Плетінь О. О.,
студентка навчально-наукового інституту інформаційної безпеки,
Національна академія Служби безпеки України
(м. Київ, Україна)

Науковий керівник:
Тиква В.,
старший викладач кафедри інформаційної безпеки держави, підполковник,
Національна академія Служби безпеки України
(м. Київ, Україна)

НАЦІОНАЛЬНІ МЕХАНІЗМИ ТА СТРАТЕРІЇ ПРОТИДІЇ ІНФОРМАЦІЙНИМ ЗАГРОЗАМ

У межах теорії національної безпеки механізм протидії загрозам розглядають у *вузькому* та *широкому* значенні. **У вузькому розумінні** він є складовою державного апарату і включає систему органів влади, установ та недержавних структур, що виконують спеціальні функції із захисту національної безпеки та взаємодіють між собою (сили забезпечення національної безпеки). **У широкому сенсі** цей механізм охоплює не лише сили, а й засоби протидії загрозам: технології, технічні, програмні, правові, організаційні та комунікаційні інструменти, які використовуються для збору, передачі, обробки та захисту інформації, а також методи та прийоми, використовувані суб'єктами забезпечення національної безпеки для вирішення завдань щодо протидії загрозам національній безпеці.

Механізм забезпечення національної безпеки є динамічною системою, що включає такі стадії: визначення інтересів, прогнозування загроз, вироблення заходів протидії, їх нейтралізацію та відновлення стабільного функціонування об'єктів. Через різноманітність способів і засобів протидії інформаційним загрозам доречно говорити про множинність таких механізмів.

Загрози традиційно поділяють на *внутрішні* та *зовнішні*. Для інформаційної безпеки **внутрішніми** вважають ті, що виникають у самому об'єкті, а **зовнішніми** — ті, що пов'язані з його взаємодією з іншими структурами.

Стратегія національної безпеки України серед ключових загроз в інформаційній сфері виокремлює агресивні дії Росії, інформаційно-психологічну війну, дискредитацію української мови й культури, перекручування історії, нав'язування спотвореної інформаційної картини світу, кібератаки на критичну інфраструктуру, а також низький рівень медіакультури суспільства. Недоліком є

те, що у Стратегії не зовсім логічно відмежовані інформаційно-психологічні загрози, кіберзагрози та власне загрози інформаційній безпеці.

Доктрина інформаційної безпеки та Стратегія кібербезпеки України визначають широкий спектр небезпек у цій сфері. У сучасному інформаційному протиборстві активно застосовуються пропаганда, дезінформація, кібератаки на критичні системи, а також маніпуляція громадською свідомістю. Інформаційна агресія зазвичай проходить три етапи: формування ядра невдоволених, створення альтернативного інформаційного простору та поступове зміщення суспільної думки. Завдання держави полягає у захисті інформаційних ресурсів, свідомості громадян та обмеженні доступу супротивника до критичних даних.

Інтернет є головним полем інформаційних атак, тому заходи держави мають бути спрямовані на підвищення стійкості суспільства до деструктивних впливів. Реалізація зовнішніх загроз відбувається через пошук вразливостей у інформаційній інфраструктурі та використання різних видів «інформаційної зброї» — від шкідливих програм до психологічних технологій впливу.

Складність аналізу зовнішніх загроз посилюється тим, що в доктринальних документах України бракує чіткої класифікації та ранжування небезпек. Тому особливого значення набуває моніторинг, прогнозування та моделювання розвитку подій. Основою прогнозування є визначення мети, ключових факторів, їх взаємозв'язків і варіантів впливу на систему безпеки.

Серед найбільш небезпечних зовнішніх інформаційних загроз для України можна виокремити:

- спроби несанкціонованого доступу до державних інформаційних ресурсів та інфраструктури;
- поширення дезінформації про внутрішню й зовнішню політику;
- маніпулятивний вплив іноземних структур на прийняття рішень;
- порушення прав українських громадян та організацій в інформаційній сфері за кордоном.

Ефективний захист передбачає багаторівневу систему заходів, яка враховує геополітичний контекст, регіональну специфіку та вплив транснаціональної злочинності.

Отже, своєчасний моніторинг характеру, особливостей, масштабів загроз та їх наступне прогнозування мають особливе значення. Прогнозування є важливим і самостійним елементом профілактики інформаційних загроз зовнішніх джерел, та, відповідно, забезпечення національної безпеки.

Список використаних джерел:

1. Дереко В. Н. Теоретико-методологічні засади класифікації загроз об'єктам інформаційної безпеки. Інформаційна безпека людини, суспільства, держави. 2015. № 2 (18). С. 16-22. Дата звернення: 25.09.2025.

2. Хілько О. Л. Визначення загроз національній безпеці в українській теоретико-політичній думці. Дата звернення: 25.09.2025.

3. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України»: Стратегія національної безпеки України, затверджена Указом Президента України від 26 травня 2015 року № 287/2015. Дата звернення: 25.09.2025.