ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ПЕДАГОГІЧНИЙ
УНІВЕРСИТЕТ ІМЕНІ Г.С. СКОВОРОДИ

МАТЕРІАЛИ

XIV МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

СОЦІАЛІЗАЦІЯ ОСОБИСТОСТІ

У СУЧАСНИХ СОЦІОКУЛЬТУРНИХ ТА СОЦІАЛЬНО-ПОЛІТИЧНИХ КОНТЕКСТАХ

2024

на життя чи здоров'я ні в чому не винних людей або погрози вчинення злочинних дій з метою досягнення злочинних цілей» (ЗУ «Про боротьбу з тероризмом», 2003, ст.1). Активні воєнні дії докорінним чином змінюють характер відносин між суб'єктами політики, розділяють країни на протиборчі сторони, продовжуючи ведення політики з використанням будь-яких форм діяльності, у тому числі і терористичної. Вирішення будь-якої конфліктної ситуації суб'єктами політики відбувається за умови ідейної одержимості, абсолютизації та максималізму рішень, що приймаються; реалізуються спроби віднайти методи розв'язання складних соціально-економічних, соціально-політичних, соціально-культурних тощо, проблем простими, універсальними способами з обов'язковою наявністю насильницького компоненту.

Стан сучасного українського суспільства, що перебуває під впливом військового вторгнення з боку Російської Федерації, яке можна визначити як форму прояву терористичної діяльності, обумовлює необхідність підтримувати безпеку суспільства та держави збройними засобами, вдаватися до вирішальних способів ведення війни, з метою забезпечити принцип суверенності та гарантувати суверенітет національної держави.

ЛІТЕРАТУРА

1. Закон України «Про боротьбу з тероризмом» [online]. Доступно: https://zakon.rada.gov.ua/laws/show/638-15#Text [Дата звернення 5 Лютого 2024 рік].
2. Стрельнікова О. Війна як прояв політичного радикалізму. Міжнародна наукова конференція «Наративи про війну» (Познань, 17 жовтня 2023 р.). Познань, 2023. С. 56-58.

К.Ю. Ушкало

(Україна)

ЗАБЕЗПЕЧЕННЯ ГРОМАДСЬКОЇ БЕЗПЕКИ В КОНТЕКСТІ ВРАЗЛИВОСТІ ІНФОРМАЦІЙНОГО ПРОСТОРУ

В сучасному світі вразливість інформаційного простору стала неодмінною частиною загального поняття громадської безпеки. Швидкі технологічні зміни та зростання обсягів інформації в електронному форматі

породжують нові виклики, зокрема, стосовно забезпечення конфіденційності, цілісності та доступності інформації. Інформаційні системи та мережі стають об’єктом не лише технічних атак, а й специфічних загроз для суспільства.

В контексті вразливості інформаційного простору неможливо уникнути розгляду питань кібербезпеки, захисту від кіберзлочинності та управління ризиками в цьому сегменті. Зловживанням та недостатньою захищеністю інформації можна нанести значний шкідливий вплив на економіку, політичну стабільність та соціальну гармонію [2, с. 84].

Одним із ключових завдань у цьому контексті є постійне удосконалення технологічних заходів та систем захисту інформаційних ресурсів. Нині, зловмисники активно використовують нові методи та технології для реалізації кібератак, що вимагає відповідного розвитку та оновлення систем захисту. Системи захисту повинні бути націлені на ефективний захист цих критичних точок.

Крім того, необхідно акцентувати увагу на розробці та впровадженні новітніх засобів захисту. Це може включати в себе розробку нових алгоритмів шифрування, вдосконалення методів аутентифікації та використання передових технологій машинного навчання для виявлення аномалій та ідентифікації атак.

Біометричні технології базуються на унікальних фізичних або поведінкових характеристиках особи і включають в себе такі елементи, як відбитки пальців, розпізнавання обличчя, розпізнавання рукопису, голосу тощо. Однією з основних переваг біометричних технологій є їх висока точність та надійність. В порівнянні з традиційними методами аутентифікації, такими як паролі чи PIN-коди, біометричні технології складніше підробити чи втратити, що забезпечує вищий рівень безпеки. Розвиток біометричних систем також включає в себе використання передових алгоритмів обробки зображень та штучного інтелекту для поліпшення точності виявлення та уникнення помилок.

Слід зазначити, що у сучасному інформаційному суспільстві, де динаміка змін і технологічний розвиток визначають новий соціальний контекст, аспекти вразливості інформаційного поля виявляють суттєвий вплив на соціальну

динаміку та психологічний стан індивідів. Вивчення соціальних та психологічних аспектів інформаційної вразливості є важливою складовою стратегії забезпечення громадської безпеки.

Одним із ключових аспектів є взаємозв'язок між інформаційними загрозами та сприйняттям громадською свідомістю. Індивіди та громадяни стають учасниками високого динамічного обміну інформацією, і їхнє сприйняття загроз безпеки тісно пов'язане з емоційним та когнітивним фоном. Дослідження психологічних реакцій на інформаційні загрози дозволяє розуміти, як вони впливають на рішення, поведінку та соціальну адаптацію.

Крім того, необхідно аналізувати, як інформаційна вразливість впливає на соціальну структуру. Зростання кількості дезінформації та маніпуляційної інформації може призводити до дисбалансу у громадській довірі та формування негативних стереотипів. Дослідження впливу інформаційної вразливості на соціальну стабільність та взаємовідносини в громаді є ключовим для визначення стратегій управління цим впливом. Забезпечення громадської безпеки включає в себе розробку ефективних механізмів виявлення та контролю розповсюдження дезінформації, а також формування освітніх програм для підвищення інформаційної грамотності [4, с. 229].

У Стратегії інформаційної безпеки України йдеться про нарощування інформаційного впливу на населення України та використання механізмів інформаційного впливу на індивідуальну, групову та суспільну свідомість. На першому рівні об'єктами інформаційної безпеки виступають особа, великі та малі соціальні групи. Первинним об'єктом інформаційної безпеки є особа, щодо якої здійснюється деструктивний інформаційний вплив. На другому рівні як об'єкти інформаційної безпеки визначені психіка людини, що включає свідомість і несвідоме, групові психічні структури, що складаються з групової свідомості та колективної несвідомої. На третьому рівні як об'єкти інформаційної безпеки виділено індивідуальні та групові психічні процеси і утворення свідомого та несвідомого характеру [1, с. 57-58].

На думку О.Р. Ткачишиної, вплив небезпечної інформації та психології на свідомість особистості може призвести до двох взаємозалежних змін: зміни психології людини, психічного здоров'я та зміни особистісних цінностей, життєвої позиції, світогляду. Такі зміни спричиняють антисоціальні вчинки і становлять небезпеку вже для всього суспільства і держави [5, с. 180].

Ефективне забезпечення громадської безпеки в умовах вразливості інформаційного простору вимагає не лише технологічних заходів, але і ретельного правового регулювання, що віддзеркалює сучасні виклики та реалії цифрового суспільства. Визначення прав та обов'язків у контексті захисту інформації, а також встановлення ефективних механізмів відповідальності є ключовим елементом для створення стійких правових фундаментів безпеки.

Управління ризиками в інформаційній сфері на сучасному етапі викликає значні труднощі через постійні зміни та ускладнення природи інформаційних загроз. Забезпечення громадської безпеки у цьому контексті передбачає систематичний та стратегічний підхід до ідентифікації, оцінки та управління ризиками.

По-перше, постійні зміни в технологічному середовищі вимагають постійного вдосконалення методів управління ризиками. Розробка та вдосконалення стратегій прогнозування та аналізу нових типів загроз є критичним завданням. Сучасні технології, такі як штучний інтелект та аналітика великих обсягів даних, можуть служити інструментами для розпізнавання важливих змін у сфері кібербезпеки та визначення потенційних ризиків.

По-друге, ускладнення природи інформаційних загроз вимагає розробки та впровадження ефективних систем виявлення та реагування на інциденти. Це включає в себе створення механізмів миттєвого реагування, аналізу інцидентів у реальному часі та розробку планів кризового управління. Важливим є також вдосконалення систем взаємодії між різними суб'єктами (організаціями, урядовими структурами, приватним сектором тощо) для спільного реагування на інформаційні загрози [3, с. 138].

Отже, у сучасному цифровому суспільстві, де інформаційна вразливість стала неодмінною частиною нашого повсякденного життя, ефективне забезпечення громадської безпеки вимагає інтегрованого та комплексного підходу. Ретельний аналіз технічних, соціальних, правових та управлінських аспектів є необхідним для розуміння суті інформаційної вразливості та розробки стратегій, спрямованих на ефективний захист суспільства. Лише комплексний підхід до забезпечення інформаційної безпеки, заснований на глибокому розумінні сучасних викликів та можливостей, забезпечить стійкість та захист суспільства у цифровому столітті.

ЛІТЕРАТУРА

1. Барабаш О.О., Грищук А.Б. (2022). Забезпечення інформаційної безпеки в контексті захисту від деструктивного інформаційного впливу. Правовий часопис Донбасу, 4 (81), 55-60.
2. Ковалів М.В., Єсімов С.С., Ярема О.Г. (2022). Інформаційне право України: навчальний посібник. Львів: Львівський державний університет внутрішніх справ, 416.
3. Кукін І.В. (2020). Комплексний механізм публічного управління інформаційною безпекою особистості у сфері національної безпеки та її прикордонному секторі. Публічне управління та митне адміністрування, 4 (27), 134-139.
4. Панченко О.А., Кабанцева А.В. (2020). Людська психіка в інформаційній небезпеці. Вчені записки ТНУ імені В. І. Вернадського. Сер.: Державне управління, 3, 226-233.
5. Ткачишина О.Р. (2019). Психологічна безпека у контексті маніпулятивного впливу на свідомість особистості. Теорія і практика сучасної психології, 1, 178-182.

І.О. Фомін

(Україна)

СОЦІАЛІЗАЦІЯ ТА ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВ В УКРАЇНІ: ВИКЛИКИ ТА СТРАТЕГІЇ В УМОВАХ ВОЄННОГО СТАНУ

Інформаційна безпека підприємства – це комплекс заходів і стратегій, спрямованих на забезпечення конфіденційності, цілісності та доступності інформації в організації. Ця концепція охоплює весь спектр заходів, що мають на меті захист важливих даних від несанкціонованого доступу, втрати, руйнування чи неправильного використання.

В умовах воєнного стану інформаційна безпека набуває особливого значення, оскільки підприємства можуть стати об’єктами кібератак, шпигунства або інших форм кіберзагроз. Важливо розробляти та