

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ

БЕЛКОВА ТЕТЯНА ВЯЧЕСЛАВІВНА

УДК 621.327: 681.5

**МЕТОДИ ВИЯВЛЕННЯ ДЕСТРУКТИВНОГО ІНФОРМАЦІЙНО-
ПСИХОЛОГІЧНОГО ВПЛИВУ ДЛЯ ІНФОРМАЦІЙНИХ
ТЕХНОЛОГІЙ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ПІДЛІТКІВ**

05.13.06 – інформаційні технології

Автореферат
дисертації на здобуття наукового ступеня
кандидата технічних наук

Черкаси – 2019

Дисертацією є рукопис.

Робота виконана в Черкаському державному технологічному університеті Міністерства освіти і науки України.

Науковий керівник: доктор технічних наук, професор
Бараннік Володимир Вікторович,
Харківський національний університет Повітряних
Сил імені Івана Кожедуба, Міністерство оборони
України,
начальник кафедри «Бойового застосування та
експлуатації АСУ».

Офіційні опоненти: доктор технічних наук, професор
Оксіюк Олександр Глібович
Київський національний університет імені Тараса
Шевченка Міністерства освіти і науки України,
завідувач кафедри кібербезпеки та захисту
інформації;

доктор технічних наук, професор
Шостак Ігор Володимирович
Національний аерокосмічний університет імені
М.Є. Жуковського “Харківський авіаційний інсти-
тут” Міністерства освіти і науки України, профе-
сор кафедри інженерії програмного забезпечення;

Захист відбудеться « 23 » жовтня 2019 р. о 10⁰⁰ на засіданні спеціалізованої
вченої ради К 73.052.04 у Черкаському державному технологічному
університеті за адресою: 18006, м. Черкаси, бул. Шевченка, 460.

З дисертацією можна ознайомитись у бібліотеці Черкаського державного
технологічного університету за адресою: 18006, м. Черкаси,
бул. Шевченка, 460, корп.2.

Автореферат розісланий «___» _____ 2019 р.

Учений секретар
спеціалізованої вченої ради

Е.В. Фауре

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. В умовах проведення гібридної та інформаційної війн з врахуванням наявності множини внутрішньодержавних дестабілізуючих чинників ключовий ефект в забезпеченні інформаційної переваги досягається у разі проведення інформаційно-психологічних атак. Це обумовлено наявністю дисбалансу між технологіями і засобами інформаційного протидіяння в Україні. При цьому найуразливішими об'єктами деструктивної інформаційно-психологічної дії є підлітки. У разі атак на підлітків і молодь найбільш ефективними каналами комунікаційної дії є Інтернет і телебачення. З врахуванням чого виникає концептуальна суперечність. З одного боку підвищується рівень інформованості підлітків; з іншого боку формується множина загроз втрати інформаційно-психологічної безпеки. Тоді в умовах наявності множини дестабілізуючих внутрішньодержавних чинників, недостатньої контрольованості Інтернет-простору і дисбалансів на рівні: інформаційної культури підлітка; використання джерел комунікаційних каналів - виникають істотні втрати інформаційно-психологічної (ІП) безпеки підлітків. Тому підвищення інформаційної безпеки підлітків відносно деструктивних інформаційно-психологічних дій в інфокомунікаційному просторі є **актуальною науково-прикладною задачею**. Для вирішення сформульованої задачі пропонується удосконалити інформаційну технологію забезпечення протидії загрозам ІП безпеки підлітків. Одним з ключових її технологічних етапів є методи виявлення ІП деструкцій в інформаційних ресурсах (ІР).

Питаннями розробки та розвитку технологій інформаційної боротьби займається багато вчених. Серед них Богданович В.Ю., Бурячок В.Л., Горбулін В. П., Додонов О.Г., Жук С.Я., Ланде Д.В., Певцов Г.В., Почепцов Г.Г., Расторгуев С. П., Руснак І.С., Телелим В.М., Толубко В.Б., Косевцов В.О., Юдін О.К. та інші. Серед закордонних дослідників: Дж. Бойд, Гриняев С.Н., Комов С.А., Манойло А.В. та інші.

Проте сфера розробки технологічних рішень в напрямку виявлення ІП впливів знаходяться в критичному стані. Відповідні технології мають недостатній рівень розвитку, щоб бути адекватними існуючим інформаційно-технологічним можливостям протидіяючої сторони щодо організації і проведення деструктивних ІП впливів. Отже, розробка методу виявлення деструктивних ІП впливів для інформаційної технології забезпечення інформаційної безпеки підлітків в інфокомунікаційних системах, є **актуальною тематикою науково-прикладних досліджень**.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційні дослідження проводилися відповідно до наступних програм і нормативних документів: Закону України "Про Концепцію Національної програми інформатизації" від 04.02.1998 р. № 75/98-ВР; Постанови Верховної Ради України "Концепція національної безпеки України" від 16 січня 1997 № 3/97-ВР; Указа Президента України "Про рішення Ради

національної безпеки і оборони України “Про Стратегічний оборонний бюлетень України” від 20 травня 2016 року № 240/2016, положення “Стратегії розвитку інформаційного суспільства в Україні” (затверджено Кабінетом Міністрів України від 15 травня 2013 р.); планами наукової, науково-технічної діяльності Черкаського державного технологічного університету, Харківського національного університету Повітряних Сил імені Івана Кожедуба, у рамках яких була виконана НДР “Обґрунтування заходів щодо удосконалення навчального процесу та підвищення якості підготовки військових фахівців”, шифр “Фахівець” (№ 0101U001347), в якій автор дисертації був виконавцем.

Мета і задачі дослідження. Мета дисертаційної роботи полягає в розробці методів виявлення деструктивної інформаційно-психологічної дії в інфокомунікаційному просторі для інформаційних технологій забезпечення безпеки підлітків.

Для досягнення сформульованої мети необхідно вирішити такі задачі:

1. Побудувати модель загроз ІІІ безпеки підлітків в інфокомунікаційному просторі та обґрунтувати напрямком виявлення прихованих деструктивних інформаційно-психологічних впливів в інформаційних ресурсах для підвищення ефективності інформаційних технологій забезпечення ІІІ безпеки.

2. Розробити методи виявлення сугестивних деструктивних інформаційно-психологічних атак на підсвідомість підлітків на основі семантичного диференціалу в інфокомунікаційному просторі.

3. Створити методи динамічного аналізу текстових інформаційних ресурсів в багатовимірному фонетичному просторі за лінгвістичними ознаками для виявлення сугестивних інформаційних деструкцій з маскуванням.

4. Розробити програмний продукт для методів виявлення сугестивних деструктивних інформаційно-психологічних впливів в текстових ресурсах (ТІР) та оцінити їх ефективність.

Об’єкт дослідження. Процеси підвищення ефективності інформаційних технологій забезпечення інформаційної безпеки підлітків відносно деструктивних інформаційно-психологічних атак.

Предмет дослідження. Методи виявлення деструктивних інформаційно-психологічних атак для забезпечення інформаційної безпеки підлітків в інфокомунікаційному просторі.

Методи дослідження. Обґрунтування напрямку підвищення ефективності функціонування інформаційних технологій забезпечення безпеки підлітків ґрунтується на положеннях теорії інформаційного протистояння та складних систем. Визначення актуальності та значимості загроз ІІІ безпеки особистості базується на системному підході з використанням положень теорії інформаційної безпеки. Розробка методів виявлення сугестивних інформаційних деструкцій в ТІР проводилось з застосуванням положень теорії інформації, кодування та інтелектуального

аналізу даних. Оцінка адекватності теоретичних і практичних результатів проводилась на основі методів планування експериментів та математичної статистики.

Наукова новизна одержаних результатів дослідження полягає в наступному.

1. Вперше розроблена модель інформаційно-психологічної безпеки особистості на основі мережецентричного підходу. Відмінностями є те, що враховується: сугестивні деструктивні ІІ впливи на підсвідомість; наявність дисбалансу з категоріями інформаційної безпеки в інформаційно-технічному просторі. Це дозволяє оцінити значимість і актуальність загроз ІІ безпеки особистості в умовах інформаційного протистояння і демократизації соціуму.

2. Вдосконалена модель побудови одновимірного семантичного диференціалу для оцінки рівня і напрямку ІІ впливу структурних компонент ТІР на основі формування фонетичних оцінок звуко-букв. Відмінність полягає у використанні для побудови фонетичного простору тільки значущих біполярних лінгвістичних (ЛБ) ознак. Це дозволяє в автоматизованому режимі провести оцінку значущості і наявності прихованих інформаційних деструкцій для структурних компонент ТІР з врахуванням їх залежності від ЛБ ознак.

3. Вперше розроблено метод ідентифікації ІІ впливів структурних компонент ТІР на підсвідомість особи на основі формування векторного семантичного диференціалу. Основними відмінними особливостями методу є: визначення рівня та напрямку ІІ впливу структурної компоненти ТІР на підсвідомість особи за всіма звуко-буквами в значущому ЛБ просторі, який представляється дійсним нерівноважним базисом; визначення векторного семантичного диференціалу на основі ідентифікації інтегрованих фонетичних оцінок за всіма градаційними шкалами значущих ЛБ ознак з врахуванням детектування двонаправленості ІІ впливів в двовимірному дійсному нерівноважному просторі. Це створює умови для підвищення ефективності і автоматичного виявлення сугестивного деструктивного ІІ впливу в структурних компонентах ТІР на підсвідомість особистості в інфокомунікаційному просторі.

4. Удосконалено інформаційну технологію забезпечення ІІ безпеки підлітків на основі виявлення сугестивних інформаційних деструкцій в ТІР. Базові відмінності від існуючих технологій полягають в тому, що: побудований комплексний метод виявлення прихованого ІІ впливу в ТІР на підсвідомість особи в багатовимірному фонетичному просторі з прив'язкою до векторних градаційних шкал значущих лінгвістичних ознак на основі формування семантичного диференціалу слів і обробкою їх за динамічною технологією з накопиченням фрагментарної інформації. Це дозволяє підвищити ефективність функціонування інформаційних технологій забезпечення ІІ безпеки підлітків в інфокомунікаційному просторі.

Новизна отриманих результатів підтверджується відсутністю розроблених моделей і методів в існуючих інформаційних технологіях забезпечення ІІ безпеки підлітків.

Практичне значення одержаних результатів отриманих результатів полягає в тому, що інтеграція програмних реалізацій розроблених методів виявлення сугестивних інформаційних деструкцій текстових ресурсів в інформаційну технологію забезпечення ІІ безпеки підлітків забезпечує:

- автоматичне виявлення деструктивних та конструктивних сугестивних ІІ впливів на підсвідомість особистості в ТІР;

- визначення спрямованості ТІР здійснюється в статичному та динамічному режимах, що дозволяє виявити сугестивний ІІ вплив у разі додаткового його маскування з боку протиборчої сторони в послідовності фрагментів ТІР та врахувати особливості сприйняття інформації підлітками;

- виявлення та оцінку спрямованості сугестивних ІІ впливів на підсвідомість особистості в ТІР в реальному часі. Процес виявлення швидше майже в 90 разів в порівнянні з експертами (підготовленими фахівцями);

- приріст ефективності виявлення сугестивних ІІ впливів в ТІР на підсвідомість особистості у середньому до 16 % в порівнянні з експертами та у середньому до 59 % в порівнянні з тими, на кого здійснюється такий вплив;

- ефективність виявлення сугестивних ІІ впливів на підсвідомість людини в ТІР складає від 98 до 100 %, що на 10 - 17 % більше в порівнянні з відомими методами аналізу на основі ключової інформації, які оцінюють наявність сугестивного ІІ впливу на підсвідомість з урахуванням семантичної складової текстів;

- в порівнянні з відомими на даний час програмними засобами (технологія “ВААЛ 2000”) виявлення сугестивних ІІ впливів забезпечує істотне розширення функцій аналізу, обробки, редагування текстових документів, відображення інформації. При цьому сам процес виявлення конструктивного або деструктивного впливів в розробленій технології здійснюється швидше за рахунок методу векторного семантичного диференціалу в значимому ЛБ просторі, представленому дійсним нерівноважним базисом.

Створюється можливість для забезпечення комплексної ІІ безпеки підлітків на рівнях: роботи експертів з оцінки та виявлення шкідливих ІІ дій; моніторингу інфокомунікаційного (ІК) простору для виявлення прихованих інформаційних деструкцій в інформаційних ресурсах (ІР).

Практична значущість отриманих результатів дисертації підтверджується їх застосуванням при виконанні дослідно-конструкторських робіт щодо розробки методики аналізу ризиків порушення інформаційної безпеки та моніторингу Інтернет ресурсів в управлінні зв'язку та телекомунікацій Головного управління національної поліції в Харківській області (акт реалізації від 13.03.2018 р.); в навчальному процесі Харківського національного університету Повітряних Сил імені Івана Кожедуба (акт реалізації від 13.04.2018 р.),

Національного університету цивільного захисту України (акт реалізації від 13.02.2018 р.).

Особистий внесок здобувача. Усі положення, які виносяться на захист, отримано автором особисто. У наукових працях, опублікованих у співавторстві, здобувачеві належить наступне: в працях [1, 7, 10] - викладаються основні етапи створення і будується план проведення експериментів для оцінки ефективності інформаційної технології забезпечення ІІ безпеки підлітків в інфокомунікаційному просторі; в працях [2, 16, 22] - розробляється метод векторного семантичного диференціалу в багатовимірному фонетичному просторі по значущих лінгвістичних ознаках; в праці [3] - будується комплексний метод виявлення інформаційних деструкцій в ТІР на основі динамічного аналізу в багатовимірному фонетичному просторі значущих лінгвістичних ознак з накопиченням фрагментарної інформації; в працях [4, 15, 21] - створюється метод і здійснюється оцінка ефективності динамічного аналізу ІІР на основі семантичного диференціалу з накопиченням фрагментарної інформації; в працях [8, 13] - висловлюється підхід для оцінки значущості лінгвістичних ознак в нерівноважному позиційному просторі; в працях [9, 12, 24] - формується технологія ідентифікації рівня і напрямку сугестивного ІІ впливу на підсвідомість підлітка на основі використання двовимірного дійсного нерівноважного позиційного простору; в працях [11, 18] - пропонується модель оцінки ІІ загроз безпеці особистості; в працях [14, 17, 20] - проводиться оцінка впливу процесу детектування інформаційних деструкцій на характеристики сервісів реального часу в інфокомунікаційних системах; в праці [23] - висловлюється методика проведення тестування груп підлітків для встановлення рівня і направленості сугестивних ІІ впливів в ТІР.

Апробація результатів дисертації. Основні результати дисертації доповідались і були схвалені на: XXII Міжнародній науково-практичній конференції, "Інформаційні технології: наука, техніка, технологія, освіта, здоров'я (МикроКАД)", (Харків, 21-23 травня 2014 р.); International Symposium "IEEE East-West Design & Test", (Kiev, Ukraine, September 26–29, 2014); 15 Міжнародній науково-практичній конференції, "Проблеми інформатики та моделювання: матеріали", (Харків - Одеса, 14 - 18 вересня 2015 р.); V Міжнародній науково-практичній конференції, "Захист інформації і безпека інформаційних систем", (Львів, 2 - 03 червня 2016 р.); International Symposium "IEEE East-West Design & Test", (Batumi, 2016); V, VII Міжнародних науково-практичних конференціях, "Фізико-технологічні проблеми передавання, оброблення та зберігання інформації в інфокомунікаційних системах", (Чернівці, 3-5 листопада 2016 р.); Engineer of XXI Century - We Design the Future, Bielsko-Biala, Poland: ATH, 2016; 14th International Conference, "The Experience of Designing and Application of CAD Systems in Microelectronics CADSM'2017", (21-25 February 2017 Polyana-Svalyava (Zakarpattia), Ukraine); III Міжнародній науково-практичній

конференції, "Актуальні питання забезпечення кібернетичної безпеки та захисту інформації", (Закарпатська область Міжгірський район село Верхнє Студене, 22-25 лютого 2017 р.); VI Міжнародній науково-практичній конференції, "Обробка сигналів і негаусівських процесів», присвяченій пам'яті професора Кунченка Ю.П.", (Черкаси, 24 - 26 травня 2017 р.); XIII Міжнародній науково-технічній конференції, "AVIA-2017", (Київ, 19-21 квітня, 2017 р.); I науково-технічній конференції "Проблеми кібербезпеки інформаційно-комунікаційних систем (PCSITS)", (Київ 5–6 квітня 2018 р.); IV Науково-практичній конференції "Перспективні напрямки захисту інформації", (Одеса, 2 - 6 вересня 2018 р.); 3rd IEEE International Conference, "on Advanced Information and Communication Technologies (AICT 2019)", (Lviv, July, 2019).

Публікації. Основні положення і результати дисертаційної роботи опубліковано в 24 наукових працях, серед яких одна колективна монографія, 8 статей, зокрема, дві одноосібні статті та сім статей опубліковано в журналах, які входять до міжнародних наукометричних баз. Апробація результатів дисертації відображена у 15 тезах доповідей на міжнародних науково-технічних та науково-практичних конференціях, зокрема 4 публікації у матеріалах конференцій, що входять до міжнародної наукометричної бази Scopus.

Структура і обсяг дисертації. Дисертація складається із вступу, чотирьох розділів, списку використаної літератури і чотирьох додатків. Загальний обсяг дисертації становить 223 сторінки, з них: 43 ілюстрації, з яких 21 на цілих сторінках, 14 таблиць, з яких 7 на цілих сторінках, список використаної літератури зі 129 джерел на 13 сторінках та чотири додатки на 29 сторінках. Дисертація написана українською мовою.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі доводиться актуальність тематики дисертаційних досліджень, обґрунтовується мета досліджень, наводиться об'єкт та предмет досліджень, формулюється наукова новизна, практична значимість та достовірність отриманих наукових результатів. Приводяться відомості про особистий внесок автора дисертації у наукових статтях, які виконано у співавторстві.

У першому розділі обґрунтовується актуальність і значимість загроз втрати інформаційної безпеки підлітків обумовлених дією прихованих деструктивних ІІІ атак. Обґрунтовується значимість інфокомунікаційних (ІК) каналів як інформаційного середовища проведення деструктивних ІІІ впливів на підлітків.

Найбільш вразливими об'єктами деструктивної ІІІ дії є підлітки. Це обумовлено тим, що: характерний високий рівень потреби нових знань і мінімальний час засвоєння нової інформації; з іншого боку характерний найменший ступінь: критичності сприйняття інформації; стійкості морально-психологічних установок. В той же час для підлітків найбільш ефективними

каналами комунікаційної дії є *Интернет і телебачення*. Відповідна затребуваність в цих джерел інформації для підлітків і молоді досягає 70%, а рівень довіри до них - 60%. Тоді в умовах наявності множини дестабілізуючих внутрішньодержавних чинників, недостатній контрольованості Інтернет-простору і дисбалансів на рівні: інформаційної культури підлітка; використання джерел комунікаційних каналів - виникають істотні втрати інформаційно-психологічної безпеки підлітків. Отже, потрібно мінімізувати ймовірність $P_{\text{дмо}}$ модифікації психологічного стану підлітків, обумовленого діями множини шкідливих ІІ впливів $\Psi_{\text{атк/іп}}$ з використанням множини $\Psi_{\text{ік/к}}$ ІК каналів в умовах наявності множини $\Psi_{\text{зіб}}$ загроз ІІ безпеки, множини дестабілізуючих чинників $\Psi_{\text{дф}}$ та множини $\Psi_{\text{вібо}}$ вразливостей інформаційної безпеки особистості. Для цього *пропонується* удосконалити інформаційну технологію забезпечення протидії загрозам ІІ безпеки підлітків. Одним з ключових її етапів є методи виявлення ІІ деструкцій в ІР. Тому потрібно створити такий метод виявлення деструктивних інформаційних трансформацій, що описується функціоналом $F_{\text{вдіпа}}$, щоб забезпечити максимальну ймовірність виявлення шкідливих ІІ атак (збільшити ймовірність $P_{\text{віпв}}$ виявлення ІІ впливів в ІР): $F_{\text{вдіпа}} : P_{\text{віпв}} = n_{\text{ірв}} / n_{\text{дір}} \rightarrow \max$ та $P_{\text{дмо}} \rightarrow \min$.

Другий розділ дисертаційної роботи присвячено розробці моделі загроз ІІ безпеки особи в умовах інформаційного протиборства і демократизації соціуму. Обґрунтовується, що найбільш актуальними і значущими загрозами ІІ безпеки особи є сугестивні деструктивні ІІ впливи в аудіоконтейнерах та електронних текстових ресурсах. Стверджується необхідність розробки комплексних методів виявлення таких інформаційних деструкцій.

Пропонується наступна класифікація загроз інформаційній безпеці підлітків, а саме:

1. Множина загроз в ІІ просторі. Залежно від глибини використання інформаційних деструкцій розрізняють такі види: до першого виду відносяться загрози, які обумовлені відкритими ІІ атаками на свідомість підлітків, які застосовують інформаційні деструкції на рівні морфологічного опису ТІР; ІІ загрози, які додатково використовують інформаційні деструкції на семантичному опису ІР, створюють другий вид; третій вид ІІ загроз це загрози які пов'язані з сугестивними деструктивними ІІ атаками на підсвідомість підлітків, з додатковим використанням інформаційних деструкцій ТІР на рівні врахування психологічно-емоційної складової особистості.

2. Множина загроз в інформаційно-технічному просторі. Даний вид загроз пов'язано з втратою інформаційної безпеки за такими категоріями як доступність, цілісність та конфіденційність.

Розгляд таких загроз в єдиному *мережецентричному* просторі щодо інформаційної безпеки підлітків пов'язано з наявністю взаємозв'язків між за-

грозами в ІІ та ІІ просторах. Наявність взаємозв'язків обумовлена наступними причинами: деструктивні модифікації можуть організовуватися на базі інформаційних потоків, відповідних сервісам реального часу; дії, пов'язані з блокуванням деструктивних ІІ атак супроводжуються необхідністю додаткових обчислювальних та інформаційних витрат, тобто формуються додаткові затримки на обробку інформаційних ресурсів;

Тому в процесі створення інформаційних технологій протидії деструктивним ІІ впливам потрібно враховувати наявність *суперечності* на рівні категорій інформаційної безпеки. З урахуванням чого побудову узагальненої моделі загроз ІІ безпеки підлітків *пропонується* здійснювати при виконанні наступних вимог відносно забезпечення потрібного рівня: сумарних часових $t_{обр\Sigma}$ витрат на виявлення та локалізацію загроз ІІ безпеки підлітків, $t_{обр\Sigma} \leq t_{пот\Sigma}$, $t_{пот\Sigma}$ - потрібний рівень; часу $t_{ді}$ доступу користувачів до інформаційних ресурсів (ІР), $t_{ді} \leq t_{пот}$, $t_{пот}$ - потрібний рівень часу доступу к ІР; цілісності та повноти ІР, $P_{ц} \geq P_{ц/пот}$. В умовах: заданого рівня $P_{випв/пот}$ вивлення інформаційних деструкцій, за потрібний час $t_{потр}$ з використанням необхідного об'єму $w_{потр}$ ІР; заданого комплексу характеристик ІК систем, включаючи продуктивність $U_{обр}$ обчислювальної апаратури, характеристики пропускної спроможності $U_{пск}$ мережі. Все це можна описати наступною системою виразів:

$$P_{лок/ін} = F_{ол}(P_{випв}; U_{обр}; U_{пск}; v_2; w_{потр}; t_{рбл/дж}; \Psi_{атк/іт}; \Psi_{атк/ін}) \rightarrow \max;$$

$$\Psi_{зіб} : \{ \Psi_{дзіб}; \{ \Psi_{вібо/ву}; \Psi_{вібо/вп}; \Psi_{вібо/рп}; \Psi_{вібо/взв}; \Psi_{вібо/вс} \} \} \rightarrow \Psi_{пск} \rightarrow \min;$$

$$t_{обр\Sigma} \leq t_{пот\Sigma} \ \& \ t_{ді} \leq t_{пот}; \quad t(w_{\min})_{обр} \leq t_{потр} \ \& \ w_{\min} \leq w_{потр}.$$

Тут $F_{ол}(P_{випв}; U_{обр}; U_{пск}; v_2; w_{потр}; t_{рбл/дж}; \Psi_{атк/іт}; \Psi_{атк/ін})$ - функціонал, який описує залежність показника $P_{лок/ін}$ (ймовірність локалізації (усунення) загрози деструктивного ІІ впливу) від технологічних характеристик інформаційної технології забезпечення інформаційної безпеки підлітка (ІТБП); $t(w_{\min})_{обр}$ - часові витрати на обробку ІР для виявлення деструктивних інформаційних модифікацій, залежно від мінімально достатнього об'єму w_{\min} інформації, який необхідно для прийняття відповідного рішення.

Найбільш актуальними і значущими з позиції виявлення і організації протидії та нанесення збитків є сугестивні деструктивні ІІ впливи. Це обумовлено тим, що сугестивні ІІ атаки: на відміну від відкритих атак впливають на підсвідомість особи; за своєю суттю є прихованими і можуть маскуватися під конструктивні ІР; для їх виявлення необхідно набагато більше ви-

трат часового ресурсу. Одними з ключових інформаційних контейнерів, на базі яких здійснюються інформаційні деструкції є: аудіоресурси та електронні текстові ресурси. В той же час дослідження існуючих інформаційних технологій забезпечення інформаційної безпеки підлітків показали наступне.

1. Інформаційні технології, які базуються на методах пошуку, аналізу, складання та формування текстів, не забезпечують виявлення сугестивних деструктивних ІІ атак на підсвідомість особистості.

2. Інформаційні технології, які враховують можливість виявлення сугестивного впливу на підсвідомість, характеризуються тим, що: орієнтовані тільки на російськомовні тексти і є вузьконаправлені; у відкритих джерелах відсутній опис їх математичної бази; 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 ІІ атакам на підсвідомість особистості створює критичний рівень загроз порушення національної безпеки держави.

Отже існує необхідність в розробці комплексних методів виявлення сугестивних деструктивних ІІ впливів на підсвідомість особистості в електронних текстових ресурсах з врахуванням сучасних технологічних аспектів створення інформаційних деструкцій протиборчою стороною.

У третьому розділі дисертаційної роботи основна увага приділяється розробці методів виявлення прихованих інформаційних деструкцій на основі формування семантичного диференціалу з формуванням динамічного накопичування фрагментів ТІР, та вдосконаленню інформаційної технології забезпечення ІІ безпеки особистості.

Для виявлення прихованих ІІ впливів в структурних компонентах ТІР *пропонується* використовувати технологію семантичного диференціалу. В цьому випадку структурна компонента $S(\ell; t)_u$ ТІР представляється в фонетичному просторі $F(\ell; t)_u$ з врахуванням прив'язки до біполярної шкали лінгвістичних (ЛБ) ознак $\theta_i = \{\alpha_i; \bar{\alpha}_i\}$, тобто з обліком позицій відносно негативного $\bar{\alpha}_i$ та позитивного α_i полюсів. Для отримання фонетичних значень $f(\ell; t; u)_{i, \tau}$, ($f(\ell; t; u)_{i, \tau}$ - фонетичне значення τ -ї звуко-букви за i -ю ЛБ ознакою для u -го звуко-слова t -го фрагменту ℓ -го документу) букв $s(\ell; t)_{u, \tau}$ необхідно попередньо сформувані їх опис у вигляді звуко-букв $b(\ell; t)_{u, \tau}$. Це пояснюється тим, що самі букви при написанні не враховують всіх психологічно важливих особливостей звуків. Дане перетворення задається функціоналом φ_{vc} , $B(\ell; t)_u = \varphi_{vc}(S(\ell; t)_u)$, де $B(\ell; t)_u$ - u -е звуко-слово для t -го фрагменту ℓ -го документу (закінченого за змістом повідомлення); $\tau = 1, |B(\ell; t)_u|$. Після чого для всіх звуко-букв слова $B(\ell; t)_u$ експе-

ртним шляхом формуються фонетичні значення $f(\ell; t; u)_{i, \tau}$, а саме $f(\ell; t; u)_{i, \tau} = \varphi_{sd}(b(\ell; t)_{u, \tau}; \theta_i)$, $\tau = \overline{1, |B(\ell; t)_u|}$, $i = \overline{1, Q_\theta}$. Це дозволяє ідентифікувати рівень впливу кожної звуко-букви та звуко-слова в просторі звукових відчуттів особистості відповідно до вибраних шкал ЛБ ознак.

Для скорочення часових затримок на аналіз ТІР пропонується провести відбір значущих ознак ЛБ за всьома звуко-буквами в алфавіті з використанням *інформаційного підходу*. Проведення такої оцінки ґрунтується на отриманні величин $\Delta f_{i, \tau}$, $\Delta f_{i, \tau} = |h_0 - f_{i, \tau}|$, h_0 - нульовий рівень градаційної шкали біполярних ознак θ_i . При цьому для обліку інформації за всьома звуко-буквами необхідно розглядати послідовність ΔF_1 , $\Delta F_1 = \{ \Delta f_{i, 1}, \dots, \Delta f_{i, \tau}, \dots, \Delta f_{i, Q_\theta} \}$, яку пропонується інтерпретувати як *число в дійсному нерівноважному ознаковому просторі* Ω з кроком дискретизації, який дорівнює δ_i . Відповідно для відсічі незначущих ознак використовується нерівність $V(F_1) < V(F)_h$, де $V(F)_h$ - порогове значення. Тоді, якщо нерівність виконується то i -а ознака є незначимою. Навпаки, для умови $V(F_1) \geq V(F)_h$ i -а біполярна ознака буде значимою.

Для визначення спрямованості прихованого ІІ впливу слова на підсвідомість особи в значущому фонетичному просторі *пропонується розробити метод векторного семантичного диференціалу*. Тут створюються умови для забезпечення таких категорій інформаційної безпеки особи як доступність і цілісність ІР. Основними базовими технологічними компонентами методу є наступні етапи.

1. Утворюються дві підматриці $\Delta F(\ell; t)_u^{(\phi)}$, величин $\Delta f(\ell; t; u)_{i, \tau}^{(\phi)}$, які характеризуються конструктивним $\phi = "+"$ та деструктивним $\phi = "-"$ напрямком впливу на підсвідомість особистості.

2. Визначаються інтегровані фонетичні оцінки (векторний семантичний диференціал) $V(Q(\ell; t; u)_h^{(\phi)}; |B(\ell; t; u)_h^{(\phi)}|)$, за всіма значимими ЛБ ознаками по всім звуко-буквам в слові, тобто:

$$V(Q(\ell; t; u)_h^{(\phi)}; |B(\ell; t; u)_h^{(\phi)}|) = \left[\sum_{\tau=1}^{|B(\ell; t; u)_h^{(\phi)}|} \log_2 \prod_{i=1}^{Q(\ell; t; u)_h^{(\phi)}} (\Delta f(\ell; t; u; \max)_{i, \tau}^{(\phi)}) \right] + 1.$$

3. Встановлюється значимість напрямку впливу звуко-слова на підсвідомість особистості з обліком всього ознакового простору, а саме:

$$V(Q(\ell; t; u)_h^{(+)}; |B(\ell; t; u)_h^{(+)}|) < V(Q(\ell; t; u)_h^{(-)}; |B(\ell; t; u)_h^{(-)}|)$$

Якщо нерівність виконується, то слово надає деструктивний ІІ вплив на підсвідомість особистості через його звукове сприйняття.

Отже побудовано метод виявлення прихованого ІП впливу в компоненті ТІР на підсвідомість особи в багатовимірному фонетичному просторі з прив'язкою до векторних градаційних шкал значущих ЛБ ознак на основі формування семантичного диференціалу.

Для підвищення ефективності виявлення сугестивних інформаційних деструкцій з врахуванням: можливості їх додаткового маскуванню в конструктивному ТІР; особливостей сприйняття інформації підлітками *пропонується* створювати динамічний аналіз з накопиченням фрагментів. Структурно-функціональна схема такого методу наведено на рис. 1.

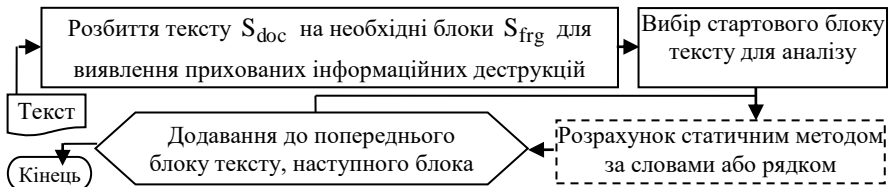


Рисунок 1. Структурно-функціональна схема методу динамічного виявлення прихованих інформаційних деструкцій в АІР та ТІР з накопиченням фрагментів

Створення методу динамічного аналізу ТІР з накопиченням їх фрагментів S_{frg} пропонується здійснювати з використанням технології формування одновимірного семантичного диференціалу. Метод базується на таких базових технологічних етапах.

1) проводиться аналіз накопиченого тексту методом одновимірного семантичного диференціалу за словами. Для цього визначається величина $F'(\ell; t; u)_i$ для кожного слова $S(\ell; t)_u$ з накопиченого ТІР з прив'язкою до окремих ЛБ ознак за всіма звуко-буквами. При цьому з використанням коефіцієнтів $k(\ell; t; u)_{i, \tau}$ посилення звуко-букв враховуються психо-звукові особливості їх сприйняття підсвідомістю підлітка. Для цього використовується співвідношення:

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

2) оцінюються середні значення $F'(\ell; t)_i$ семантичного диференціалу

$$\text{для всіх слів, } F'(\ell; t)_i = \left(\sum_{u=1}^U F'(\ell; t; u)_i \right) / U ;$$

3) виконується перевірка входження величини $F'(\ell; t)_i$ в інтервал $[h_0; h_-]$ негативної спрямованості шкали ЛБ ознаки. Якщо виконується нерівність $h_0 \leq F'(\ell; t)_i \leq h_-$, то слово $S(\ell; t)_u$ має деструктивну фонетичну направленість. Та, навпаки.

Для зниження ймовірності помилок першого і другого роду в процесі оцінки деструктивності ПП впливу текстових ресурсів особистість *пропонується* в комплексі додатково використовувати метод фонетичного аналізу семантичної складової слова, який враховує однополярність фонетичного впливу букв на підсвідомість підлітків. Тут здійснюється аналіз накопиченого тексту методом фонетичного аналізу семантичної складової за словами з прив'язкою до однополярної градаційної шкали лінгвістичної ознаки. Для цього визначається фонетичне значення $F''(\ell; t; u)_i$ для кожного слова $S(\ell; t)_u$ з накопиченого тексту. Це включає наступні розрахунки:

1. Розрахунок відхилення $\Delta f'(\ell; t; u)_{i, \tau}$ частотності звуко-букв від норми.
2. Розрахунок внеску кожної звуко-букви в загальний звуковий тон $F''(\ell; t; u)_i$ слова.

Після аналізу всіх слів $S(\ell; t)_u$ накопиченого тексту, проводиться визначення середнього значення $F''(\ell; t)_i$ для всіх слів.

На заключному етапі організується оцінка характерності накопиченого фрагменту з позиції градаційної однополярної шкали лінгвістичних ознак. Таку оцінку пропонується визначати шляхом порівняння величини $F''(\ell; t)_i$ з пороговим рівнем $F(\ell; t; u)_i^{(\text{пор})}$. Відповідно порогове значення пропонується знаходити з використанням формули: $F(\ell; t; u)_i^{(\text{пор})} = 0,9 \max_{1 \leq i \leq 20} \{F''(\ell; t; u)_i\}$.

Отже створено комплексний метод виявлення прихованого ПП впливу в ТІР на підсвідомість особистості в багатовимірному фонетичному просторі з прив'язкою до векторних градаційних шкал лінгвістичних ознак на основі формування семантичного диференціалу слів і обробкою їх за динамічною технологією з накопиченням фрагментарної інформації.

У четвертому розділі дисертаційної роботи наводиться оцінка ефективності виявлення сугестивних деструктивних ПП впливів на підсвідомість особистості для розробленого методу та існуючих. Доводиться адекватність створених моделей оцінки рівня прихованих інформаційних деструкцій.

Для оцінки ефективності $E_{\text{іпв}}$ виявлення сугестивних ПП впливів в ТІР на підсвідомість підлітків за рахунок реалізації розроблених методів використовується зважений показник приросту, який має вид: $E_{\text{іпв}} = (E_M - E)/(1 - E)$, де E_M – ефективність виявлення сугестивних ПП впливів в ТІР за допомогою розроблених методів; E – ефективність виявлення сугестивних ПП в ТІР експертною або тестовою групами. Відповідна оцінка наведена на рис. 2. З аналізу даних можна зробити висновок, що приріст ефективності щодо виявлення сугестивного ПП впливу на підсвідомість особистості в ТІР досягається за рахунок використання запропонованих в дисер-

тації методів та складає у середньому до 16 % в порівнянні з експертною групою та у середньому до 59 % в порівнянні з тестовою групою.

З метою практичного дослідження ймовірності виявлення сугестивних ІП впливів на підсвідомість особистості був проведений експеримент з аналізу ТІР в мережі Інтернет різної спрямованості. Текстові інформаційні ресурси перевірялися на наявність конструктивного або деструктивного сугестивного ІП впливу на підсвідомість підлітків: програмним забезпеченням, розробленим на основі методу визначення векторного семантичного диференціалу; програмним забезпеченням щодо виявлення ІП впливу на основі ключових слів. Результати проведення експерименту наведені на рис. 3.

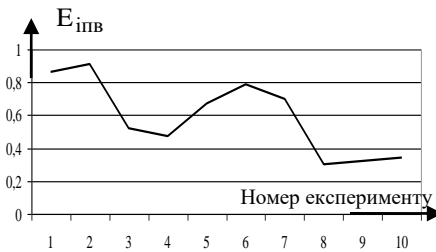


Рис. 2. Значення показника $E_{ІПВ}$ для розробленого методу в порівнянні з тестовою групою

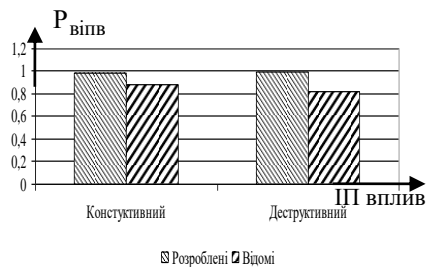


Рис. 3. Залежність величини $P_{ВІПВ}$ для різних методів

З аналізу даних, представлених на рис. 3, можна зробити наступні висновки: ймовірність виявлення сугестивних ІП впливів в ТІР на підсвідомість підлітків на основі розроблених підходів збігається з оцінками, отриманими групою експертів, відхилення складає не більше 2 %. Ефективність виявлення сугестивних ІП впливів на підсвідомість особистості в ТІР складає від 98 до 100 %; в порівнянні з відомими методами оцінки на основі ключових слів, розроблені методи виявили від 10 до 17 % більше ТІР, що носять сугестивний деструктивний ІП вплив на підсвідомість особистості.

ВИСНОВКИ

У дисертаційній роботі вирішено науково-прикладну задачу, яка полягає в підвищенні інформаційної безпеки підлітків відносно деструктивних інформаційно-психологічних дій в інфокомунікаційному просторі. Удосконалено інформаційну технологію забезпечення ІП безпеки підлітків на основі комплексного методу виявлення прихованого ІП впливу в ТІР на підсвідомість особистості в багатовимірному фонетичному просторі з формуванням семантичного диференціалу слів і обробкою їх за динамічною технологією з накопиченням фрагментарної інформації.

Основними науковими результатами, отриманими в роботі, є наступні.

1. Розроблено модель загроз ІІ безпеки особистості з врахуванням інформаційного протиборства і демократизації соціуму в умовах забезпечення мережецентричності безпеки підлітка в інформаційному просторі. Це дозволило обґрунтувати актуальні та значимі загрози ІІ безпеки особистості та визначити вимоги до створення методів їх локалізації.

2. Побудовано інформаційна модель аналізу ТІР на основі формування семантичного диференціалу, та розроблено метод виділення значущих лінгвістичних біполярних ознак на основі представлення фонетичних оцінок звуко-букв в дійсному нерівноважному позиційному просторі. Це дозволяє скороти часові затримки на формування багатовимірного фонетичного простору.

3. Розроблено метод ідентифікації прихованого інформаційно-психологічного впливу структурних компонент текстових інформаційних ресурсів на підсвідомість особи на основі формування векторного семантичного диференціалу з ідентифікацією інтегрованих фонетичних оцінок по всіх значущих ЛБ ознак з врахуванням детектування ІІ впливів в двовимірному нерівноважному просторі. В цьому випадку досягається виявлення інформаційних деструкцій одночасно за всіма ЛБ ознаками по всій структурній компоненті ТІР, та значне скорочення часу на аналіз інформаційних ресурсів.

4. Створено комплексний метод виявлення прихованого ІІ впливу в ТІР на підсвідомість особи в багатовимірному фонетичному просторі з прив'язкою до векторних градаційних значущих лінгвістичних ознак на основі формування семантичного диференціалу слів і обробкою їх за динамічною технологією з накопиченням фрагментарної інформації. Це дозволяє виявити сугестивні інформаційні деструкції у разі їх додаткового маскування в ТІР.

Основними практичними результатами роботи є наступні.

1. Комплексне дослідження зі застосуванням розроблених методів на основі 10 експериментів з виявлення сугестивного ІІ впливу на підсвідомість особистості в 100 різних коротких ТІР в кожному експерименті, показало, що приріст ефективності виявлення сугестивних ІІ впливів на підсвідомість особистості в ТІР складає у середньому до 16 % в порівнянні з експертною групою та у середньому до 59 % в порівнянні з тестовою групою.

2. За рахунок автоматизації, розроблених в дисертаційній роботі технології та методів, значно зменшується час для виявлення сугестивного ІІ впливу на підсвідомість особистості, а саме майже в 90 разів в порівнянні з роботою експертів.

3. Практичні дослідження відносно ймовірності виявлення сугестивних інформаційно-психологічних впливів на підсвідомість особистості в ТІР по Інтернет ресурсах показали, що: ефективність виявлення сугестивних ІІ впливів на підсвідомість людини в ТІР складає від 98 до 100%; розроблені в

дисертаційної роботі технологія та методи забезпечують виявлення від 10 до 17 % більше ТІР з ІІ впливом на підсвідомість особистості в порівнянні з відомими методами аналізу на основі ключових слів.

Достовірність отриманих результатів підтверджується: адекватністю результатів отриманих на основі експертних оцінок та результатів застосування програмної реалізації методів виявлення сугестивних інформаційних деструкцій в ТІР довільного та заданого (еталонного) змісту; не суперечністю отриманих результатів положенням теорії інформації, методам забезпечення інформаційної безпеки.

СПИСОК ПРАЦЬ, ОПУБЛІКОВАНИХ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Беликова Т.В., Баранник В.В. Методы выявления суггестивных воздействий на подсознание человека в текстовых сообщениях в условиях информационно-психологического противоборства. Научные технологии в инфокоммуникациях: обработка информации, кибербезопасность, информационная борьба: коллективная монография / под редакцией В.М.Безрука. – Х.: ТОВ Вид. «Лідер», 2017. – С. 435 – 455.

2. Сапрыкина Т.В., Сидченко С.А., Школяренко В.А. Информационная технология тестирования семантической составляющей для выявления суггестивного воздействия методом фонетического анализа накопительным итогом. *Автоматизированные системы управления и приборы автоматики*. 2013. № 165. С. 111 – 117.

3. Saprykina T.V., Sidchenko S.A. Method of complex information and psychological document analysis. *Science-Based Technologies*. 2014. № 1(21). P. 79 – 83.

4. Сапрыкина Т.В., Сидченко С.А., Школяренко В.А. Метод составления текста с заданной суггестивной направленностью контекста. *Системы обработки информации*. Х.: ХУПС. 2014. № 4(120). С. 96 – 101.

5. Беликова Т.В. Методы выявления деструктивных суггестивных информационно-психологических операций в информационно-социальном пространстве. *Радиоэлектроника и информатика*. 2017. №2. С. 45 – 50.

6. Belikova T.V. The Technology Of Suggestive Information-Psychological Operations Masking In The Infocommunication Space. *Science-Based Technologies*. 2017. № 3. P. 21 – 26.

7. Алімпієв А.М., Бараннік В.В., Белікова Т.В., Сідченко С.О. Теоретичні основи створення технологій протидії прихованим інформаційним атакам в сучасній гібридній війні. *Системи обробки інформації*. Харків: ХНУПС. 2017. № 4(150). С. 113 – 121.

8. Баранник В.В., Беликова Т.В., Довбенко О.В. Методы выявления прихованих інформаційно-психологічних дій в інформаційному просторі. *Наукові технології*. 2018. №3. С. 24 – 30.

9. Бараннік В.В., Белікова Т.В., Капко М.О., Гуржій І.А. Комплексний метод автоматичного фоносемантичного аналізу текстової інформації на основі оцінки вагомих семантичних одиниць в умовах інформаційного протиборства. *Кібербезпека. освіта, наука, техніка*. 2019. №1(1). С. 13 – 22.

10. Сапрыкіна Т.В., Школяренко В.А. Информационная технология выявления суггестивных воздействий на подсознание человека. *Інформаційні технології: наука, техніка, технологія, освіта, здоров'я* (МикроКАД): матеріали XXII Міжн. наук.-практ. конф., тези доп., (Харків, 21-23 травня 2014 р.). Харків, НТУ «ХПІ», 2014. С. 71.

11. Saprykina T., Komolov Dm., Vlasov A., Sidchenko S. Assessment of Video Information Resource Security of Videoconferencing in Public Administration. *International Symposium «IEEE East-West Design & Test»*, (Kiev, Ukraine, September 26–29, 2014). Kiev: 2014. P. 329 – 331.

12. Бараннік В.В., Сидченко С.А., Сапрыкіна Т.В. Методология построения стойких к несанкционированной дешифровке изображений на базе систем компактного представления. *Проблеми інформатики та моделювання: матеріали 15 Міжн. наук.-практ. конф.* (Харків - Одеса, 14 - 18 вересня 2015 р.). Харків-Одеса, НТУ «ХПІ», 2015. С. 56.

13. Бараннік В.В., Белікова Т.В., Тупиця І.М. Кластеризація даних вхідного сигналу для підвищення захисту інформаційного ресурсу. *Захист інформації і безпека інформаційних систем: матеріали V Міжн. наук.-практ. конф.*, (Львів, 2 - 03 червня 2016 р.). Львів: нац. ун-т “Львівська політехніка”, 2016. С. 23 – 25.

14. Barannik V., Belikova T., Komolov D., Krivonos V., Tarnopolov R. Estimate of the capacity of the closed video channel for the method based on the selection of relevant structural units. *International Symposium «IEEE East-West Design & Test»*, (Batumi, 2016). Batumi: 2016. P. 325 – 328.

15. Белікова Т.В., Бараннік В.В. Методика автоматичного підвищення суггестивної спрямованості семантичної складової тексту. *Фізико-технологічні проблеми передавання, оброблення та зберігання інформації в інфокомунікаційних системах: матеріали V Міжн. наук.-практ. конф.*, (Чернівці, 3-5 листопада 2016 р.). Чернівці: Чернівецький нац. ун-т імені Юрія Федьковича, 2016. С. 45 – 48.

16. Belikova T., Barannik V., Karpinskyi V. Development of technology analys for the content semantics, *Engineer of XXI Century - We Design the Future*, Bielsko-Biala, Poland: ATH, 2016. P.65-72.

17. Barannik V., Belikova T., Podlesny S., Suprun O. The Alignment Method of Code Structures for Enhancing the Information's Reliability in the Infocommunication Networks. *The Experience of Designing and Application of CAD Systems in Microelectronics CADSM'2017: The 14th International Conference*, (Polyana-Svalyava (Zakarpattya), Ukraine, 21-25 February 2017). 2017. P. 29-31.

18. Баранник В.В., Беликова Т.В. Метод анализа информационных ресурсов с выявлением семантики контента. *Актуальні питання забезпечення кібернетичної безпеки та захисту інформації*: матеріали III Міжн. наук.-практ. конф., (Закарпатська область Міжгірський район село Верхне Студене, 22-25 лютого 2017 р.). Навчально-науковий інститут права та безпеки підприємництва Європейського університету, 2017. С. 28 – 31.

19. Беликова Т.В. Методы противодействия скрытым информационно-психологическим атакам на социум в инфокоммуникационном пространстве. *Обработка сигналов і негаусівських процесів», присвячений пам'яті професора Кунченка Ю.П.*: матеріали VI Міжн. наук.-практ. конф., (Черкаси, 24 - 26 травня 2017 р.). Черкаси: ЧДТУ, 2017. С. 23-24.

20. Баранник В.В., Беликова Т.В., Подлесный С.А., Хаханова А.В. Способ повышения целостности и доступности видеоконтента в условиях проведения кибернетических атак *AVIA-2017*: матеріали XIII Міжн. наук.-техн. конф., (Київ, 19-21 квітня, 2017 р.). Київ: НАУ, 2017. С. 40 – 43.

21. Баранник В. В., Белікова Т. В., Довбенко О. В., Сідченко С. О. Виявлення прихованих інформаційних впливів в інформаційно-комунікаційному просторі. *Проблеми кібербезпеки інформаційно-комунікаційних систем (PCSITS)*: матеріали I наук.-практ. конф., (Київ 5–6 квітня. 2018 р.). Київ: нац. ун-т імені Тараса Шевченка, 2018. С. 223 - 226.

22. Баранник В.В., Белікова Т.В., Довбенко О.В. Методи виявлення прихованих інформаційно-психологічних дій в інформаційному просторі. *Перспективні напрямки захисту інформації*: матеріали IV Наук. практ. конф., (Одеса, 2 - 6 вересня 2018 р.). Одеса: ОНАЗ, 2018. С. 10 - 11.

23. Баранник В.В., Белікова Т.В., Довбенко О.В., Сідченко С.О., Слободянюк О.В. Методика автоматизованого виявлення прихованих інформаційно-психологічних впливів. *Фізико-технологічні проблеми передавання, оброблення та зберігання інформації в інфокомунікаційних системах*: матеріали VII Міжн. наук.-практ. конф., (Чернівці, 8 - 10 листопада 2018 р.). Чернівці: Чернівецький нац. ун-т імені Юрія Федьковича, 2018. С. 20 – 21.

24. Belikova T., Dovbenko O., Lekakh A., Dodukh O. Method of Increasing the Capacity of Information Threat Detection Filters in Modern Information and Communication Systems. *on Advanced Information and Communication Technologies, AICT 2019*: 3rd IEEE International Conference, Proceedings, (Lviv, July 2019). Lviv, 2019. P. 188 - 192.

АНОТАЦІЯ

Белікова Т.В. Методи виявлення деструктивного інформаційно-психологічного впливу для інформаційних технологій забезпечення безпеки підлітків. – Рукопис.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.06 – інформаційні технології. – Черкаський державний технологічний університет, Черкаси, 2019.

Дисертаційна робота присвячена вирішенню актуальної науково-прикладної задачі, яка полягає в підвищенні інформаційної безпеки підлітків відносно деструктивних інформаційно-психологічних дій в інфокомунікаційному просторі.

Викладаються етапи створення моделі загроз ІІ безпеки особистості в умовах інформаційного протистояння і демократизації соціуму в умовах забезпечення мережецентричності безпеки підлітка в інформаційному просторі. Це дозволило обґрунтувати актуальні та значимі загрози ІІ безпеки особистості та визначити вимоги до створення методів їх локалізації. Будується інформаційна модель аналізу ТІР на основі формування семантичного диференціалу, та розроблено метод виділення значущих лінгвістичних біполярних ознак на основі представлення фонетичних оцінок звуко-букв в дійсному нерівноважному позиційному просторі. Розроблено метод ідентифікації прихованого інформаційно-психологічного впливу структурних компонент текстових інформаційних ресурсів на підсвідомість особистості на основі формування векторного семантичного диференціалу. Здійснюється вдосконалення інформаційної технології забезпечення ІІ безпеки підлітків на основі комплексного методу виявлення прихованих інформаційних деструкцій з використанням динамічної технології накопичення фрагментів ТІР.

Ключові слова: інформаційна безпека, інформаційно-психологічний вплив, сугестивні інформаційні деструкції, інформаційні технології забезпечення безпеки, семантичний диференціал, текстові ресурси.

АННОТАЦІЯ

Беликова Т.В. Методы выявления деструктивного информационно-психологического влияния для информационных технологий обеспечения безопасности подростков. – Рукопись.

Диссертация на соискание ученой степени кандидата технических наук по специальности 05.13.06 – информационные технологии. – Черкасский государственный технологический университет, Черкассы, 2019.

Диссертационная работа посвящена решению актуальной научно-прикладной задачи, которая заключается в повышении информационной безопасности подростков относительно деструктивных информационно-психологических влияний в инфокоммуникационном пространстве.

Обосновывается необходимость исследования угроз безопасности подростков в информационно-психологическом пространстве. Показывается, что развитие инфокоммуникационных технологий и Интернет ресурсов создает условия для проведения деструктивных информационных атак на сознание и

подсознание подростков. Излагаются этапы создания модели угроз информационно-психологической (ИП) безопасности личности с учетом информационного противоборства и демократизации социума в условиях обеспечения сетцентричности безопасности подростка в информационном пространстве. Это позволило обосновать актуальные и значимые угрозы ИП безопасности личности и определить требования к созданию методов их локализации. Обосновывается, что наиболее актуальными и значимыми ИП угрозами потери безопасности личности являются суггестивные информационные деструкции. Утверждается необходимость усовершенствования информационной технологии обеспечения ИП безопасности подростков в инфокоммуникационном пространстве. Строится информационная модель анализа текстовых информационных ресурсов (ТИР) на основе формирования семантического дифференциала, и разработки метода выявления значимых лингвистических биполярных признаков на базе представления фонетических оценок звуко-букв в вещественном неравновесном позиционном пространстве. Это позволяет сократить временные задержки на формирование многомерного фонетического пространства. Проводится разработка метода идентификации скрытого информационно-психологического влияния структурных компонент текстовых информационных ресурсов на подсознание личности на основе формирования векторного семантического дифференциала с идентификацией интегрированных фонетических оценок по всем значимым биполярным лингвистическим (ЛБ) признакам с учетом детектирования ИП влияний в двумерном неравновесном пространстве. В этом случае достигается выявление информационных деструкций одновременно по всем ЛБ признаками по всей структурной компоненте ТИР, и значительное сокращение времени на анализ информационных ресурсов. Организуется создание комплексного метода выявления скрытого информационно-психологического влияния в текстовом информационном ресурсе на подсознание личности в многомерном фонетическом пространстве с привязкой к векторным градиционным шкалам значимых лингвистических признаков на основе формирования семантического дифференциала слов и обработкой их по динамической технологии с накоплением фрагментарной информации. Это позволяет обнаружить суггестивные информационные деструкции в случае их дополнительной маскировки в ТИР. Проводятся экспериментальные оценки эффективности созданных методов и доказываются их адекватность.

Ключевые слова: информационная безопасность, информационно-психологическое влияние, суггестивные информационные деструкции, информационные технологии обеспечения безопасности, семантический дифференциал, текстовые ресурсы.

ANNOTATION

Belikova T.V. Methods of detecting destructive information and psychological impact of information technology security of teenagers. – Manuscript.

Ph.D. thesis on specialty 05.13.06 – Information Technology. – Cherkasy State Technological University, Cherkasy, 2019.

The dissertation is devoted to solution of the actual scientific and applied problem, which consists in improving of the information security of teenagers against destructive information and psychological actions in information and communication space.

The stages of creating a model of threats to IP personal security are outlined, taking into account the informational confrontation and democratization of society in the context of ensuring the network-centric security of the teenager in the information space. This allowed us to substantiate the current and significant threats to IP personal security and determine the requirements for creating methods for their localization. Information model of TIR analysis based on formation of semantic differential is constructed, and developed a method of highlighting significant linguistic bipolar features based on the presentation of phonetic assessments of sound letters in the material unbalanced positional space. A method of identification of the hidden information and psychological influence of the structural component of textual information resources on the subconscious of the individual based on the formation of a vector semantic differential has been developed. The information technology for IP personal security is being improved based on a complex method of detecting hidden information destructions using dynamic technology for the accumulation of TIR fragments

Keywords: information security, information and psychological influence, suggestive information destruction, Information security technologies, semantic differential, text resources.