**СЕМІНАР 3**

**ПІДТРИМУЄМО ЕТИЧНІ СИСТЕМИ ЦІННОСТЕЙ** ТА В**ЧИМО ПРОАКТИВНОМУ ЗАХИСТУ**

Прийняття рішень у публічному управлінні та адмініструванні базується на певних системах цінностей, які виконують роль внутрішнього арбітра. Система цінностей містить набір параметрів та критеріїв (правил), за якими відбувається прийняття рішень. Проблема виявляється у тому, що системи цінностей розвиваються разом з особистістю, тобто вони не є константами. Можливість оновлення критеріїв вибору відкриває вразливі моменти для маніпуляцій зловмисників.

Це стає серйозною проблемою й для викладача: з одного боку, – заохочувати гнучкість пріоритетів, що створює умови для розвитку особистості; а з іншого – навчити зберігати стійкість системи цінностей та не піддаватись маніпуляціям.

Вирішення цієї проблеми дозволить сформувати головну компетентність, потрібну в умовах гібридних впливів: вміння зберігати не лише сьогоднішню сталу систему цінностей, але й зберігати здатність для її свідомого неманіпулятивного вдосконалення. Все це обумовлює важливість двох моментів, які мають бути враховані у навчальному процесі:

1. Формулювання та обговорення на заняттях етичних принципів та норм в різних сферах професійної діяльності та громадського життя.

2. Розгляд складних прикладів, в яких немає простих рішень, що дозволить підготувати студентів до стійкості в умовах гібридних загроз.

Часто викладачі дисциплін професійного спрямування на своїх заняттях "не встигають" розглянути приклади з етичними викликами, бо крім обмеженого часу аудиторної роботи, ці приклади занадто складні, можуть завести бесіду в неочікуване русло, мають чутливий контент тощо. Це дійсно складні заняття.

До цього додається ще один виклик – такі заняття вимагають нарощування власної стійкості самого викладача. Це – додаткове ретельне опрацювання великої кількості різних аргументів та можливих напрямків розвитку заняття, розуміння етичних принципів прийняття рішень у складних ситуаціях, психологічна рівновага та делікатність.

Але такі складові на заняттях дуже потрібні. Це не обов'язково мають бути окремі модулі чи спеціальні завдання. Акцент на системі цінностей та етично-складних професійних ситуаціях можна додати до будь-якого заняття. Це необхідний елемент для підготовки студентів до роботи в умовах гібридних загроз.

Гібридні загрози часто називають **"злісними проблемами"** (Wicked problem) через те, що такі проблеми складно або неможливо вирішити внаслідок неповноти, суперечності або мінливості інформації і вхідних умов.

Такі проблеми легко стають мішенню гібридних зловмисників, бо злісні проблеми неможливо вирішити. Прийняття рішень у цій площині не буває легким та вимагає міцної системи цінностей, вміння знайти потрібну інформацію та побачити повну картину, розуміння поняття "справедливість" та моральної готовності обирати краще з поганих рішень.

Рішення злісних проблем завжди міститиме негативні наслідки. Але, на відміну від маніпуляцій, стійкість особи, що приймає рішення, має проявлятись у наступному:

– **пильність**: вміння знаходити та обирати джерела інформації з вимогами до достовірності (підтвердження об'єктивності даних), надійності (підтвердження інформації з кількох джерел), авторитетності (підтвердження експертності джерела) та актуальності (своєчасності);

– **свідомий вибір**: вміння формувати та розмірковувати над аргументами;

– **стійкість**: спроможність приймати ефективні обґрунтовані рішення навіть під впливом негативних чинників.

**Вчимо проактивному захисту**

Гібридні впливи досягають своєї мети на рівні окремої людини (особи, яка приймає рішення) через когнітивний злам (cognitive hack). Когнітивний злам містить три складові, які можна назвати "3D":

– дезорієнтація: люди втрачають впевненість у своїх цінностях;

– деморалізація: люди стають абсолютно байдужими своїх цінностей ("пофігізм");

– дестабілізація: люди несвідомо руйнують своє середовище на користь зловмисника через неправильні рішення.

Для того, щоб наш розум створив імунітет проти когнітивного зламу, який є основою гібридних впливів, потрібна "академічна вакцина". Так само, як імунітет людини, захист від гібридних загроз вимагає не лише вміння протидіяти вже відомим загрозам (так званим "відомим невідомим"), але й виявляти та протидіяти "невідомим невідомим" – тобто таким новим типам випливів, навіть про існування яких ніхто не обізнаний.

Інформація про "Невідомі невідомі" не піддається моніторингу, який побудованій на сприйнятті того, що ми очікуємо сприймати (за допомогою шаблонів розпізнавання або використання набору індикаторів). Це пов’язано з тим, що аналітик ніколи раніше не бачив цієї закономірності і не може мати набір індикаторів для того виду атаки, який раніше ніколи не мав місця або навіть не був уявним. Проблема захисту системи в умовах "невідомих невідомих" атак добре знайома спеціалістам в області кіберзахисту: сукупність технологій, яка використовується в антивірусному програмному забезпеченні для превентивного виявлення потенційно небезпечних вразливостей, створює механізм **проактивного захисту**.

Проактивна безпека запобігає невідомим раніше атакам. Вона допомагає усувати будь-яку вразливість, яка робить нас сприйнятливими до атак, перш ніж злочинці використають їх. Рис. 1 дозволяє виявити ключові підходи, які мають бути втілені у навчанні для забезпечення навичок проактивного захисту:

– моделювання поведінки супротивника: потрібно навчити студентів виходити за межи власної позиції і "залазити у шкуру" ворога;

– симуляція атак, протидії, суперництва, спарингів та інших видів конкурентної інтерактивності.

Це означає, що пасивного слухання матеріалу недостатньо для протидії гібридним загрозам. Це вимагає **активного навчання** (Active learning), тобто залученості студентів до емпіричних завдань. Існує багато форм активного навчання, серед яких корисними для навчання проактивному захисту, є наступні:

**1. Експериментальне навчання** (experiential learning, ExL) – філософія та методологія, згідно з якою викладачі цілеспрямовано взаємодіють зі студентами у практичному досвіді та зосередженій рефлексії, щоб збільшити знання, розвинути навички та роз’яснити цінності (*Northern Illinois University, 2012а*). Існує велика кількість підходів та методів експериментального навчання, серед яких в умовах гібридних загроз особливу увагу привертають:

– **симуляція** (simulation), яка дозволяє розвивати критичне мислення, самостійне навчання та є ефективним засобом боротьби з неправильними уявленнями студентів (*Caniglia, 2019*). Метод передбачає створення ситуацій, які вимагають швидкої реакції та дії, які стимулюють студентів до проактивної поведінки;

– **рольові ігри** (role-playing): техніка, яка дозволяє студентам досліджувати реалістичні ситуації, керовано взаємодіючи з іншими людьми, щоб отримати досвід і випробувати різні стратегії у певному середовищі ([*Glover*](https://blogs.shu.ac.uk/shutel/author/slsig1/)*, 2014*). Цей підхід дозволить студентам побувати зловмисником, але не стати зловмисником. Не можна зрозуміти, як діятиме ворог, якщо не змоделювати його поведінку, не програти можливі сценарії омани, маніпуляції, перекручування, не спробувати атакувати. У такому навчанні важливо зберігати власну систему цінностей. Саме входження у роль та вихід з неї дозволять зрозуміти ворога, але залишитись собою.

**2. Діяльне навчання** (action learning) – навчання через вирішення конкретної проблеми, який включає виконання дій і рефлексію над результатами (*Corporate Finance Institute, 2022*).

**3. Групове або кооперативне навчання** (cooperative learning) – метод навчання, що оснований на співробітництві студентів у групах. При такому підході студенти досягають успіхів у навчанні, лише за умови ефективної взаємодії між собою (*SERC Pedagogic Service, n.d.*)

**4. Навчання служінню** (service-learning) – освітній підхід, який поєднує цілі навчання з громадською роботою (волонтерством), щоб забезпечити прагматичний, прогресивний досвід навчання, одночасно задовольняючи потреби суспільства (*Suffolk University, n.d*.).

**5. Ситуаційне навчання** (situated learning) – студенти навчаються, беручи активну участь у вирішенні проблем, які формуються у реальних життєвих ситуаціях (*Northern Illinois University, 2012b*).