Доценко В.В., кандидат психологічних наук,
доцент, доцент кафедри педагогіки та
психології факультету № 3 ХНУВС
Макаренко П.В., кандидат психологічних наук,
доцент, заступник декана факультету № 4 з
навчально-методичної роботи ХНУВС

ТРЕНІНГОВІ ТЕХНОЛОГІЇ У ПІДГОТОВЦІ ПРАВООХОРОНЦІВ ДО ПРОТИДІЇ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОМУ ВПЛИВУ

В сучасному світі системи розповсюдження, зберігання і оброблення інформації набувають небувалого темпу розвитку. Прискорення процесу обігу інформації, в першу чергу, стосується мережі Інтернет, як найбільш розширеної і швидкісної інформаційної складової розвитку суспільства. І в цьому динамічному процесі людині стає дедалі складніше приймати рішення і орієнтуватися в ситуаціях, які постійно змінюються та мають значний масив як позитивної так і негативної інформації.

Автори (В. Малахов, Т. Чернігівська) наголошують, що сучасне покоління молодих людей, які зростають в епоху цифрових технологій, живуть за нав'язаними рекламою стереотипами, мало читають, недостатньо часу витрачають на отримання і закріплення знань з певних дисциплін чи галузей наук. Сучасна молодь має доступ до будь-якої інформації (до сайтів будь-яких бібліотек), але витрачають свій час на спілкування в соціальних мережах і прокручування сторінок Instagram. Вони більше налаштовані на те, що підкаже Інтернет, і тому самі втрачають здатність до запам'ятовування і самостійного відповідального мислення [1].

Як навчитися орієнтуватися в умовах надмірного потоку інформації? Як забезпечити інформаційну безпеку як окремій особистості так суспільству і державі в цілому? При цьому, під інформаційно безпекою особистості ми розуміємо не лише захист персональних даних, а й захищеність психіки, свідомості людини від деструктивних інформаційних впливів: маніпулювання свідомістю, розповсюдження чуток, нав'язування фальшивої або беззмістовної інформації, дезінформування, спонукання до самогубства, кібербулінгу тощо.

Ці питання гостро постають перед правоохоронними органами. Особливо в контексті підготовки фахівців до виконання завдань в особливих умовах. Адже інформаційно-психологічний вплив здійснюється як у мирний, так і у воєнний часи; із залученням телебачення, радіомовлення, преси, інформаційних систем (Internet), телефону, мистецтва (кіно, театри, виставки), літератури (документальної, мемуарної, художньої й т.д.), освітніх установ, а також за допомогою чуток, листівок та у ході особистого спілкування [2].

На даний час, в системі Національної поліції створенні підрозділи по боротьбі з кіберзлочинністю. До їх основних завдань відносять протидію кіберзлочинам у сфері інформаційної безпеки, а саме:

- соціальна інженерія – технологія управління людьми в Інтернет просторі;
- мальваре – створення та розповсюдження вірусів і шкідливого

програмного забезпечення;

- протиправний контент – пропагує екстремізм, тероризм, наркоманію, порнографію, культ жорстокості і насильства;

- рефайлінг – незаконна підміна телефонного трафіку;

- завчасне інформування населення про появу новітніх кіберзлочинів.

На нашу думку, правоохоронцям, які протидіють кіберзлочинності крім обов'язкової технічної підготовки, володіння навичками роботи з комп'ютером і загальним орієнтуванням в інформаційному просторі необхідна професійно-психологічна підготовка щодо протидії негативному інформаційно-психологічному впливу з використанням інтерактивних методів навчання. Одним з таких методів є соціально-психологічний тренінг, який дозволяє ефективно вирішувати завдання, пов'язані з розвитком мотиваційної, пізнавально-когнітивної, емоційно-вольової та комунікативно-поведінкової сфер особистості. Зазначимо, що саме через ці сфери особистості здійснюється інформаційно-психологічний вплив на психіку і свідомість людей.

Так, для курсантів Харківського національного університету внутрішніх справ, професійна діяльність яких в майбутньому буде пов'язана із забезпеченням публічної безпеки і порядку, превентивною та профілактичною діяльності, запобіганням та припиненням насильства в сім'ї (факультет № 3) та з профілактикою і розкриттям кіберзлочинів (факультет № 4) ми пропонуємо тренінг «Інформаційно-психологічна безпека». Метою даного тренінгу є розвиток навичок протидії негативному інформаційно-психологічному впливу на психіку і свідомість людини.

Впродовж тренінгу учасники відпрацьовують наступні теми:

Тема 1. Базові поняття інформаційної війни.

Поняття, цілі і завдання інформаційної війни [2, 3, 5]. Форми, види і закономірності інформаційно-психологічних впливів. Базові методи впливу в інформаційній війні: переконування і навіювання.

Виконуючи практичні вправи курсанти на власному досвіді знайомляться з методами впливу на пізнавально-когнітивну сферу особистості. Наприклад, відпрацьовуючи метод переконування, учасника тренінгу доводять до внутрішньої злагоди з певними умовиводами, а потім, на їх основі, формують нові установки (або трансформують старі), що відповідають поставленій меті. Крім того, курсанти знайомляться з різними способами і прийомами навіювання (переклеювання ярликів, перетасовки фактів, залякування, емоційного придушення) і навчаються аналізувати інформацію, яку їм пробують навіяти, шляхом зіставлення навіювання зі своїми цінностями, знаннями, поглядами, установками тощо.

Тема 2. Специфічні способи та прийоми інформаційно-психологічного впливу.

Формування знань про дезінформацію, маніпулювання свідомістю і розповсюдження чуток. Курсанти знайомляться з такими способами маніпулювання як інформаційне перевантаження, дозування інформації, велика брехня, зволікання та ін. Відпрацьовують навички протидії маніпулятивному впливу.

Тема 3. Соціальна інженерія в інформаційних технологіях

Дана тема є особливо актуальною для фахівців з організації інформаційної безпеки оскільки розкриває соціальну інженерію, як метод маніпулювання людиною або групою людей з метою злому систем безпеки і викрадення важливої інформації. Цитуючи американського криптографа, письменника і фахівця з комп'ютерної безпеки Б. Шнайєра «Лише атаки дилетантів націлені на машини; атаки професіоналів націлені на людей» [4] учасники тренінгу знайомляться з механізмами навмисного впливу на психічні особливості людини (ціннісні орієнтації, норми поведінки, життєві цілі, рівень знань тощо) для отримання необхідної інформації. Наприклад, соціоінженер – це зловмисник (шахрай), який здійснює атаку на людину, яка є частиною системи «людина-комп'ютер» і руйнує найдосконаліші і дорогі системи захисту інформаційних технологій.

Тема 4. Аналіз негативної інформації, розробка матеріалів контрвпливу та прийомів протидії.

Використовується методика протидії негативному інформаційно-психологічному впливу на особовий склад Національної гвардії України в умовах масових заворушень [2].

Тема 5. Забезпечення інформаційно-психологічної безпеки

Формується поняття про інформаційно-психологічну безпеку як стан захищеності духовного, душевного та фізичного благополуччя людини від впливів, які призводять до ураження її прав і свобод [5].

Представлений тренінг включає в себе наступні методи роботи: психотренінгові вправи, рольові ігри, дискусії, групове рішення проблем, моделювання ситуацій, психогімнастика, методи зворотного зв'язку і рефлексії тощо. Реалізація тренінгу «Інформаційна-психологічна безпека» буде сприяти як особистісному так і професійному розвитку майбутніх працівників поліції.

Список використаних джерел

1. Опанасенко Л. Правила життя для підростаючого покоління // *Голос України*.- 2010. – № 206.- С. 4.

2. Протидія негативному інформаційно-психологічному впливу на особовий склад Національної гвардії України в умовах масових заворушень: монографія / І.І. Ліпатов, Г.А. Дробаха, К.Ю. Гунбін та ін. – Х. : Нац. акад. НГ України, 2015. – 229 с.

3. Сенченко О. Новітні війни з використанням інформаційно-психологічної зброї // *Вісник книжкової палати*. – 2014. – № 8. – С. 1 – 6.

4. Шнайер Б. Материал из Викицитатника / Б. Шнайер. [Електронний ресурс]. – Режим доступу : https://ru.wikiquote.org

5. Юдін О.К., Богуш В.М. Інформаційна безпека держави. – Харків: Консум, 2004. 508 с.