виникають внаслідок протидії загрозам в інформаційно-психологічному просторі**,** а саме: безліч загроз доступності, цілісності і конфіденційності.

Ефективність протидії деструктивному інформаційно-психологічному впливу на суспільство визначається тим, що:

І. З одного боку необхідно мінімізувати ступінь втрати доступності до інформаційних ресурсів (тобто потрібно забезпечити вільний доступ до відкритої інформації відповідно до прийнятої політики безпеки). Тут використовуються такі показники як: показники доступності або своєчасності отримання інформації; показники достовірності інформації; ступінь повноти інформації; ступінь актуальності інформації.

1. Категорія ***доступності до інформаційного ресурсу***. Доступність це гарантія отримання необхідної інформації або інформаційної послуги користувачем за певний час $t_{пот}$. При цьому фактор часу у визначенні доступності інформації в ряді випадків є дуже важливим і визначає ступінь актуальності отриманої інформації. Це обумовлено тим, що деякі види інформації та інформаційні послуги мають сенс тільки в певний проміжок часу $t_{пот}$ [4, 5]. У цьому випадку затримки відносно отримання інформації користувачами, навіть такі, які обумовлені додатковими часовими витратами на проведення фільтрації інформаційного ресурсу на предмет наявності деструктивного інформаційно-психологічного впливу, також є порушенням категорії інформаційної безпеки. З одного боку противник прагне заблокувати джерела або створити інші перешкоди для отримання користувачами своєчасної актуальної конструктивної інформації, що відображає інтереси суспільства і держави. Характеристикою такого процесу

є часові затримки $t_{рбл}$/ $_{дж}$ на розблокування доступу до інформаційного ресурсу.

З іншого боку для здійснення фільтрації інформаційних ресурсів, які містять деструктивний інформаційно-психологічний вплив, потрібно вносити додаткові затримки $t_{обр}$ / $i_п$ на реалізацію відповідної обробки.

2. Цілісність інформаційного ресурсу здатність зберігати вихідний семантичний зміст відеоінформації, в умовах: ведення інформаційного протиборства; існуючих характеристик процесів обробки, передачі, зберігання інформації в незалежності від територіальної прихильності її джерела і одержувача [6, 5]. З одного боку противник прагне порушити категорію цілісності інформаційного ресурсу, які відображають конструктивний підхід в інтересах суспільства і державної політики. Тут використовується показник ступеня внесених втрат цілісності інформації в результаті деструктивного ІТ впливу противника. З іншого боку процеси фільтрації деструктивного інформаційно-психологічного впливу можуть супроводжуватись внесенням коригувань в передані інформаційні потоки. Цей процес також може супроводжуватись втратами цілісності інформації.

3. Конфіденційність інформаційного ресурсу. З одного боку противник прагне отримати несанкціонований доступ до інформаційних ресурсів для збору відомостей про об'єкти деструктивного ІП впливу. З іншого боку для виявлення деструктивного інформаційно-психологічного впливу потрібно такий же доступ отримати для відповідних технологій протидії деструктивним впливам.

ІІ. З іншого боку потрібно забезпечити безпеку суспільства в інформаційно-психологічному просторі, тобто мінімізувати збиток від деструктивного інформаційно-психологічного впливу, а саме мінімізувати ймовірність модифікації психологічного, морального, мотиваційного та інтелектуального стану особистості.

В цьому випадку в процесі створення технологій протидії деструктивному інформаційно-психологічному впливу потрібно враховувати наявність наступного протиріччя.

Проведемо визначення найбільш актуальних і значущих загроз втрати інформаційно-психологічної безпеки суспільства.

Деструктивні інформаційно-психологічні впливи діляться на дві групи, а саме: відкритий і прихований інформаційно-психологічний вплив.

Відкритий деструктивний інформаційно-психологічний - такий вплив, коли об'єкт цілком усвідомлює цілі впливу, засоби, які використовує суб'єкт, особливості процесу впливу.

Прихований (сугестивний) деструктивний інформаційно-психологічний вплив (маніпуляція) це такий вплив, коли жоден з перерахованих аспектів об'єктом не усвідомлюється.

Найбільш складними з позиції: виявлення та організації протидії; нанесення шкоди є сугестивні деструктивні інформаційно-психологічні впливи. Це обумовлено тим, що:

1) сугестивні інформаційно-психологічні атаки на відміну від відкритих атак впливають на підсвідомість особистості. У зв'язку з чим, збиток від дії таких атак більш значний і досягається за більш короткі часові терміни з залученням меншої кількості інформаційних контейнерів;

2) сугестивні інформаційно-психологічні атаки по своїй суті є прихованими і можуть маскуватися під конструктивні інформаційні ресурси. Необхідно враховувати, що в інформації, що є за своїм змістом конструктивною може виявитися деструктивною за своєю дією на підсвідомість (сугестивного канал). Також інформація, яка є "цікавою" може призвести до неусвідомлюваних психобіологічніх негараздів, стимулюючі девіантну поведінку особини та руйнуючі позитивні соціальні тенденції в суспільстві. Це є причиною виникнення складнощів виявлення таких інформаційних деструкцій;

3) виявлення прихованих деструктивних інформаційно-психологічних впливів вимагає набагато більших витрат часового ресурсу на їх виявлення і блокування. Це обумовлено тим, що такі атаки додатково залучають більшу глибину аналізу тестової інформації до рівня врахування психологічно-емоційної та внутрішньо-установочної складової особистості. Така обставина призводить до втрати доступності інформаційного контейнера, тобто порушується інформаційна безпека в ІТ просторі.

Отже, сугестивні деструктивні інформаційно-психологічні атаки є найбільш перспективними, та складають базу для інформаційних операцій третього покоління. Такі інформаційно-психологічні впливи є найбільш актуальними та значущими серед різних типів деструктивних ІП атак (рис. 3.4).

Одними з ключових інформаційно-психологічних атак, які здійснюються в сучасному інформаційно-комунікаційному просторі, тут є наступні:

а) аудіосуггестія, приховані вставки в аудіопотоки;

б) сугестія текстів.

Це пояснюється найбільшим опрацюванням відповідних ІТ засобів і методів у протиборчої сторони щодо організації деструктивних впливів на інформаційно-психологічних та інформаційно-емоційному рівнях. Тому потрібно провести дослідження існуючих інформаційних технологій і методів протидії різним інформаційно-психологічним атакам. Тут потрібно враховувати умови (обмеження) інформаційної протидії, а саме забезпечення вимог (категорій інформаційної безпеки підлітків в ІТ просторі) щодо доступності, цілісності інформаційних ресурсів особистості, соціуму і держави. Іншими словами потрібно забезпечить умови мережецентричності безпеки підлітка в інформаційному просторі.

Значить по викладеному матеріалу можна зробити такі висновки:

- розроблена модель загроз інформаційно-психологічної безпеки особистості в умовах інформаційного протиборства і демократизації соціуму, коли потрібно забезпечити баланс безпеки особистості одночасно в інформаційно-психологічних та ІТ просторах (умова мережецентричності безпеки людини в інформаційному просторі);
- обґрунтовано, що найбільш актуальними і значущими загрозами ІП безпеки особистості з позиції: виявлення та організації протидії; нанесення шкоди є сугестивні деструктивні інформаційно-психологічні впливи;
- показано, що одними з ключових інформаційно-психологічних атак, які здійснюються в сучасному інформаційно-комунікаційному просторі, є деструктивні інформаційні модифікації в аудіоконтейнерах і електронних текстових ресурсах, а саме: аудіосуггестія, приховані вставки в аудіопотоки

3.2. Інформаційна технологія виявлення деструктивного інформаційно-психологічного впливу на підсвідомість особистості

Викладається побудова інформаційної моделі аналізу ТІР на основі формування семантичного диференціала. На основі розробляється метод виділення значущих лінгвістичних біполярних ознак.

Розробляється метод ідентифікації інформаційно-психологічний вплив структурних компонент (слів) текстових інформаційних ресурсів на підсвідомість особистості на основі формування векторного семантичного диференціала.

Викладаються основні етапи побудови статичних підходів до статичного аналізу інформаційно-психологічного впливу тексту на підсвідомість особистості на основі усереднення ВП впливу окремих слів на підсвідомість особистості. Створюється комплексний метод виявлення прихованого інформаційно-психологічного впливу в текстовому інформаційному ресурсі на підсвідомість особистості в багатовимірному

фонетичному просторі з прив'язкою до векторних градаційних двополюсних шкал значущих біполярних лінгвістичних ознак на основі формування семантичного диференціала слів і обробкою їх по динамічній технології з накопиченням фрагментарної інформації. Тут базовими технологічними компонентами є: метод динамічного аналізу ТІР з накопиченням його фрагментів на основі формування одновимірного семантичного диференціала; метод динамічного аналізу ТІР з накопиченням його фрагментів на основі оцінки фонетичної значущості слова за однополярною значимою лінгвістичною ознакою

3.2.1. Дослідження інформаційної моделі аналізу текстових інформаційних ресурсів на основі формування семантичного диференціалу для виявлення прихованого впливу на підсвідомість особистості

Виявлення сугестивних інформаційних деструкцій в ТІР забезпечується на основі відповідного їх аналізу. При цьому такий аналіз потрібно здійснювати з врахуванням закономірностей звукового впливу ТІР на підсвідомість особистості.

В цьому напрямку ключовим підходом є метод семантичного диференціалу [4, 13, 16].

Семантичний диференціал – це технологія аналізу текстових структурних одиниць (елементів) S на основі встановлення кількісних оцінок (фонетичних значень) за сукупністю Θ характерних лінгвістичних біполярних ознак (область ознакового аспекту), що формуються на основі пар антонімів.

Залежно від рівня інтегрованості текстові структурні одиниці (елементи) розглядаються на трьох рівнях, а саме:

- рівень окремих слів S_{word} (текстовий структурний компонент першого порядку);

- рівень текстових фрагментів S_{frg} (текстовий структурний компонент другого порядку);
- рівень цілих текстових документів S_{doc} (текстовий структурний компонент третього порядку – ***текстовий інформаційний ресурс***).

Кількість Q_θ таких лінгвістичних біполярних (ЛБ) ознак вибирається експертним шляхом з урахуванням адаптації щодо предметної області. Відповідно сукупність Θ таких ЛБ ознак, $\Theta = \{\theta_i\}$, $i=\overline{1,Q_i}$, з урахуванням предметної області характеризує простір Ω підсвідомого звукового відчуття особистості.

Біполярність ознаки θ_i має на увазі під собою наявність пари антонімів, тобто $\theta_i = \{\alpha_i; \overline{\alpha}_i\}$, $i = \overline{1,Q_\theta}$ [5, 3, 10]. Відповідно формуються два полюси - антонімів характерних лінгвістичних ознак, а саме α_i - позитивний полюс і-го лінгвістичного ознаки з позиції сприйняття звуків на підсвідомість особистості. Відповідно $\overline{\alpha}_i$ - негативний полюс і-го лінгвістичного ознаки, формується як антонім щодо позитивного полюса α_i (рис. 3.4).

Зони істотних відхилень Рисунок 3.4 – Структурна схема лінгвістичної біполярної ознаки

У центрі шкали такого ознаки знаходиться нульовий (нейтральний) рівень $\alpha_{0,i}$, навколо якого утворюється нейтральна зона. Нейтральна зона використовується для виявлення незначущості впливу вибраної ознаки на підсвідомість особистості з урахуванням особливостей обраної предметної області. В табл. 3.1 наведено характерний приклад формування біполярних

ознак для $Q_\theta = 25$. У цьому випадку формується 25 біполярних шкал для лінгвістичних біполярних ознак, за якими визначається семантичний диференціал. Для отримання фонетичних значень $f_{i,\tau}$ букв s_τ (s_τ - τ -я буква алфавіту) текстових інформаційних ресурсів по ЛБ ознаками необхідно сформувати їх.

№ шкали, i	Ознаковий аспект, θ_i		№ шкали, i	Ознаковий аспект, θ_i	
	антонім 1	антонім 2		антонім 1	антонім 2
1	хороший	поганий	14	веселий	сумний
2	великий	маленький	15	безпечний	страшний
3	ніжний	грубий	16	величний	низинний
4	жіночий	мужній	17	яскравий	тьмяний
5	світлий	темний	18	округлий	незграбний
6	активний	пасивний	19	радісний	сумний
7	простий	складний	20	гучний	тихий
8	сильний	слабкий	21	довгий	короткий
9	гарячий	холодний	22	хоробрий	боягузливий
10	швидкий	повільний	23	добрий	злий
11	гарний	відштовхуючий	24	могутній	кволий
12	гладкий	шорсткий	25	рухомий	повільний
13	легкий	важкий			

Таблиця 3.1 — Характерне формування 25 пар антонімів лінгвістичних біполярних ознак для розрахунку семантичного диференціалу.

Для отримання фонетичних значень $f_{i,\tau}$ букв s_τ (s_τ - τ -я буква алфавіту) текстових інформаційних ресурсів по ЛБ ознаками необхідно сформувати їх пис у вигляді звуко-букв b_τ (b_τ - τ -а звуко-буква). Це пояснюється тим, що самі літери при написанні не враховують всіх психологічно важливих

особливостей звуків. Одна буква безпосередньо не може відобразити м'яку і тверду приголосну. Навпаки, звуко-букви враховують особливості вимови.

У цьому випадку забезпечується облік вимови двох букв (поточної і наступної за нею). Відповідно варіації звучання всіляких двобуквених комбінацій утворюють алфавіт звуко-букв. Потужність такого алфавіту позначається як Q_b . Наприклад, для українських текстів існує Q_b =33 звуко-букв b_τ, τ=1,33 в залежності від звучання букв алфавіту української мови.

Кожній звуко-букві b_τ потрібно поставити кількісне значення $f_{i,\tau}$ відповідно до обраної шкали лінгвістичних біполярних ознак. Це дозволяє ідентифікувати рівень впливу кожної звуко-букви в просторі звукових відчуттів особистості. У цьому випадку кожна звуко-буква алфавіту детектується (розкладається) по Q_θ характерними біполярним ознаками

Таке детектування проводиться експертним шляхом. В цьому випадку виставляються експертні оцінки $f_{i,\tau}$ з урахуванням сприйняття кожної звуко-букви по градаціях шкал біполярного ознакового простору. Це задається таким співвідношенням:

$$\varphi_{sd} : b_\tau \xrightarrow{\theta_i = \{\alpha_i ; \overline{\alpha}_i\}} f_{i,\tau}, \quad \tau = \overline{1, Q_b}, \quad i = \overline{1, Q_\theta}.$$

Тут φ_{sd} - функціонал встановлення кількісного відповідності кожної звукобукви біполярній ознаці; $f_{i,\tau}$ - фонетичне значення τ -й звуко-букви по і-ій біполярній ознаці.

Фізичний сенс фонетичного значення. Величина $f_{i,\tau}$ позиціонує τ -у звукобукву по шкалі і-і біполярної ознаки.

Величина $f_{i,\tau}$ кількісно відображає рівень позиціонування звуко-букви щодо позитивного і негативного її відчуття на підсвідомому рівні особистості (підлітка). Значить величина $f_{i,\tau}$ кількісним чином встановлює рівень і напрямок інформаційно-психологічного впливу τ-й звуко-букви на підсвідомість підлітка по і-ій біполярній ознаці.

Весь процес можна назвати як ***ідентифікація звуко-букви в просторі ознак звукових відчуттів особистості на його підсвідомому рівні***. Така ідентифікація проводиться шляхом позиціонування звуко-букви на шкалах біполярних ознак. Приклад таблиці формування фонетичних оцінок для 33 звуко-букв за Q_b ЛБ ознаками наведено в **Додатоку Б**.

Для кількісної оцінки ступеня значимості біполярної ознаки θ_i ***пропонується*** використовувати ***інформаційний підхід***. Тоді, чим більше ступінь $V(F_i)$ невизначеності (інформативності ознаки), тим вище його значимість для визначення рівня впливу звуко-букв на підсвідомість людини через звукове сприйняття. В даному випадку цікавить невизначеність без урахування знака впливу звукобукв на підсвідомість людини (позитивне чи деструктивне). Тому для проведення такої оцінки пропонується використовувати величини ${}_{\Delta}f_{i,\tau}$, рівні абсолютним значенням відхилень відповідних фонетичних значень $f_{i,\tau}$ щодо нульового рівня h_0 градаційній шкали біполярних ознак θ_i, а саме:

$$ {}_{\Delta}f_{i,\tau} = |h_0 - f_{i,\tau}|. $$

В цьому випадку для і-ї біполярної ознаки утворюється послідовність ${}_{\Delta}F_i$ відліків (фонетичних значень), тобто:

$$ {}_{\Delta}F_i = \{ {}_{\Delta}f_{i,1}, \ldots, {}_{\Delta}f_{i,\tau}, \ldots, {}_{\Delta}f_{i,Q_b} \}, $$

довжина якої дорівнює Q_b.

Кожен такий відлік ${}_{\Delta}f_{i,\tau}$ в загальному випадку є дійсним числом, і буде обмежений зверху цілочисельною величиною ${}_{\Delta}f_{i,max}$, що задається наступною нерівністю:

$$ 0 \le {}_{\Delta}f_{i,\tau} < {}_{\Delta}f_{i,max}. $$

У цьому співвідношенні величина $_{\Delta}f_{i,max}$ визначається за формулою:

$$_{\Delta}f_{i,max} = ((\max_{1\le\tau\le Q_b} {}_{\Delta}f_{i,\tau} - \min_{1\le\tau\le Q_b} {}_{\Delta}f_{i,\tau})/\delta_i) + 1,$$

де δ_i - крок дискретизації величин $_{\Delta}f_{i,\tau}$ для послідовності $_{\Delta}F_i$.

Тому *послідовність* $_{\Delta}F_i$ *пропонується розглядати як число в матеріальному нерівноважному просторі ознак* Ω. Звідки кількість $V(F_i)$ інформації (ступінь інформативності ознаки θi) буде визначатися як

$$V(F_i) = [\ell og_2 \prod_{\tau=1}^{Q_b}((\max_{1\le\tau\le Q_b} {}_{\Delta}f_{i,\tau} - \min_{1\le\tau\le Q_b} {}_{\Delta}f_{i,\tau})/\delta_i) + 1)] + 1.$$

Чим більше величина $V(F_i)$, тим вище інформативність біполярної ознаки θ_i. І, навпаки, зниження величини ($_{\Delta}f_{i,\tau}$ +1) відповідає зменшенню ступеня невизначеності розподілу значень $_{\Delta}f_{i,\tau}$ для відповідної ознаки.

Визначення величин $V(F_i)$ для всіх ознак простору Ω, тобто. i=1, Q_θ дозволяє виділити найбільш значущі біполярні ознаки для проведення оцінки ступеня ІП впливу звуко-букв на підсвідомість людини через його звукове сприйняття. Відсікання незначущих ознак проводиться з використанням порогового значення $V(F)_h$. Тоді, якщо виконується нерівність

$$V(F_i) < V(F)_h, \qquad (3.6)$$

то і-й ознака є незначимим. Навпаки, для умови $V(F_i) \ge V(F)_h$ біполярна і-а ознака буде значимою, тобто. $\theta_i \rightarrow \theta(h)_i$. Послідовність значущих ознак буде позначатися як $\Theta(h)_i = \{\theta(h)_1,...,\theta(h)_i,...,\theta(h)_{Qh}\}$. В результаті такої селекції подальша обробка ТІР буде здійснюватися з використанням інформації тільки по значимим біполярним ознакам $\theta(h)_i$

Значить по викладеному матеріалу можна зробити висновок, побудована (***вперше***) інформаційна модель аналізу ТІР на основі формування семантичного диференціала (формування фонетичних оцінок з прив'язкою до двополюсної шкали лінгвістичних ознак). На основі чого були розроблені:

- метод виділення значущих лінгвістичних біполярних ознак на основі представлення фонетичних оцінок звуко-букв алфавіту в матеріальному нерівноважному позиційному просторі. Основна відмінність тут складається в тому, що векторний фонетичний простір лінгвістичної біполярної ознаки по всім звуко-буквах представляється в двополярному матеріальному нерівноважному позиційному базисі. Це дозволяє використовувати в процесі аналізу ТІР тільки значущі ЛБ ознаки, що в кінцевому підсумку скорочує часові затримки на обробку ТІР.

3.3. Розробка методу виявлення прихованого інформаційно-психологічного впливу в локальній компоненті текстового інформаційного ресурсу на підсвідомість особистості на основі семантичного диференціала

Для виявлення прихованого інформаційно-психологічного впливу в структурних компонентах ТІР ***пропонується*** використовувати технологію семантичного диференціала. В цьому випадку структурна компонента ТІР представляється в фонетичному просторі (просторі сприйняття звуків на рівні підсвідомості особистості) з урахуванням прив'язки до двополюсної (біполярної) шкали лінгвістичних ознак, тобто з урахуванням позиціонування щодо негативного і позитивного полюсів.

Фонетичний опис структурних компонент ТІР представляє собою семантику їх звукового сприйняття але тільки не на свідомому рівні, а на рівні підсвідомості особистості. Диференціал визначається наявністю прив'язки до двополюсної шкали лінгвістичних ознак.

У загальному випадку визначення спрямованості прихованого ІП впливу слова на підсвідомість особистості в фонетичному просторі з

використанням технології семантичного диференціала пропонується організовувати на основі двох підходів, а саме:

1. Перший підхід базується на визначенні прихованого ІП впливу структурних компонент ТІР на основі фонетичних оцінок з прив'язкою до окремих лінгвістичних біполярних ознак (одномірний фонетичний простір по ЛБ ознаці). Відповідно кількість таких оцінок буде дорівнює кількості Q_h значимих ЛБ ознак.

2. Другий підхід полягає у визначенні інтегрованих оцінок фонетичного впливу структурних компонент ТІР на підсвідомість особистості за всіма ЛБ ознаками. Тут розглядається векторний простір звукового впливу на підсвідомість особистості.

Перевага першого підходу полягає в тому, що існує можливість визначити деструктивність прихованого ІП впливу слова (структурної компоненти ТІР першого порядку) по конкретним лінгвістичним ознаками, тобто досягається деталізація аналізу ТІР за словами на предмет виявлення інформаційних деструкцій. Таку інформаційну технологію аналізу ТІР допускається використовувати для створення експертних систем підтримки та прийняття рішень спеціальними психологічними і реабілітаційними центрами. Наприклад, така технологія може використовуватися для створення автоматизованих робочих місць дитячих психологів, як підтримка процесу оцінки морально-психологічного стану підлітків, оцінки наявності інформаційних деструкцій в ІР в автоматизованому режимі, створення спеціальних ТІР для коригувальних ІП впливів в напрямку нормалізації і гармонійності розвитку особистості.

У той же час такий підхід не забезпечує отримання інтегрованих оцінок. У свою чергу інтегровані оцінки дозволяють підвищити ефективність всього інформаційно-технологічного процесу інформаційно-психологічної протидії, а саме:

- по-перше скорочуються часові затримки на обробку великої сукупності фонетичних значень по кожній ЛБ ознаці, а також знижується обсяг пам'яті на зберігання результатів аналізу. Це створює умови для забезпечення таких категорій інформаційної безпеки особистості як доступність і цілісність ІР;

- по-друге інтегрована оцінка створює можливість для створення технологій інформаційно-психологічної корекції ТІР без їх блокування.

Другий підхід для аналізу ТІР допускає своє використання як складова етапу інформаційної технології забезпечення ІП безпеки підлітків в інфокомунікаційних просторі. Тут використовується перевага другого підходу, що складається в автоматичної обробки ТІР без участі особи приймаючої рішення. Тоді існує можливість використовувати такий підхід для:

- моніторингу Інтернет ресурсів;
- створення спеціальних мережевих фільтрів для виявлення прихованого деструктивного ІП впливу в автоматичному режимі.

Введемо структурну одиницю текстового повідомлення першого порядку

$S^{(}\ell;t)_u$, де $S^{(}\ell;t)_u$ - u -е слово для t -го фрагмента ℓ -го документа (закінченого за змістом повідомлення). Величина $S(\ell;t)_u$ є лінгвістичної змінною, довжина

$|\ S(\ell;t)_u\ |$ якої дорівнює кількості букв в слові, тобто.

$$S(\ell;t)_u=\{s(\ell;t)_{u,1},...,s(\ell;t)_{u,\tau},...,s(\ell;t)_{u,|S(\ell;t)u|}\}, \qquad (3.7)$$

де $s(\ell;t)_{u,\tau}$ - τ-а буква для слова $S(\ell;t)_u$, $\tau = 1, |S(\ell;t)_u|$.

Для оцінки такого сугестії все вихідне текстове слово $S(\ell;t)_u$ виражається через звуко-слово $B(\ell;t)_u$. Дане перетворення задається

функціоналом φ_{vc}, званим також звуковим компілятором (voice compiling) текстового слова, тобто:

$$\varphi_{vc} : S(\ell;t)_u \rightarrow B(\ell;t)_u . \qquad (3.8)$$

В результаті чого, формується лінгвістична змінна (звуко-слово)$B(\ell;t)_u$, що має довжину $| B(\ell;t)_u |$ звуко-букв., тобто

$$B(\ell;t)_u = \{b(\ell;t)_{u,1},...,b(\ell;t)_{u,\tau},...,b(\ell;t)_{u,|B(\ell;t)u|}\}, \qquad (3.9)$$

де $B(\ell;t)_u$ - u -е звуко-слово для t -го фрагмента ℓ -го документа (закінченого за змістом повідомлення); $b(\ell;t)_{u,\tau}$ - τ-я звуко-буква для звуко-слова $B(\ell;t)_u$,

$\tau = 1, | B(\ell;t)_u$.

Після чого здійснюється фонетичний аналіз кожної звуко-букви $b(\ell;t)_{u,\tau}$ окремо. Для всіх звуко-букв слова $B(\ell;t)_u$ формуються фонетичні значення

$f(\ell;t;u)_{i,\tau}$. Тут використовується наступне функціональне перетворення:

$$\varphi_{sd} : b(\ell;t)_{u,\tau} \xrightarrow{\theta_i = \{\alpha_i; \overline{\alpha}_i\}} f(\ell;t;u)_{i,\tau}, \quad \tau = \overline{1, | B(\ell;t)_u |}, \quad i = \overline{1, Q_h},$$

(3.10)

де $f(\ell;t;u)_{i,\tau}$ - фонетичне значення τ-ї звуко-букви по і-ій біполярній ознаці для u -го звуко-слова t -го фрагмента ℓ -го документа (закінченого за змістом повідомлення або текстового інформаційного ресурсу (ТІР)); Q_h - кількість значущих ознак для досліджуваної предметної сфери з позиції значущості впливу на підсвідомість людини через його звукові відчуття.

Шкала відхилень семантичного диференціала по їх фонетичним значенням для лінгвістичного біполярного ознаки представлена на рис. 3.1. Центральне значення шкали h_0 дорівнює 3,0. Це нейтральне значення, яке не може виділити жоден ознаковий аспект. Так само нейтральною зоною вважається зона від 2,5 до 3,5. Значення в цих межах вважаються незначними коливаннями. Все що виходить за межі коливань, можна вважати відхиленням від норми відповідно в напрямку позитивного або негативного інформаційно-психологічного впливу. Саме зони істотного відхилення говорять нам про те, до якого ознакового аспекту можна віднести букву та все слово, як структурний компонент текстового інформаційного ресурсу. Оцінки є імовірнісними, тобто, підтверджені випадковим коливанням. При цьому самі ознакові аспекти не варто погоджувати із значенням слова. Це обумовлено тим, що оцінка дається по змістовності звукової форми, а не за значенням слова.

Розглянемо перший підхід. Тут проводиться оцінка сугестивного впливу звуко-слова на підсвідомість особистості через його звукове сприйняття в одновимірному фонетичному просторі, тобто в фонетичному просторі з прив'язкою до шкалою окремих ЛБ ознак.

Визначити семантичну складову для слова на базі першого підходу можна ***двома основними способами***.

Першим і більш простим варіантом розрахунку є визначення середньої

$F(\ell;t;u)_i$ значимості всіх звуко-букв в слові по і-ій лінгвістичній біполярній ознаці. Визначення величини $^{F}(\ell;t;u)_i$ проводиться по формулі:

$$F(\ell;t;u)_i = \sum_{\tau=1}^{|B(\ell;t)_u|} f(\ell;t;u)_{i,\tau},$$

де $f(\ell;t;u)_{i,\tau}$ - фонетичне значення τ-й звуко-букви по і-му біполярному признаку для u -го звуко-слова t -го фрагмента ℓ -го документа (закінченого по змістом повідомлення або TIP);

$|B^{(\ell};t)_u|$ - кількість звуко-букв в слові $B^{(\ell};t)_u$.

Фонетичне значення $f(\ell;t;u)_{i,\tau}$ звуко-букв це встановлена ймовірнісна величина, яка визначається та корегується експериментальним шляхом. Фонетичне значення $f(\ell;t;u)_{i,\tau}$ для кожної звуко-букви встановлюється окремо залежно від шкали ЛБ ознак, за якою здійснюється аналіз. У табл. 3.2 наведена частина фонетичних значень звуко-букв для трьох шкал ЛБ ознак.

Ознакова шкала для розрахунку семантичного диференціалу	Звуко-буква				
	А	Б	В	Г	Д
хороший – поганий	1,5	2,4	2,9	3,2	2,4
світлий – темний	2,2	3,2	3,0	3,3	3,2
красивий – відштовхуючий	2,0	2,6	3,0	2,8	2,4

Таблиця 3.2 — Фрагмент фонетичного значення звуко-букв

Однак даний підхід визначення семантичної складової для слова за формулою (3.11) не дає точного уявлення про значущість слова, так як не всі звуко-букви в слові є рівноправними.

В цьому випадку пропонується враховувати наступні особливості.

По-перше. Психологи вважають, що для людини перший звук у слові має куди більше значення, ніж інші, за їх твердженням він в 4 рази помітніше. Так само не варто забувати про ударний звук, він так само виділяється в слові, хоча і не так як перший, тільки в 2 рази. Це говорить нам про те, що при розрахунку сумарної фонетичної складової всіх звуко-букв слова, вагу першого потрібно збільшити в 4 рази, а ударного в 2 рази.

По-друге. Крім розташування букв у слові, не менш важливу роль грає зустрічальність букв в словах. Тобто, є букви, які часто зустрічаються (наприклад, А, О, Т, Н), а є, які рідко зустрічаються (наприклад, Ф, Х). Пи цьому ті букви, що рідко зустрічаються є більш помітними в словах в процесі їх фонетичного представлення. Звідси випливає висновок, що при розрахунку фонетичної значимості слова потрібно брати до уваги зустрічальність букв в словах. Коефіцієнт зустрічальності, або частотність, визначається з урахуванням кількості разів зустрічаємості букви на тисячу звукобукв.

По-третє. Звукобукви ж у свою чергу ще поділяються на ударні і безударні.

З цього випливає що інформативність (фонетична помітність) звуко-букви знаходиться в зворотній залежності від її частотності (зустрічальності). Тобто найменш інформативна звуко-буква має максимальну частотність. Навпаки звукобуква буде в стільки разів інформативніше, скільки разів її частотність менше максимальної для звуко-букв даного слова.

Тому, при розрахунку фонетичної складової звукового комплексу потрібно збільшити вагу середніх оцінок для: першої, ударної звуко-букви, та для всіх звуко-букв, крім звуко-букви з максимальною частотою. Вираз для визначення коефіцієнту $k(\ell;t;u)_{i,\tau}$ кожної звуко-букви $b(\ell;t)_{u,\tau}$ в звуко-слові $B(\ell;t)_u$ має наступний вигляд:

$$k(\ell;t;u)_{i,\tau} = P(\ell;t;u)_{i,\tau}^{(max)} / P_\tau,$$

де $P(\ell;t;u)_{i,\tau}^{(max)}$ – це максимальна частотність звуко-букви $b(\ell;t)_{u,\tau}$ в даному

слові $B(\ell;t)_u$; P_τ – це табличне значення частотності звукобукви (**Додаток Б**).

Відповідно для першої звуко-букви необхідно збільшити значення коефіцієнта $k(\ell;t;u)_i,1$ в 4 рази. Тоді вираз (3.12) запишеться як:

$$k(\ell;t;u)_{i,l} := 4k(\ell;t;u)_{i,l} = 4P(\ell;t;u)_{i,\tau}^{(max)} / P_{\tau}.$$

Для ударної звуко-букви необхідно збільшити значення коефіцієнта в 2 рази, тобто вираз (3.12) прийме вигляд:

$$k(\ell;t;u)_{i,\tau}^{(уд)} = 2\, k(\ell;t;u)_{i,\tau} = 2P(\ell;t;u)_{i,\tau}^{(max)} / P_{\tau}. \qquad (3.14)$$

З урахуванням коефіцієнтів $k(\ell;t;u)_{i,\tau}$ кожної звуко-букви $b(\ell;t)_{u,\tau}$, оцінка фонетичної складової $F'(\ell;t;u)_i$ слова $B(\ell;t)_u$ *по* і-*ій лінгвістичній біполярній ознаці* проводиться за такою формулою:

$$F'(\ell;t;u)_i = \Big(\sum_{\tau=1}^{|B(\ell;t)_u|} k(\ell;t;u)_{i,\tau}\, f(\ell;t;u)_{i,\tau}\Big) / \sum_{\tau=1}^{|B(\ell;t)_u|} k_i\,,$$

де $f(\ell;t;u)_{i,\tau}$ - фонетичне значення τ-й звуко-букви по і-ій біполярній ознаці для u -го звуко-слова t -го фрагмента ℓ -го документа (закінченого за змістом повідомлення або текстового інформаційного ресурсу (ТІР)); $|B(\ell;t)_u|$ - кількість звуко-букв в слові $B(\ell;t)_u$.

1. Створений (*вдосконалений*) метод побудови одновимірного семантичного диференціала для оцінки рівня і напряму ІП впливу структурних компонент ТІР в фонетичному просторі з урахуванням прив'язки до градаційних двополюсних шкал окремих значущих ЛБ ознак. Відмінний аспект полягає у використанні для побудови фонетичного простору тільки значущих біполярних лінгвістичних ознак..

2. Розроблений (*вперше*) метод ідентифікації інформаційно-психологічний вплив структурних компонент (слів) текстових інформаційних ресурсів на підсвідомість особистості на основі формування векторного семантичного диференціала. Метод базується на таких етапах:

– встановленні векторної фонетичної оцінки рівня і спрямованості ІП впливу звуко-букв по всім біполярним лінгвістичним ознакам;

- здійснення векторної фонетичної ідентифікації рівня і напряму ІП впливу структурної компоненти (слова) ТІР на підсвідомість особистості за всіма звукобуквами в значнимому двополюсному лінгвістичному біполярному просторі, який представлений як матерільний нерівноважний базис;
- визначення векторного семантичного диференціала на основі ідентифікації інтегрованих фонетичних оцінок за всіма біполярним поступовим шкалами значущих лінгвістичних ознак з урахуванням детектування двобічного ІП впливу (конструктивний і деструктивний) в двовимірному матеріальному нерівноважному просторі.

3. Побудований (*отримав подальший розвиток*) комплексний метод виявлення прихованого ІП впливу в локальній компоненті ТІР на підсвідомість особистості в багатовимірному фонетичному просторі з прив'язкою до векторних градаційних двополюсних шкал біполярних лінгвістичних ознак на основі формування семантичного диференціала.

У той же час метод аналізу ТІР на основі формування семантичного диференціала має суб'єктивний розмах з урахуванням біполярності лінгвістичного простору, тобто фонетичні оцінки можуть «тяжіти» до різнополярних характеристик. Це розмиває кінцевий результат оцінки ІП впливу слова (структурної компоненти ТІР) на підсвідомість особистості, і може створити невизначеність. Тому *пропонується* додатково враховувати фонетичний аналіз семантичної складової слова, що враховує тільки однополярні характеристики. Тут додатково *пропонується* розглянути закономірність в фонетичному поданні звуко-слів, що складається у врахуванні частоти відхилення фонетичних значень звуко-букв щодо нормативного рівня частоти появи звуко-букв в текстах.

ВИСНОВКИ

Метод виявлення деструктивного інформаційно-психологічного впливу в соціотехнічних системах є актуальним та важливим в сучасному світі, особливо з відкриттям нових можливостей для впливу на суспільство за допомогою інформаційних технологій.

Розроблений метод виявлення деструктивного інформаційно-психологічного впливу в соціотехнічних системах є важливою складовою інформаційної безпеки сьогодення, оскільки він стосується різних сфер життя і може мати велике значення для сучасного соціуму, захисту від маніпуляцій та покращення психологічного здоров'я користувачів.

У нашому дослідженні нами було виконано усі визначені завдання, а саме:

1. Проаналізовано сучасні алгоритми виявлення деструктивного впливу в соціотехнічних системах, розкрито психологічні аспекти деструктивного впливу, зокрема впливу на психіку та поведінку користувачів, що можуть допомогти краще розуміти механізми атак та розвивати ефективні методи захисту. Зроблено висновок, щодо важливості розвивати механізми взаємодії з користувачами та співпрацю з ними для виявлення та реагування на деструктивний вплив.

2. Досліджено методології виявлення видів деструктивного інформаційно-психологічного впливу в соціотехнічних системах. А саме:

Існуючі інформаційні технології та методи в залежності від глибини аналізу текстової інформації розглянуто за трьома класами. До першого класу відносяться технології та методи, які забезпечують аналіз IP за ключовими словами. Відповідно такі методи дозволяють з одного боку створювати, а з іншого боку виявляти інформаційні атаки першого покоління. До другого – інформаційні технології та методи, які додатково дозволяють аналізувати семантичний контент електронних TIP. Третій клас інформаційних технологій та методів формують такі технологічні рішення,

які додатково дозволяють збільшити глибину аналізу текстової інформації до рівня врахування психологічно-емоційної та внутрішньо-установочної складової особистості.

3. Проаналізовано сучасні алгоритми та програмні засоби для виявлення деструктивного впливу на основі відкритих методологій.

4. Розроблено метод виявлення деструктивного інформаційно-психологічного впливу в соціотехнічних системах. Який включає головну особливість - це ідентифікація інформаційно-психологічного впливу структурних компонент (слів) текстових інформаційних ресурсів на підсвідомість особистості на основі формування векторного семантичного диференціала

Наше дослідження спрямоване на досягнення загальної мети - створення ефективного методу виявлення деструктивного впливу в соціотехнічних системах і забезпечення захисту суспільства від цього впливу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Voitovych, O., Kupershtein, L., Holovenko, V. (2022). Виявлення фейкових облікових записів в соціальних мережах. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(18), 86-98. https://doi.org/10.28925/2663-4023.2022.18.8698

2. ChenhaoTan.(ICWSM 2016).Unfolding News Cycles from the Source.Proceedings of the Tenth International Conference on Web and Social Media C.378-387.

http://www.aaai.org/ocs/index.php/ICWSM/ICWSM16/paper/view/13011

3. Gnatyuk, S., Zhmurko, T. (2016). Information-Psychological Security of Society in the Context of Information Warfare. In J. Rysiński (Ed.), Inżynier XXI wiekuprojectujemyprzyszlosc (pp. 321-341). Bielsko-Biała: Wydawnictwo Naukowe AkademiiTechniczno-Humanistycznej w Bielsku-Białej.

4. Komarov, M., Honchar, S., Dimitriieva, D. (2021). Дослідження проблеми кіберживучості об'єктів критичної інформаційної інфраструктури. Ядерна та радіаційна безпека, 1(89), 59-66.

https://doi.org/10.32918/nrs.2021.1(89).07https://nuclear-journal.com/index.php/journal/article/view/771

5. Richard Brodie. (2011)Virus of the Mind: The New Science of the Meme Paperback. 256 p. Hay House Inc.; Reissueedition.

6. GeneSharp198 METHODS OF NONVIOLENT ACTION.

https://www.aeinstein.org/nonviolentaction/198-methods-of-nonviolent-action/

7. Cook, T. (2019). Technology does not need vasttroves of personal data. Advertising existed and thrived for decades with outit. https://www.marketingweek.com/apple-data-privacy

8. Васильків І. М. (2020). Основи теорії ймовірностей і математичної статистики.

https://new.mmf.lnu.edu.ua/wp-content/uploads/2020/04/Vasyl-kiv-I.M.-TIMS_CHASTYNA_1.pdf

9. Дудатьєв, А. В., Войтович, О. П. (2017). Інформаційна безпека соціотехнічних систем: Модель інформаційного впливу. Інформаційні технології та комп'ютерна інженерія, 38(1), 16–21. https://itce.vntu.edu.ua/index.php/itce/article/view/657

10. Лужецький В. А., Дудатьєв А.В. (2017). Концептуальна модель системи інформаційного впливу. Безпека інформації, 23 (1), 45–49.https://doi.org/10.18372/2225-5036.23.11550

11. С. В. Волобуев, *Безопасность социотехнических систем*. Обнинск, Россия: Викинг, 2012.

12. Г. А. Остапенко, и Е. А. Мешкова, *Информационные операции и атаки в социотехнических системах*. Москва, Россия: Горячая линия-Телеком, 2016.

13. А. В. Дудатьев, В. А. Лужецкий, и Д. А. Коротаев, "Метод оценки информационной устойчивости социотехнических систем в условиях информационной войны", *Восточно-Европейский журнал передовых технологий*, т. 2, № 2 (80), с. 4-11, 2016. doi: 10.15587/1729-4061.2016.65691

14. С. И. Кравченко, "Безопасность социотехнических систем", *НБИ технологии*, т. 12, № 2, с. 20-24, 2018. doi: 10.15688/NBIT.jvolsu.2018.2.3.

15. Д. А. Горницкая, А. Г. Корченко, та В. П. Харченко, "Система социотехнических атак в информационной среде", на *Второй международной научно-практической конференции Проблемы экономики и управления на железнодорожном транспорте*, Киев, 2007, с. 137-138.

16. ДП "УкрНДНЦ". (2016, Груд. 27). *ДСТУ ISO/IEC 27032. Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки (ISO/IEC 27032:2012, IDT)*. Київ, 2018, 50 с.

17. V. V. Mokhor, O. V. Tsurkan, R. P. Herasymov, and V. V. Tsurkan, "Information Security Assessment of Computer Systems by Socio-engineering

Approach", *Selected Papers of the XVII International Scientific and Practical Conference Information Technologies and Security*, Kyiv, 2017, pp. 92-98. [Online]. Available: http://ceur-ws.org/Vol-2067/paper13.pdf. Accessed on: February 12, 2020.

18. О. Цуркан, Р. Герасимов, та О. Крук, "Методи протидії використанню соціальної інженерії", *Information Technology and Security*, vol. 7, iss. 2 (13), pp. 161-170, July-December 2019. doi:

10.20535/2411-1031.2019.7.2.190563.

19. В. В. Мохор, О. В. Цуркан, та Р. П. Герасимов, "Маніпулятивна форма соціоінженерного впливу на особистість в кіберпросторі", на *Науково-практичній конференції Актуальні проблеми управління інформаційною безпекою держави*, Київ, 2015, с. 303-304.

20. А. Л. Тулупьев, А. Е. Пащенко, и А. А. Азаров, "Информационная модель пользователя, находящегося под угрозой социоинженерной атаки", Тр. СПИИ-РАН, вып. 13, с. 143-155, 2010.

21. В. Л. Бурячок, О. Г. Корченко, та Л. В. Бурячок, "Соціальна інженерія як метод розвідки інформаційно-телекомунікаційних систем", *Захист інформації*, т. 14, № 4 (57), с. 5-12, 2012. doi: 10.18372/2410-7840.14.3471.

22. О. Г. Корченко, Д. А. Горніцька, та А. Ю. Гололобов, "Розширена класифікація методів соціального інжинірингу", *Безпека інформації*, т. 20, № 2, с. 197-205, 2014. doi: 10.18372/22255036.20.7308.

23. F. Mouton, L. Leenen, and H. Venter, "Social engineering attack examples, templates and scenarios", *Computers & Security*, vol. 59, pp. 1-54, June 2016. doi: 10.1016/j.cose. 2016.03.004.

24. F.-F. M. Amir, H.-K. Mostafa, and T.-M. Reza, "The Social Engineering Optimizer (SEO)", *Engineering Applications of Artificial Intelligence*, vol. 72, pp. 267-293, 2018, doi: 10.1016/j.engappai.2018.04.009.

25. S. Wasserman, and K. Faust, *Social Network Analysis: Methods and Applications*. Cambridge, England: Cambridge University Press, 2012. doi: 10.1017/CBO9780511815478.

26. O. V. Tsurkan, R. P. Herasymov, and O. M. Kruk, “Presentation the interaction of the subject and the object of socio-engineering influence with a social graph”, in *Proc. Fourth International Scientific and Technical Conference Computer and Informational Systems and Technologies*, Kharkiv, 2020, pp. 46. doi: 10.30837/IVcsitic2020201371.

27. О. В. Цуркан, та Т. М. Клименко, “Аналіз вразливостей соціотехнічних систем на основі нечітких соціальних графів”, на *Науково-практичній конференції Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України Безпека енергетики в епоху цифрової трансформації*, Київ, 2019, с. 28.