НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ЦИВІЛЬНОГО ЗАХИСТУ УКРАЇНИ

Факультет пожежної безпеки

Кафедра автоматичних систем безпеки та інформаційних технологій

Начальник кафедри
полковник служби Ц.З.
доктор техн. наук, професор

Роман ШЕВЧЕНКО

"*26*" *серпня* 2024 р.

навчально-методичні матеріали

ВПЛИВ ВОЄННОГО СТАНУ

освітні компоненти "Основи інформаційних технологій",
"Прикладні інформаційні технології в сфері пожежної безпеки",
"Інформаційні технології в практиці наукових досліджень"

для здобувачів освіти в галузі знань 26 «Цивільна безпека»

першого освітнього рівня бакалавра освітньо-професійних програм «Пожежогасіння та аварійно-рятувальні роботи», «Пожежна безпека», «Цивільний захист», «Охорона праці»

другого освітнього рівня магістра освітньо-професійних програм "Пожежна безпека", "Управління пожежною безпекою", "Пожежогасіння та аварійно-рятувальні роботи"

третього освітнього рівня доктора філософії освітньо-професійних програм "Пожежна безпека", "Цивільний захист"

2024

ЗМІСТ

Тема 1. УКРАЇНА – НЕЗАЛЕЖНА, СУВЕРЕННА ДЕРЖАВА. ПЕРЕМАГАЄ ТОЙ, ХТО ПАМ'ЯТАЄ

Вже пройшло 33 роки з моменту отримання незалежності нашої держави – України. Але можна сказали, що у 1991 році відбулося відновлення нашої державності. Оскільки державність на наших землях існувала ще у часи Русі-України, козацькі часи та часи Української революції 1917-1921 років. Українці завжди відзначалися своїм волелюбним характером, мужністю та любов'ю до своєї землі. І українці завжди ставали на захист своєї землі, своїх домівок та своїх родин. Важкі часи переживає наша держава, бо сьогодні ми воюємо із підступним, злим та сильним ворогом державою російська федерація, проти якої українці воювали ще з давніх-давен.

Нажаль, як і багато років тому, Україна втрачає у війні з ворогом найкращих своїх синів та доньок, що кладуть своє життя на вівтар майбутньої сильної та вільної нашої держави. 29 серпня в Україні відзначається День пам'яті захисників України, які загинули в боротьбі за незалежність, суверенітет і територіальну цілісність України. Цей день встановлено Указом Президента України від 23 серпня 2019 року № 621 для увічнення героїзму військовослужбовців і добровольців, котрі віддали життя за батьківщину. Збереження і гідне вшанування пам'яті полеглих захисників України є обов'язком держави і суспільства.

У 1991 році Україна відновила незалежність. Однак російська федерація не відмовилася від спроб повернути контроль над Україною. Тиск посилився з приходом до влади у росії колишнього співробітника репресивного органу КДБ В.Путіна. Його система управління державою заснована на культі лідера, його монополії на владу, згортанні свободи слова і використанні "ручних" засобів масової (дез)інформації, нарощуванні силових органів із їх репресивно-каральним апаратом і переслідуванні незгідних. А ще Кремль повернувся до практики "збирання земель". Розпочав із підкорення Чечні, а продовжив підбуренням сепаратистських рухів у колишніх республіках – Молдові, Грузії, провокацією конфлікту на українському острові Тузлі. Зрештою в 2014 році рашисти розпочали гібридну агресію проти України. Так світ знову зіткнувся із режимом, який прагне переділу кордонів держав і прямує до новітнього тоталітаризму.

Сучасна російсько-українська війна розпочалася після Революція Гідності, головною вимогою якої було повернення України до європейського шляху розвитку і підписання Угоди про асоціацію з Європейським Союзом. Трагічною ціною протистояння на майдані стала Небесна Сотня – 107 загиблих героїв, різних за віком, статтю, освітою, з різних куточків України та з-за кордону. Віктор Янукович втік до росії та закликав Путіна здійснити військове вторгнення в Україну для відновлення його влади. російська федерація здійснила активну агресію – в Криму так звані "зелені чоловічки" (російські військовослужбовці без розпізнавальних знаків) захоплювали адміністративні будівлі, військові частини та інші стратегічні об'єкти.

Збройна агресія Російської Федерації проти України розпочалася 20

лютого 2014 року, коли були зафіксовані перші випадки порушення Збройними Силами російської федерації всупереч міжнародно-правовим зобов'язанням російської федерації порядку перетину державного кордону України в районі Керченської протоки та використання нею своїх військових формувань, дислокованих у Криму відповідно до Угоди між Україною і російською федерацією про статус та умови перебування Чорноморського флоту російської федерації на території України від 28 травня 1997 року, для блокування українських військових частин. На початковій стадії агресії особовий склад окремих російських збройних формувань не мав розпізнавальних знаків. Тож у лютому–березні 2014 року із захоплення росією Кримського півострова розпочалася сучасна російсько-українська війна. Про це заявив український парламент у своїй заяві "Про відсіч збройній агресії російської федерації та подолання її наслідків" від 21 квітня 2015 року і міжнародні суди. Зокрема, Європейський суд з прав людини підтвердив, що рф встановила контроль над Кримом з 27 лютого 2014 року.

У березні–квітні 2014 року російські спецслужби та диверсанти почали розхитувати ситуацію в південних і східних областях України, організовуючи антиукраїнські мітинги і спроби утворити незаконні квазідержавні утворення. У відповідь патріотичні українські сили чинили спротив масовими акціями з метою зберегти територіальну цілісність держави. На початку квітня росія приступила до реалізації плану "Новоросія" – захоплення території східних областей України. Після проголошення так званих "народних республік" на Донеччину та Луганщину безперешкодно і масово прибували загони російських диверсантів із військовою технікою і зброєю.

Проте план на повторення швидкого "кримського сценарію" дав збій. Боєздатні частини Збройних Сил України, підрозділів Міністерства внутрішніх справ України, Національної гвардії та добровольчі формування зламали намір агресора. Влітку 2014 року російські гібридні сили на сході України зазнавали значних втрат в особовому складі, озброєнні, військовій техніці. 23–25 серпня на територію Донецької та Луганської областей зайшли вісім батальйонних тактичних Збройних сил рф. До наступу залучили 70 російських військових частин, зібраних з усієї федерації, які розпочали новий виток ескалації агресії.

Але вже за травень – серпень 2014 року українські підрозділи провели більше 40 операцій – звільнили дві третини окупованих територій, понад 100 населених пунктів Донецької та Луганської областей. Сили АТО поступово брали ситуацію під контроль, локалізували деякі угруповання, звужували кільце ізоляції, віддаляли його від державного кордону. З'явилася можливість блокувати російських окупантів у районах Донецька, Макіївки, Горлівки, Луганська і розділити їх на окремі осередки і створити передумови для успішного завершення збройного конфлікту на Сході України. З 11 серпня 2014 року Штаб АТО планував операцію з розгрому основних сил незаконних збройних формувань "ДНР" і "ЛНР" у містах Єнакієвому, Горлівці, Первомайську, Стаханові та завершити зачистку Іловайська Донецької області від терористів і взяти його під контроль. Це дало б змогу блокувати незаконні озброєні підрозділи у Донецьку із півдня та сприяло б просуванню сил АТО для

звільнення Донецька. Але вторгнення регулярних російських військ та іловайська трагедія змусили українську сторону погодитися на умови перемир'я за крок до перемоги над окупантами. Тож 5 вересня було підписано Мінську тристоронню угоду (так званий Мінський протокол). А 24 лютого 2022 року російська федерація розпочала новий етап повномасштабної агресії проти України, який триває і досі.

Нам всім потрібно пам'ятати про полеглих від 2014 року в сучасній російсько-українській війні захисників і захисниць України. Вони стоять в одному ряду з усіма поколіннями борців за волю і державну самостійність – від воїнів Русі-України, лицарів Костянтина Острозького, козаків Петра Сагайдачного, Богдана Хмельницького та Івана Мазепи до бійців Армії Української Народної Республіки та Галицької армії Західно-Української Народної Республіки, Антигітлерівської коаліції часів Другої світової війни, Української Повстанської Армії. Це воїнство мужньо здобувало героїчні перемоги і ризикувало життям за українську свободу.

Україна вже 10 років переживає найбільше випробування в новітній історії – веде збройну боротьбу за незалежність і територіальну цілісність проти російського агресора. У нинішній війні ми платимо надзвичайно велику ціну. Безперечно, це не єдиний день у році, коли згадуються полеглі та віддається їм шана. Але це особливий день, нагода для всього суспільства зосередитися на вдячності та пошануванні, зробити все можливе, аби пам'ять про героїв була збережена та зміцнена на багато поколінь вперед. Тому що перемоги здобуває лише той, хто пам'ятає – vincit qui meminit. Поки триває війна, ми не можемо знати точну кількість загиблих, назвати всіх поіменно або розповісти всі героїчні або трагічні історії. Проте впевнені, що українське суспільство докладе максимум зусиль, щоб загиблі герої залишилися в нашій пам'яті не абстрактним образом або цифрою, а отримали належну шану. Аби наша пам'ять про них була живою і дієвою.

Поки триває воєнний стан і постійні загрози, ми не можемо збиратися на велелюдних мітингах на площах своїх населених пунктів, але **можемо поодинці прийти до поховання героїв, щоб віддати їм шану. Ми можемо підтримати їхні родини не лише увагою, добрим словом і турботою, а й конкретними справами.** Можемо розповісти – публічно чи у вузькому колі – про тих, кого знали особисто. Ми переконані, що після перемоги віднайдемо та плекатимемо й інші традиції пам'яті про загиблих воїнів. Ми вже називаємо і продовжимо називати на їхню честь вулиці, висаджуємо меморіальні сквери, засновуємо іменні стипендії, проводимо різні спортивні, патріотичні та культурно-мистецькі заходи. У нас уже є місця пам'яті та меморіальні об'єкти у публічному просторі. Також створюються сектори військових поховань, нові військові меморіали і Національне військове меморіальне кладовище, де з почестями ховатимуть загиблих (померлих) захисників і захисниць. Після перемоги в країні повинні постати особливі місця, з сучасною архітектурою і людяними меморіальним практиками, як свідчення, що ми шануємо, цінуємо і дякуємо. **Пам'ятаємо і будемо пам'ятати.**

Література

1. Матеріал надано заступником начальника центру-начальником відділу організації освітньої діяльності навчально-методичного центру М. Журавським.

Тема 2. ДЕРЖАВНІ РІШЕННЯ ЩОДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНИХ ПРАВ ГРОМАДЯН В УМОВАХ ВОЄННОГО СТАНУ

Гібридні конфлікти включають в себе різні елементи, в тому числі розвідку, яка іноді є більш важливою, ніж військові елементи. Володіння зброєю масового знищення не гарантує державі перемогу, якщо вона не має інформаційної переваги. Така перевага створюється системою заходів, яка переводить інформаційну безпеку держави у воєнний стан. Важливість безпеки у праві важко переоцінити. Зокрема, реалізація права на життя, безсумнівно, пов'язана з правом на безпеку. У саме поняття «безпека» сьогодні вкладається захист державою нас самих і того, що нам належить, від посягань інших осіб.

Інформаційна безпека включає не лише нормативно-політичну складову, а й інституційну сферу, яка передбачає діяльність органів, що її забезпечують, а також використання програмно-технічних засобів.

Сучасні технології, інтернет, мобільний зв'язок та використання різних систем комунікації не лише забезпечують зручність, але й роблять всю систему безпеки вразливою до атак. Створюються передумови для витоку інформації, з'являється можливість технологічного впливу для формування бажаної громадської думки, а також можливість фіксації та передачі стратегічної інформації противнику за допомогою незначних технологічних зусиль.

Втрата юрисдикції над окремими частинами України та прямі загрози існуванню Української держави та її народу часто унеможливлюють реалізацію прав, гарантованих Конституцією. Саме тому указом Президента України № 64/2022 тимчасово, на період дії правового режиму воєнного стану, можуть обмежуватися конституційні права і свободи людини і громадянина, передбачені статтями 30–34, 38, 39, 41–44, 53 Конституції України, а також вводяться тимчасові обмеження прав і законних інтересів юридичних осіб в межах та обсязі, що необхідні для забезпечення можливості запровадження та здійснення заходів правового режиму воєнного стану, які передбачені частиною першою статті 8 Закону України «Про правовий режим воєнного стану». Окрему і вагому групу у цих обмеженнях становлять інформаційні права та свободи людини і громадянина.

Захист національної безпеки визначається Конституцією України як найважливіша функція держави (ст. 17). Одна з причин виключно формального характеру та практичного незастосування різних концепцій безпеки, в тому числі, інформаційної полягала у відсутності до лютого 2022 року конкретизацій джерел інформаційних загроз для України, оцінки геополітичної обстановки й формування засобів інформаційної протидії.

У 2021 році була прийнята нова Стратегія інформаційної безпеки, яка передбачає комплексну взаємодію на основі Конституції України,

законодавства України, Стратегії національної безпеки України, затвердженої також стратегії кібербезпеки України та міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України.

Було передбачено наступне інформування: потенційні інформаційні загрози вже визначені: «Інформаційна політика російської федерації є загрозою не лише для України, а й для інших демократичних держав».

«Інформаційна безпека» – невід'ємна складова національної безпеки України, тобто стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших життєво важливих інтересів особи, суспільства і держави, за якого забезпечуються конституційні права і свободи людини і громадянина на збирання, зберігання, використання та поширення інформації. Одним з елементів інформаційної безпеки є стан захищеності демократичного устрою, що сприяє забезпеченню конституційних прав і свобод особистості та людей у державі.

«Інформаційна загроза» – потенційне або реальне негативне явище, тенденція чи чинник інформаційного впливу на особу, суспільство і державу, що застосовується в інформаційній сфері з метою перешкоджання чи ускладнення реалізації національних інтересів України, утвердження національних цінностей і може завдати прямої чи опосередкованої шкоди державним інтересам, національній безпеці та обороні [Про Стратегію інформаційної безпеки України. Указ Президента України від 28.12.2021].

Очевидно, що у воєнний час акцент на виявленні загроз та реагуванні на них змістився з необхідності забезпечення впливу на потенційні та існуючі загрози до звуження прав людини заради збереження держави. Так, у зв'язку із введенням в Україні воєнного стану тимчасово, на період дії правового режиму воєнного стану, вводяться тимчасові обмеження прав і законних інтересів юридичних осіб в межах та обсязі, що необхідні для забезпечення можливості запровадження та здійснення заходів правового режиму воєнного стану, які передбачені частиною першою статті 8 Закону України «Про правовий режим воєнного стану».

З моменту оголошення воєнного стану до регуляторних законів були внесені зміни, які враховують реалії війни. Вони стосуються регулювання окремих аспектів інформаційних відносин щодо заборони поширення певної інформації суспільно небезпечного характеру, врегулювання важливих аспектів технічної фіксації інформації в умовах воєнного стану та війни, встановлення або посилення відповідальності за поширення певної інформації та регулювання процесуальних заходів щодо вилучення розвідувальних даних.

Так, Верховна Рада ухвалила законопроєкт про кримінальну відповідальність за незаконну фото та відеозйомку переміщення ЗСУ та міжнародної військової допомоги під час воєнного стану.

Сьогоднішня військова реальність чітко демонструє, що інформація є «зброєю масового знищення». Тому існує потреба у забезпеченні національної інформаційної безпеки та дотриманні прав людини, водночас створюючи ефективні механізми, які дозволять людям уникнути наслідків порушень їх свободи та демократії.

Література

1. Боднар О. Б. Поняття та зміст права людини на безпеку та його співвідношення з суміжними правами // Актуальні проблеми юридичної науки. Київ, 2011. С. 88–93.
2. Конституція України; Верховна Рада України від 28.06.1996
3. «Про Стратегію національної безпеки України» Указ Президента України : Стратегія від 14.09.2020 № 392/2020.
4. «Про Стратегія інформаційної безпеки України» Указ Президента України від 28.12.2021 № 685/202.
5. Закон України про «Медіа» від 13.12.2022 № 2849-IX.
6. Русакевич А. І. Інформаційна безпека в умовах воєнного стану у аспекти забезпечення інформаційних прав громадян. DOI https://doi.org/10.32840/1813-338X-2023.2.31 // Держава та регіони. Серія: Право, 2023 р., № 2 (80).- С. 177-180

Тема 3. ІНФОРМАЦІЙНА БЕЗПЕКА В УМОВАХ ВОЄННОГО СТАНУ

Ми є свідками того, як здійснюється інформаційний вплив, спрямований на людську свідомість суспільства. Об'єктом цього впливу є як окремі особи, групи осіб, так і цілі держави. Психологічний вплив здійснюється за допомогою засобів масової інформації, а основою використання такого впливу є легкість сприйняття і поверховість. Створення масових інформаційних атак, ботів, фейків, як свідчать сучасні реалії, є ефективними інструментами дезорієнтації суспільства, залякування, маніпулювання та паніки. Спеціально створені інформаційні ресурси привчають людину бездумно сприймати інформацію і вірити в неї.

Питання інформаційної безпеки та культури в умовах війни є питанням виживання людини, суспільства та держави. Адже забезпечення інформаційної безпеки визначається не тільки інтересами держави, а й інтересами особи в контексті забезпечення її прав і свобод. Основою сучасної інформаційної безпеки є цілісність даних, доступність інформації, конфіденційність і надійність її збереження.

Захист інформаційних ресурсів є пріоритетним завданням фахівців з безпеки. Експерти поділяють види джерел загроз на дві групи: внутрішні; зовнішні. Важливою загрозою є спрямований вплив на моральний стан військ шляхом фальсифікації фактів військової історії, посилення соціальної напруги, спроб втягнути особовий склад у розгортання політичних конфліктів. Виконавцями таких погроз інформаційного характеру найчастіше виступають засоби масової інформації, спрямовані на створення напруженої ситуації. У ряді випадків навіть контакт особового складу з представниками преси може стати способом спеціальної обробки поданої ними інформації, що призведе до можливої втрати бойового духу особового складу. Іноді заходами такого впливу досягаються не тільки психологічні зриви, що призводять до військових злочинів чи дезертирства, а й створення у військах угруповань, спрямованих на

свідомий підрив обороноздатності країни.

Військовослужбовці, працівники ДСНС, МВС тощо зобов'язані вміти ідентифікувати такі загрози. Найбільш серйозною проблемою безпеки є соціальні мережі, за допомогою яких військовослужбовці можуть випадково оприлюднити важливу інформацію. Одним із основних завдань захисту безпеки держави має стати виявлення таких загроз та їх своєчасне усунення.

Заходи, які можуть бути застосовані для захисту інформації та забезпечення безпеки, також поділяються на дві групи:

– захист інформаційних систем від пошкодження та інформації від витоку та перехоплення;

– захист психіки особового складу від цілеспрямованого інформаційно-психологічного впливу.

Ці заходи мають здійснюватися комплексно і першою групою заходів є:

– захист об'єктів військової дислокації та розташованої в них комп'ютерної техніки від пошкодження вогнем або іншого навмисного виведення з ладу;

– захист систем від віддаленого вторгнення зловмисника, зокрема з установкою програмних продуктів, що забезпечують повний захист периметра від вторгнень;

– захист інформації, яка становить державну або військову таємницю, від витоку чи умисного розкрадання;

– радіоелектронний захист;

– використання захищених моделей комп'ютерів і програмного забезпечення, які не можуть бути пошкоджені заздалегідь створеними проблемами в їх кодах;

– розробка засобів електронної розвідки;

– використання соціальних мереж для свідомої дезінформації противника;

– захист систем зв'язку.

Друга група заходів включає:

– запобігання навмисного психологічного впливу на психіку військовослужбовців;

– корекція інформації, що транслюється потенційним супротивником.

Розробка інформаційної зброї розглядається як окремий напрям оборонної стратегії. Противник досить ефективно використовує інформаційну зброю, що можна побачити на прикладі країн, які беруть участь у військових конфліктах. Зброя використовується не лише в зонах бойових дій, а й у тих регіонах, які мають стати осередками дестабілізації. П

Практично кожен військовий об'єкт зараз знаходиться в зоні можливого ураження, тому до захисту його безпеки необхідно підходити комплексно. Держава неухильно займається вирішенням цих завдань і нарощує свій оборонний потенціал.

Розробка пропрієтарного програмного забезпечення допомагає уникнути системних ризиків. Також власні канали передачі даних в мережі Інтернет повинні забезпечувати можливість спілкування без порушення архітектури Всесвітньої мережі.

Серйозна вразливість систем автоматизованої системи управління також виникає через передачу інформації закритого характеру відкритими лініями зв'язку, що іноді дозволяють собі фахівці.

Література

1. Лизанчук В.В. Інформаційна безпека України: теорія і практика: підручник. Львів: ЛНУ ім. Івана Франка, 2017. 725 с

2. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Президента України від 25 лютого 2017 року № 47/2017.

3. Про рішення Ради національної безпеки і оборони України від 18 березня 2022 року «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану»: Указ Президента України від 19 березня 2022 року № 152/2022

4. Боднар І. Інформаційна безпека як основа національної безпеки. Механізм регулювання економіки. 2014. № 1. С. 68–75.

5. Про внесення змін до деяких законодавчих актів України щодо посилення кримінальної відповідальності за виготовлення та поширення забороненої інформаційної продукції. Закон України // Науковий вісник Ужгородського Національного Університету, 2023.- 127 с.

6. Інформаційна безпека. Підручник. Під ред. В.В. Остроухова. К.: Видавництво Ліра-К, 2021. 412 с

7. Смотрич Д.В., Браілко Л. Інформаційна безпека в умовах воєнного стану // Науковий вісник Ужгородського Національного Університету. Серія ПРАВО. Випуск 77: частина 2, 2023.- С. 121- 126.

Тема 4. АДМІНІСТРАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ ГІГІЄНИ ПІД ЧАС ВОЄННОГО СТАНУ В УКРАЇНІ

В умовах особливого періоду, який триває з 24 лютого 2022 року в теперішній війні України з рф за свободу та незалежність, одним з важливіших владних завдань не суто воєнного характеру є забезпечення інформаційної гігієни серед своїх громадян починаючи з простих обивателів і завершуючи першими особами країни.

Інформаційна гігієна інколи викривлено сприймається як правила споживацької інформаційної вибірковості. Неадекватне ставлення до інформаційної гігієни з боку осіб, які причетні до інформування населення, може вартувати десятків – сотень життів як цивільних осіб так й наших військових, створення хибної уяви про об'єктивну дійсність та такої ж неправдивої оцінки тих чи інших подій, пов'язаних з війною.

Сутність інформаційних війн полягає у дискредитації свого суперника, як у середині його країни так й зовні – в очах міжнародної громадськості і держав-партнерів зокрема. Виключну роль у забезпеченні інформаційної безпеки та її невід'ємної складової – інформаційної гігієни, відіграють норми

адміністративного права, які складають основу інформаційного законодавства України. Особливо потреба у більш якісному та дієвому правовому забезпеченню суспільних інтересів в інформаційній сфері держави актуалізувалася під час гарячої стадії воєнної агресії з боку рф, яка триває понад останніх 12 місяців.

Мета інформаційної гігієни – попередження негативного впливу інформації на психічне, фізичне та соціальне благополуччя людини, соціальних груп, населення в цілому, профілактика захворювань населення, пов'язаних з інформацією, оздоровлення оточуючого інформаційного середовища.

Для українських громадян в умовах воєнного стану виникла потреба у дієвих правилах інформаційної гігієни під час війни. Зокрема, однин з варіантів таких правил містить п'ять цілком доступних і зрозумілих положень.

Перше правило – не допомагати ворогу. Зараз ІПСО (*інформаційно-психологічна спеціальна операція, до елементів ІПСО відносяться дезінформація, пропаганда, перебільшення певної інформації або применшення іншої, диверсії в тилу, кібератаки*) один з ключових інструментів російської пропаганди. Вони були завжди, але зараз їхня концентрація в інформаційному полі критична. Переселенці, дискредитація війська, мовні питання – лише однин з сотень векторів, рф буквально моніторить інформаційне поле, знаходить точки болю українців та створює на їх основі тріщини у суспільстві.

Друге правило – розпізнавати фейк. У сучасних умовах розпізнати фейк можна, оцінивши, яку емоцію викликає інформація. Якщо ми бачимо інформацію, яку хочемо почути, або боїмося почути, варто прискіпливо таку інформацію перевірити. Це як боятися ядерного удару або повторного нападу з Білорусі. Такі вкиди здійснюються, щоби дестабілізувати суспільство.

Третє правило – брати інформацію з об'єктивних джерел. Це медіа з Білого списку (загальноукраїнські онлайн-медіа, наприклад: Суспільне, Ліга, Громадське, Бабель, Дзеркало тижня, Радіо Свобода, НВ, Українська правда, Укрінформ, Еспресо.

Четверте правило – не брати інформацію з російських джерел. Необхідно пам'ятати, що всі російські медіа тією чи іншою мірою, прямо чи опосередковано підігрують російській пропаганді. Це той факт, який журналісти-експерти постійно фіксують і виявити його не так вже і просто, якщо не аналізувати це на постійній основі й глибоко не розбиратися, як працює російська пропаганда. Тому самим розбиратися в тому, що правда, а що ні – вкрай небезпечно.

П'яте правило – пам'ятати про шахрайства. Більшість з них пов'язані з нібито виплатами допомоги. Так тільки за перші сім місяців війни 2022 року жертвами такого шахрайства стали понад 5000 українців, які на цьому втратили понад 100 млн. гривень. Цілять, першочергово у людей поважного віку. Обіцяють допомогу нібито від Президента, Євросоюзу і так далі.

Метою інформаційної гігієни є зниження негативного впливу інформації на психічний, фізичний і соціальний стан особи.

Потрібно використовувати прості правила, які допоможуть виробити імунітет від фейкових новин та ЗМІ-маніпуляцій.

1. Завжди перевіряйте джерело інформації, на яке посилається автор. Людина, яка створює новину, має спостерігати події на власні очі, скористатися відповідними документами чи процитувати людей.

2. Перевіряйте "експертність", якщо в ролі експертів – представники соціологічних компаній, організацій, інституцій, яких не існує в реальності, не вказані посади, використані загальні формулювання – »експерти/вчені вважають», скоріш за все ви натрапили на фейк.

3. Не робіть висновків на основі заголовків. За статистикою, 96 % людей оцінюють новини лише за заголовками, у якому можуть бути дані, що суперечать основній меті матеріалу чи спотворюють його взагалі.

4. З особливою обережністю ставтеся до матеріалу, який викликає сильні емоції. Якщо після прочитання новини у вас з'явилася певна реакція на неї (страх, паніка, обурення тощо), необхідно перевірити цю інформацію в інших джерелах.

5. Зведіть інформаційний кошик до мінімуму. Не треба читати новини з усіх можливих і неможливих ресурсів, намагайтеся стежити за інформацією тільки з офіційних джерел: звіти ЗСУ, військово-цивільних адміністрацій, український єдиний телеефір.

Література

1. Інформаційне суспільство. Енциклопедія сучасної України. Том 11. https://esu.com.ua/search_articles.php?id=12462.

2. О. Донченко. Правила інформаційної гігієни під час війни. 6 жовтня 2022. https://law.chnu.edu.ua/pravyla-informatsiinoi-hihiieny-pid-chas-viiny/.

3. Фільтруй: як відбити інформаційний наступ під час війни. 17 червня 2022. https://it- kharkiv.com/informatsiyna_hihiyena/.

4. Я. Конощук. Новий закон про медіа: що зміниться для онлайн-медіа, блогерів та газет. Судово-юридична газета. 8 січня 2023. https://sud.ua/uk/news/publication/258656-novyy-zakon-omedia-chto-izmenitsya-dlya-onlayn-media-blogerov-i-gazet.

5. Є. Курінний. Адміністративно-правове забезпечення інформаційної гігієни під час воєнного станув Україні // Науковий вісник Дніпропетровського державного університету внутрішніх справ. 2023. № 1.- С. 38-43.

Тема 5. ДОСВІД ІНОЗЕМНИХ ДЕРЖАВ У ПИТАННІ ПРОТИДІЇ ІНФОРМАЦІЙНИМ ВПЛИВАМ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ

Російська пропаганда продовжує негативно впливати на дедалі більшу частину населення всього світу. Вона успішно використовує інструменти демократії та може діяти безперешкодно, спираючись на достатньо високий рівень прав і свобод. Своєю чергою, низка провідних держав світу почали вживати додаткових заходів задля протидії поширенню російської пропаганди. Йдеться, зокрема, про впровадження обмежень на трансляцію провідних російських державних ЗМІ на території Європейського Союзу, таких як "RT

(Russia Today)", "Sputnik" та інших, про розробку у ЄС нового правового механізму боротьби з дезінформацією, який дозволить заморожувати активи та забороняти перетинати кордон російським пропагандистам, а також про зобов'язання маркувати контент іноземних держав, які орендують час в ефірах ЗМІ США.

Із самого початку російсько-української війни у 2014 році Україна розпочала провадити системну та послідовну інформаційну політику у питанні протистояння російській дезінформації. Для здійснення ефективних заходів у сфері захисту національного інформаційного простору в Україні було ухвалено низку законодавчих ініціатив, які дозволили створити відповідне правове підґрунтя для протидії пропаганді та вжити заходів для закриття російських та проросійських ЗМІ в Україні. Це, зокрема, Доктрина інформаційної безпеки України (2016); рішення РНБО від 28 квітня 2017 року "Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)", завдяки якому було заблоковано роботу низки російських інтернет-сервісів, у тому числі соціальні мережі "ВКонтакті" та "Одноклассники", а також блокування доступу до вебресурсів компаній"Яндекс", "Mail.ru Group", АТ "Лабораторія Касперського", "Dr.Web" тощо; рішення РНБО від 2 лютого 2021 року "Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)", унаслідок якого було заблоковано проросійські телеканали "112 Україна", "ZIK" та "Newsone"; Стратегія інформаційної безпеки (2021); рішення РНБО від 11 лютого 2022 року"Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)", яким було заблоковано роботу телеканалу "НАШ", а також діяльність компанії "Вітрина ТВ", яка надавала послуги трансляції російських телеканалів, що заблоковані в Україні ("Россия 1", "Пятый канал", "Россия-24", "Рен ТВ" та інші); Закон про заборону на виготовлення та розповсюдження інформаційної продукції, спрямованої на пропагування дій Росії (2022) та інші.

Розв'язану офіційною Москвою війну проти України Китай відмовився називати вторгненням, а китайські державні ЗМІ послідовно продовжують підтримувати основну тезу російської дезінформації щодо вини НАТО у розгортанні конфлікту. Ефір телеканалів розбалансований, звернення Президента України Володимира Зеленського відсутні, у той час як неверифіковані виступи російських спікерів продовжують транслювати в ефірі. Унаслідок того, що державні ЗМІ ретранслюють інформацію з російських медіа, у лютому 2022 року фейкове повідомлення про те, що Володимир Зеленський покинув територію України, було переглянуто понад пів мільярда разів на китайській платформі "Weibo", його також продублювали 163 ЗМІ по всій країні. Окрім цього, представники правлячої партії фактично стали рупорами російської пропаганди, повторюючи у своїх виступах основні дезінформаційні наративи РФ. Так партійний телеканал у Шанхаї заявив, що український Уряд навмисно створив жахливу картину вбивств росіянами цивільного населення у місті Буча, аби викликати співчуття Заходу, а в газеті Комуністичної партії КНР в одній зі статей ішлося про те, що "брудні світлини тіл на вулицях Бучі, передмістя столиці України Києва, були містифікацією".

Інформаційна експансія Росії у світі має на меті відбілити власну репутацію, змістити фокус уваги та деморалізувати супротивника шляхом сіяння паніки та зневіри серед користувачів. Разом із тим, стратегія використання російської пропаганди передбачає, передусім, здійснення інформаційного впливу на внутрішню авдиторію. Згідно з дослідженням медіаспоживання в Росії, яке було проведено компанією "Ромір", для отримання інформації про поточну та політичну ситуацію в країні росіяни використовують телебачення (68 %), інформаційні сайти та форуми (35 %), "YouTube" (27 %), "Telegram" (25 %). Прикметно, що дізнаються новини через спілкування зі знайомими, друзями та родичами 24 % респондентів. Зважаючи на такі результати, можемо констатувати про величезний вплив телебачення на формування свідомості "внутрішнього глядача". Цю тезу також підтверджують і результати соціологічного опитування "Левада-центру", що проведене протягом 24-30 березня 2022 року, які свідчать про безпрецедентну підтримку росіянами дій президента В.Путіна – їх схвалюють 83 % опитаних. Такий результат підтверджує ефективну пропагандистську політику РФ усередині країни, а також надає умовний кредит довіри владі для здійснення подальших агресивних дій щодо України.

Потужний інформаційний вплив РФ здійснюється також і на іноземні суспільства. Таким чином Росія намагається розфокусувати увагу довкола війни проти України, яку вона сама ж розв'язала, та заручитися підтримкою інших країн. Із початком повномасштабного вторгнення Росії в Україну 2 та 3 березня у соціальній мережі Twitter знову почали набувати популярності хештеги "IStandWithRussia" та "IStandWithPutin". Результати дослідження твітів, які містили вищезгадані хештеги, оприлюднила компанія "CASM Technology". На думку аналітиків, ця інформаційна операція спрямована на поширення російської дезінформації щодо війни в Україні у Бразилії, Індії, Китаї та африканських країнах.

Окрім цього Росія модифікує і методи поширення дезінформаційного контенту. Так 30 квітня 2022 року Міністерство закордонних справ Великої Британії заявило, що РФ використовує фабрику тролів для поширення дезінформації про війну в Україні та про окремих політиків певних країн у соціальних мережах.

Ще одним новим інструментом РФ для поширення пропаганди стала соціальна мережа "Tik-Tok". За даними дослідження вебсайту, що відстежує дезінформацію в інтернеті – "NewsGuard", новим користувачам соціальної мережі може рекомендуватися неправдивий контент про Україну вже протягом перших 40 хвилин після реєстрації.

Література

1. Кантур О. Досвід іноземних держав у питанні протидії інформаційним впливам Російської Федерації // Вісник Київського національного університету імені Тараса Шевченка. Державне управління, 2022.– Вип. 2 (16).– С. 5-12.

Тема 6. ІНФОРМАЦІЙНА БЕЗПЕКА ПРАЦІВНИКІВ ДСНС В УМОВАХ ВІЙНИ

Інформаційна безпека – це стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави.

Більш детальне формулювання інформаційної безпеки – це стан захисту інформаційних потреб окремих людей, суспільств і націй незалежно від того, чи існують внутрішні та зовнішні загрози інформації, її існуванню та постійному розвитку.

Під інформаційним середовищем розуміють сферу діяльності суб'єктів, пов'язану зі створенням, перетворенням і споживанням інформації.

З розвитком Інтернету, з'явилася можливість використовувати всі його досягнення в різних його проявах. Одним з таких проявів стали соціальні мережі, які набули на сьогодні статусу невід'ємного атрибуту нашого життя. Представити сучасну людину без соціальних мереж просто неможливо. Спілкування, пошук інформації і друзів, обмін новинами, можливість слухати музику, дивитися відео і фотографії.

Особливої уваги заслуговують соціальні мережі працівників ДСНС України в умовах воєнного стану. Інформація, що міститься на персональних сторінках соціальних мереж працівників ДСНС, надає змогу ідентифікувати особу, місце роботи і перебування, оцінити політичні вподобання та особисті інтереси. Тому з метою особистої інформаційної безпеки слід закрити особисті профілі Facebook, Instagram. Прибрати із профілей соціальних мереж особисту інформацію, обмежити коментарі, обмежити доступ до вашої сторінки у настройках приватності, не додавати без критичного аналізу профілю у друзі незнайомих людей, перевіряти облікові записи (акаунти) тих, хто хоче стати вашим другом.

Аккаунт можна «убезпечити шляхом використання багатофакторної автентифікації». Усі без винятку онлайн-ресурси (електронна пошта, хмарні сховища, соціальні мережі) дають користувачам змогу захистити свої облікові записи за двофакторної автентифікації. Як багатофакторна автентифікація можуть використовуватися:

1. SMS-повідомлення з тимчасовим кодом, який приходить на телефон, зареєстрований у сервісі.

2. Спеціальні програми, які генерують одноразовий тимчасовий код, який користувачеві потрібно ввести після введення пароля. Прикладом програми для багатофакторної автентифікації є Google Authenticator.

Працівники ДСНС також можуть долучатися до вилучення неприємного і неприйнятного контенту в інтернет-сервісах шляхом скарги на дану інформацію.

Таким чином, враховуючи загрози інформаційній безпеці особам рядового та начальницького складу ДСНС, а саме: загрози впливу неякісної інформації (недостовірної, фальшивої, дезінформації) на особистість, суспільство, державу; загрози несанкціонованого й неправомірного впливу

сторонніх осіб на інформацію і інформаційні ресурси (їх виробництво, системи формування й використання); загрози інформаційним правам і свободам особистості (праву на виробництво інформації, її поширення, пошук, одержання, передавання та використання; праву на інтелектуальну власність на інформацію, в тому числі й речову), працівники ДСНС України повинні дотримуватися правил інформаційної безпеки, описаних вище і правильно і вчасно оцінювати ризики, які виникають у інформаційному просторі, особливо під час воєнного стану.

Література

1. Стратегія кібербезпеки України. Безпечний кіберпростір – запорука успішного розвитку країни. Указ Президента України від 26 серпня 2021 року № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#n12.
2. Термін «Інформаційна безпека». Термінологія законодавства. Верховна Рада України: [сайт]. URL. https://zakon.rada.gov.ua/laws/term/11458.
3. Інформаційна безпека. Визначення інформаційної безпеки. URL:https://sites.google.com/site/informacijnabezpeka15/-ponatta-informacijnoie-bezpeki/viznacenna-informacijnoie-bezpeki.
4. Захист інформації та інформаційна безпека. URL: http://referatok.com.ua/work/zahist-informacii-ta-informacijna-be.
5. Соціальні мережі: різні аспекти впливу на людину. Українське право. URL: https://ukrainepravo.com/legal_publications/essay-on-itlaw/it_law_berkiy_ Social_networks_and_there_involves/.
6. Глєбова А.О., Пістрюга Т.В., Чуткий С.І. Онлайн безпека. Навчально-методичний посібник.- К.: Піксель, 2022.- 76 с.
7. Інформаційна безпека особистості URL: https://sites.google.com/site/infobezpekaosobu/informacijna-bezpeka.
8. Павлиш Т., Єськова К. Інформаційна безпека працівників національної поліції в умовах війни // Правовий часопис Донбасу.- Кривий Ріг: Донецький ДУВС. https://rep.dnuvs.ukr.education/server/api/core/bitstreams /85571b7e-8d0b-488d-8c40-f7732434676c/content

Тема 7. ЯК ЗАХИСТИТИСЯ ВІД ІНФОРМАЦІЙНИХ МАНІПУЛЯЦІЙ ПІД ЧАС ВІЙНИ

Сьогодні, крім реалій російсько-української війни, ми також живемо в час війни інформаційної.

Інформація – ефективна зброя для маніпуляцій у сучасному цифровому суспільстві – викривлення реальності, впливу, маніпулювання суспільною думкою. Тож розпочнемо з аналізу інформаційних загроз для нашої безпеки в інтернеті.

Чи правда, що наш особистий інфопростір заповнюють великою кількістю дезінформації та фейкових новин – як точково, так і внаслідок спланованих і чітко скоординованих інформаційно-психологічних операцій?

Для початку з’ясуймо, що лежить в основі інформаційних маніпуляцій. Насамперед – це представлення інформації таким способом, щоб сформувати в інших людей вигідний для відправника спосіб мислення, а також думки, погляди чи цінності.

Кожне інформаційне повідомлення має свою мету. Друзі розповідають нам про свої життєві новини. Наш уряд комунікує про зроблені реформи чи проведені зустрічі президента. Однак в інфовійні маніпуляції з інформацією використовують і з метою досягнення політичних цілей.

Яких саме? Розпалювати конфлікти всередині суспільства. Викликати настрої недовіри до влади. Провокувати зневіру щодо стійкості й сили нашої держави.

Без сумніву, останні 9 років в Україні активно ведеться протидія російським інформаційним маніпуляціям, але українцям треба виховувати й підтримувати свій “імунітет” до будь-яких інфоманіпуляцій і викривлень правди.

Якими шляхами інформаційні маніпуляції заповнюють наш інфопростір?

- Через поширення неправдивих новин.
- Спотворення фактів або зміну їхнього контексту.
- Використання провокаційних заголовків чи фото.

Які основні завдання маніпулювання інформацією?

- Спотворювати враження про ті чи ті події.
- Розпалювати емоції.
- Створювати певний імідж (позитивний або негативний) щодо чогось чи когось.

Дезінформація як одна з найпоширеніших інофоманіпуляцій часто є системною та масштабною. Це така неправдива або викривлена інформація, яку створюють, подають та поширюють із певною метою (насамперед – вплинути на отримувача, навмисно ввести в оману, ошукати, забезпечити третій стороні економічну чи політичну вигоду). Пам’ятаймо, що дезінформація може завдавати шкоди як особі, так і суспільству.

То як розпізнавати дезінформацію? Її основні елементи – це багатоканальність і повторюваність певних наративів.

Багатоканальність означає, що ту саму інформацію ви можете бачити в різних джерелах (особливо в неправдивих), що слугують її поширенню.

Повторюваність наративів – це трансляція певної думки в різних виглядах та з різними повідомленнями, але з однією метою – цілеспрямовано сформувати та нав'язати бажане ставлення до окремих ситуацій, подій чи особистостей у процесі дезінформаційних кампаній. Для досягнення цієї мети зазвичай формують цілу систему меседжів – чітких тез і викривлених фактів, які поширюють і підтверджують загальний наратив.

Щоб краще зрозуміти механізм впливу дезінформації, проаналізуймо ілюстрацію від громадського об'єднання "Детектор Медіа".

- Ми бачимо загальний наратив, який хоче сформувати росія, а саме “Україна – неспроможна держава”.

– Цьому наративу слугують відповідні меседжі.
– Ці меседжі поширюють різними каналами й використовують для створення фейків та маніпуляцій у контексті озвученого наративу.

Чи зазнавали ви впливу дезінформаційних кампаній? Якщо неодноразово “натрапляли” на повторювану тезу з різних інфоканалів, націлену сформувати у вас ту чи ту думку, то найімовірніше, що так. Згадаймо, наприклад, чітко повторювані наративи про наступ із боку Білорусі чи про знищення великої кількості української техніки, наданої партнерами.

На відміну від дезінформації, фейкові новини означають вужче поняття; це неправдива інформація, що може бути як частиною дезінформаційної кампанії, так і поодиноким вкидом.

Наприклад, новина про введення у травні графіків відключення світла виявилася фейковою, її відразу спростувало Міненерго.

Отже, безпека в інформаційному просторі насамперед передбачає нашу захищеність як користувачів, а також можливість вибирати та керувати тим, хто і як може впливати на нашу думку, погляди та цінності. Іншими словами – це також і інформаційна грамотність як елемент цифрової безпеки загалом.

Література

1. «Безпека в інтернеті під час війни: практичний курс». Модуль 1. Інформаційна грамотність і безпека в інтернеті. // Програма підвищення кваліфікації педагогічних та науково-педагогічних працівників закладів освіти. Освітній курс ГО "ПРОМЕТЕУС".

Тема 8. РИЗИКИ В СОЦІАЛЬНИХ МЕРЕЖАХ ТА МЕТОДИ ЇХ ЗАПОБІГАННЯ

У світі сучасних технологій і соціальних мереж безпека в інтернеті стає все важливішою. Як ви вже зрозуміли, усі наші взаємодії залишаються в інтернеті назавжди й формують чіткий цифровий слід. Навмисно чи випадково користувачі часто розголошують багато персональної інформації, яка дає змогу їх ідентифікувати. Зловмисникам, які аналізують такі відомості, стає значно легше уводити звичайних користувачів в оману та отримувати доступ до їхніх особистих даних.

Тож один із головних аспектів вашої особистої безпеки – оцінка потенційних ризиків. Це процес визначення потенційних небезпек і проблем, із якими користувач або користувачка може стикатися в соціальних мережах.

Що може загрожувати безпеці наших акаунтів у соціальних мережах?

– Несанкціонований доступ.
– Фішингові атаки.
– Шкідливе програмне забезпечення.
– Порушення конфіденційності.
– Викрадення акаунтів.

- Завдання шкоди для репутації.
- Потенційний вплив на психічне здоров'я.
- Соціальна інженерія.
- Витік даних.
- Фейкові акаунти та шахрайство.

Серед найбільш розповсюджених – неавторизований доступ та фішингові атаки.

Розгляньмо кожен із цих випадків.

1. У ситуації несанкціонованого доступу хакери або зловмисники намагаються скористатися чужими акаунтами в соціальних мережах через слабкі чи повторно використані паролі.

А за допомогою методів соціальної інженерії отримати паролі до акаунтів можливо навіть від самих користувачів.

Детальніше про правила безпечного поводження з паролями ви дізнаєтеся з наступних відео курсу. Тож будьте уважні.

2. Суть фішингових атак полягає в тому, що зловмисники діють ніби від імені надійної організації, наприклад, банку, щоб дізнатися від користувачів конфіденційну інформацію, а саме: логіни, паролі, фінансові дані.

Інструментами фішингових атак зазвичай слугують повідомлення, посилання або фальшиві сторінки для входу в соціальні мережі.

Як захиститися від фішингу.

- Пам’ятайте, авторитетні компанії не надсилатимуть електронні листи або повідомлення з лінками для оновлення вашої платіжної інформації.
- Звертайте увагу, фішингові адреси можуть відрізнятися від справжніх лише одним символом. Тож уважно перевіряйте написання адрес вебсайтів та електронної пошти.
- Пильнуйте, дізнавайтеся більше про приватність у мережах і керуйте видимістю своїх облікових записів: зробіть їх доступними лише для людей, яким довіряєте.
- Потрібно завжди контролювати, хто має доступ до вашої інформації та публікацій.

Немає сумнівів, що сьогодні всім користувачам важливо бути в курсі інтернет-загроз і вживати відповідних заходів безпеки, зокрема:

- використовувати надійні й унікальні паролі;
- користуватися двоетапною перевіркою;
- виявляти обережність щодо підозрілих посилань або повідомлень;
- систематично переглядати й коригувати налаштування конфіденційності;
- регулярно ознайомлюватися з новітніми функціями безпеки, що їх пропонують платформи соціальних мереж.

Література

1. «Безпека в інтернеті під час війни: практичний курс». Модуль 2. Оцінка

ризиків для безпеки в соціальних мережах. // Програма підвищення кваліфікації педагогічних та науково-педагогічних працівників закладів освіти. Освітній курс ГО "ПРОМЕТЕУС".

Тема 9. ВИКОРИСТАННЯ ЕЛЕКТРОННИХ ТАБЛИЦЬ ДЛЯ РІШЕННЯ ЗАДАЧ ПОЖЕЖНОЇ БЕЗПЕКИ В УМОВАХ ВОЄННОГО СТАНУ

Рішення задачі автоматизації розрахунку необхідної кількості вогнегасників для рішення задач на вимогу режиму воєнного стану на підставі методичних рекомендацій "з організації і забезпечення пожежної безпеки у військових частинах (підрозділах), які залучені до виконання бойових завдань", а також порадника "Пожежна безпека та цивільний захист" для голів та управлінців освітою територіальних громад під заг. ред. Грищенко А., Мацокіна А. (Швейцарсько-український проєкт DECIDE – Децентралізація для розвитку демократичної освіти) на прикладі рішення задачі розрахунку кількості вогнегасників для бліндажа опорного пункту, палатки в таборі, приміщення тощо.

Результат рішення задачі у вигляді таблиці за ескізом:

	A	B	C	D	E	F	G
1	Розрахунок необхідної кількості вогнегасників для поверху приміщенння						
2							
3	Довжина поверху (м.)	**15**					
4				Площа поверху ($м^2$)			
5	Ширина поверху (м.)	**10**					
6							
7		маса заряду (кг.)					
8							
9	Вогнегасник порошковий ВП-3 (ОП-3)	**3**		необхідна кількість		шт.	
10	Вогнегасник порошковий ВП-5 (ОП-5)	**5**		необхідна кількість		шт.	
11	Вогнегасник порошковий ВП-6 (ОП-6)	**6**		необхідна кількість		шт.	
12							

Наприклад, виходячи з вимох Правил пожежної безпеки, будинки закладів освіти на кожному поверсі повинні мати **не менше двох** переносних (порошкових, водопінних або водяних) вогнегасників з масою заряду вогнегасної речовини **5 кг і більше**, а в разі площі поверху **більше 100 $м^2$** кількість вогнегасників приймаються з розрахунку 1 кг вогнегасної речовини на кожні 10 $м^2$ площі підлоги.

Крім того, слід передбачати по одному газовому вогнегаснику з величиною заряду вогнегасної речовини 3 кг і більше: на 20 м^2 площі підлоги в офісних приміщеннях з оргтехнікою, коморах, електрощитових, вентиляційних камерах та інших технічних приміщеннях та на 50 м^2 площі підлоги в приміщеннях архівів, машзалів, бібліотек, музеїв.

Приміщення площею менше ніж 20 м^2, у яких розміщено оргтехніку, слід оснащувати переносним газовим вогнегасником ВВК-2.

Далі, порядок виконання наступний.

1. Перейдіть на будь-який вільній аркуш робочої книги. Змінити ім'я даного робочого аркуша на ім'я *Завдання4*. (У випадку відсутності аркуша створіть новий).

2. Створити на робочому аркуші таблицю згідно ескізу. Вкажіть розміри поверху приміщення (наприклад, ширина a=10м., довжина b=15м.)

3. В комірку **F4** вписати формулу розрахунку площі приміщення *=B3*B5*.

4. В комірку **E9** вписати формулу розрахунку кількості *=($F$4/10)/B9*.

5. Для того, що кількість завжди була цілою, доопрацюємо формулу, додавши функцію закруглення до більшого цілого*: =ROUNDUP(($F$4/10)/B9;0)*.

6. Так як при маленьких площах, кількість завжди не повинна бути менше 2, доопрацюємо формулу, додавши умовну функцію наступного виду: *=IF(ROUNDUP(($F$4/10)/B9;0)<2;2;ROUNDUP(($F$4/10)/B9;0))*.

7. За допомогою маркера заповнення виконати копіювання формули у відповідні комірки таблиці (діапазон E10:E11).

8. Виконати необхідне форматування та налаштувати ширину стовбців та висоту рядків таблиці для коректного відображення даних.

9. Зберегти робочу книгу, виконавши команду **Файл – Зберегти**.

Для перевірки отриманих вмінь та набуття відповідних навичок потрібно самостійно виконати наступне завдання: створити ескіз приміщення та додати формулу для розрахунку кількості вогнегасників, певного типу, наприклад, газових згідно умов викладених в ***аналізі проекту***.

Тема 10. ІНФОРМАЦІЙНО-ЛОГІЧНА МОДЕЛЬ ПОПЕРЕДЖЕННЯ НАДЗВИЧАЙНОЇ СИТУАЦІЇ ВНАСЛІДОК УДАРНО-ІМПУЛЬСНОГО ВПЛИВУ НА УКРИТТЯ

Аналіз втрат серед цивільного населення України із-за постійних цілеспрямованих терористичних обстрілів цивільної інфраструктури міст та селиш з боку російської федерації, доводить відсутність на першому етапі широкомасштабного вторгнення дієвих засобів укриття та захисту цивільного населення від сучасних вражаючих засобів.

Відповідно на поставлене воєнним часом завданням, а саме оперативне укриття цивільного населення від загроз обстрілів, особливо у разі досяжності міської інфраструктури засобами ураження осколкового типу, було знайдено у вигляді малих об'єктів укриття.

При проектуванні та будівництві простих укриттів необхідно передбачити можливість захисту цивільного населення, як від ураження осколкового типу, в рамках існуючих проектів, так і в рамках можливого високоточного ураження верхньої полусфери об’єктів укриття бойовою частиною БПЛА фугасного або термобаричного типу.

Фахівцями розроблена інформаційно-логічна модель попередження надзвичайних ситуацій місцевого рівня внаслідок ударно-імпульсного навантаження малих об’єктів укриття.

Для створення інформаційно-логічної моделі попередження надзвичайних ситуацій місцевого рівня внаслідок ударно-імпульсного навантаження малих об’єктів укриття слід спочатку визначити загальну концепцію формування методологічного забезпечення в сфері цивільного захисту, яка полягає у наступному – будь-яка надзвичайна ситуація це просторово-часовий процес. Укриття мають типовий життєвий цикл. Цей життєвий цикл зазвичай поділяється на такі етапи: проектування, будівництво, передача або введення в експлуатацію, експлуатація (щоденне використання за призначенням, з регулярним ремонтом і модернізацією), закриття або виведення з експлуатації, демонтаж і утилізація. На всіх етапах життєвого циклу можуть статися техногенні аварії, пожежі, вибухи та інші події.

Згідно з основними положеннями теорії управління, процес управління – це процес, за допомогою якого суб'єкт управління безперервно впливає на систему управління або об'єкт управління з метою забезпечення його необхідної поведінки або зміни певних характеристик об'єкта управління. Основною метою управління в надзвичайних ситуаціях є запобігання катастрофічним подіям та мінімізація їх наслідків у разі виникнення. Об'єктом управління є організація або група людей, яку прийнято називати органом управління. Їх завданням є спостереження за суб'єктом управління. У цьому випадку моніторинг – це низка заходів, а саме спостереження за об'єктом управління, реєстрація (документування) його параметрів, обробка та систематизація зареєстрованих даних. Прогнозування стану об'єкта управління у відповідь на зміну зовнішніх факторів, що діють на об'єкт з зовні, і внутрішніх факторів, що змінюють стан об'єкта управління в результаті процесів, що відбуваються всередині об'єкта. На основі прогнозу суб'єкт управління готує та обґрунтовує управлінські рішення, які впливають на об'єкт і змінюють або підтримують його стан.

Таким чином, слід зазначити, що надзвичайна ситуація - це об'єктивний (існуючий незалежно від ставлення до нього) просторово-часовий процес, який поділяється на п'ять етапів. Це: накопичення рутинних негативних факторів, екстремальний розвиток негативних факторів, виникнення катастрофічної події, ліквідація безпосередніх наслідків цієї події та мінімізація довгострокових наслідків. Кожен тип надзвичайної ситуації пов'язаний з певною катастрофічною подією, яка може статися, відбувається або вже сталася. З іншого боку основна мета управління надзвичайними ситуаціями – запобігти виникненню катастрофи, а якщо вона все-таки сталася, то мінімізувати її наслідки. Завдання процесу управління формулюються

відповідно до стадії надзвичайної ситуації.

Враховуючи наведене була запропонована наступна інформаційно-логічна модель попередження надзвичайних ситуацій місцевого рівня внаслідок ударно-імпульсного навантаження малих об’єктів укриття, яка представлена на рис. 1.

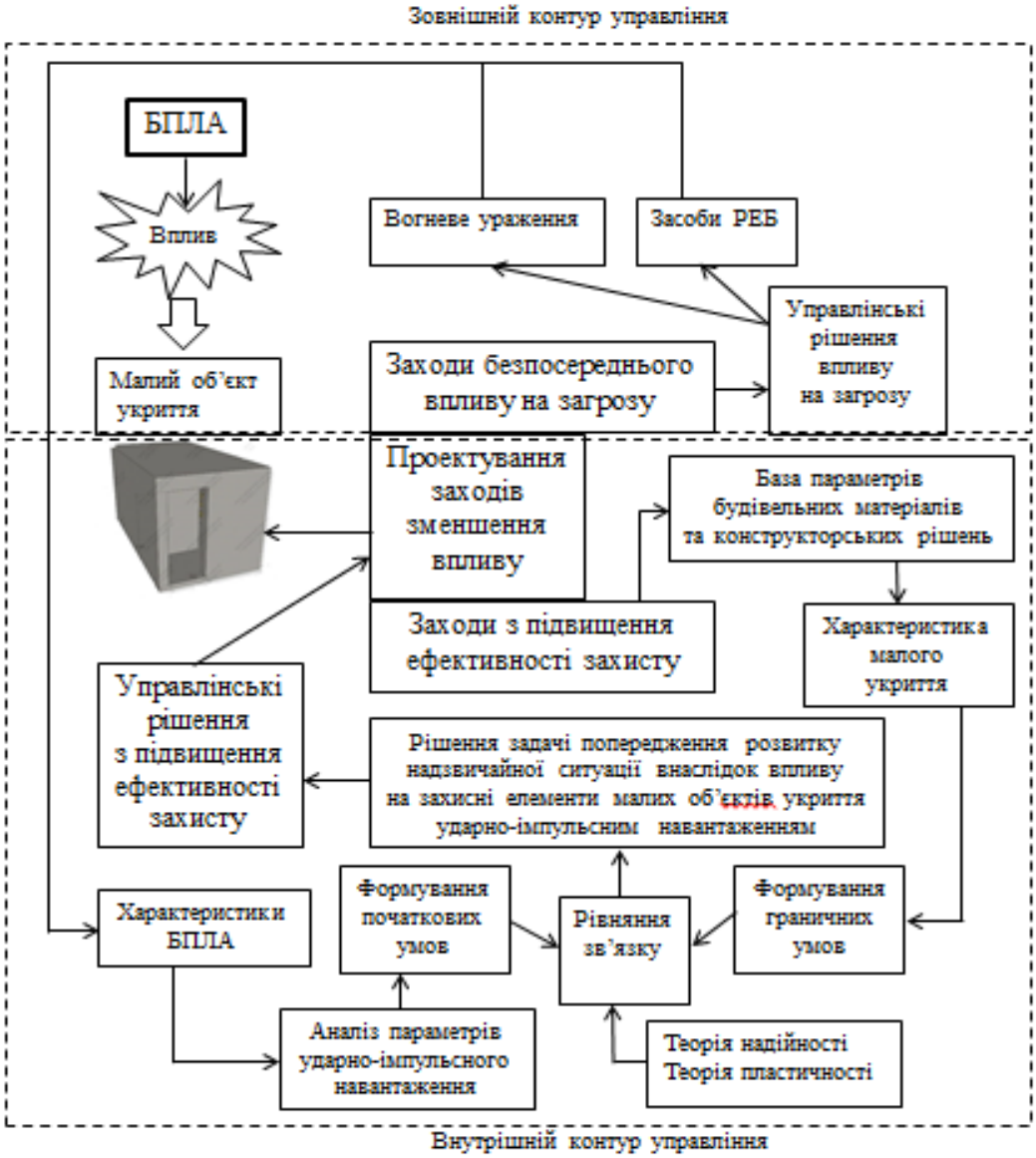

Рис. 1. Загальна схема інформаційно-логічної моделі попередження надзвичайних ситуацій місцевого рівня внаслідок ударно-імпульсного навантаження малих об’єктів укриття

Інформаційно-логічна модель передбачає наявність двох контурів управління системою безпеки малого об’єкту укриття: зовнішній та внутрішній. Слід відмітити, що зовнішній контур є невід’ємною складовою загальної міської (регіональної) системи протиповітряного захисту та включає наступні блоки, а саме блок заходів безпосереднього впливу на загрозу (ударний БПЛА) у вигляді засобів вогневого ураження та засобів РЕБ. Результатом успішного відпрацювання управлінських рішень зовнішнім контуром управління, з одного

боку є ліквідація загрози з боку ворожого ударного БПЛА, з іншого боку фактичний досвід та окремі елементи БПЛА є основою для формування початкових умов математичної моделі попередження надзвичайних ситуацій терористичного характеру внаслідок ударно-імпульсного навантаження малих об'єктів укриття. Початкові умови є результатом відпрацювання двох послідовно працюючих блоків – блок збору характеристик БПЛА та блоку аналізу ударно-імпульсного навантаження, що має місце або прогнозується виходячи з характеристик ударного БПЛА.

Підґрунтям внутрішнього контуру управління знаходиться блок проектування заходів зменшення впливу, який і визначає подальший інформаційний обмін у рамках даного контуру. А саме запускає блок підвищення ефективності захисту, який отримує статистичну та прогностичну інформацію, щодо НС які мали місце (характер ураження та наслідки). Це дозволяє у подальшому постійно оновлювати інформацію характеристик будівельних матеріалів, які використовуються при будівництві об'єктів укриття та ефективності конструкторських рішень. Як наслідок формуються характеристики малого об'єкту укриття. Результатом роботи відповідного блоку є формування граничних умов математичної моделі попередження надзвичайних ситуацій терористичного характеру внаслідок ударно-імпульсного навантаження малих об'єктів укриття. Основою блоку формування рівняння зв'язку математичної моделі попередження надзвичайних ситуацій терористичного характеру внаслідок ударно-імпульсного навантаження малих об'єктів укриття є теоретичні та практичні здобутки теорії надійності та її похідної теорії пластичності. Відповідне рішення задачі попередження надзвичайних ситуацій терористичного характеру внаслідок ударно-імпульсного навантаження малих об'єктів укриття дозволяє у подальшому управлінські рішення з підвищення ефективності захисту.

У якості загальних рекомендацій також слід зазначити, що під час будівництва малих сховищ необхідно дотримуватися всіх вимог законодавства у сфері будівництва. Захисні характеристики вище зазначених споруд після завершення будівництва повинні відповідати відповідному сховищу або протирадіаційному укриттю, а процедура реєстрації є такою ж, як і для відповідних захисних споруд цивільного захисту. Основні вимоги до евакуації населення викладені в положеннях Закону України "Про цивільний захист України". Закон визначає типи захисних споруд цивільного захисту з необхідними захисними властивостями для певних категорій населення залежно від місця проживання, сфери діяльності та/або інших загроз. Разом з цим ДБН В.1.2-4:2019 визначено основні небезпечні зони згідно яких відбувається планування розміщення захисних споруд цивільного захисту, а ДБН В.2.2-5-97 встановлено норми щодо захисних властивостей захисних споруд цивільного захисту необхідні в вищезазначених зонах. Там, де немає необхідності підтримувати постійну готовність, можна будувати споруди подвійного призначення з відповідними захисними характеристиками. З огляду на вищезазначене, при виборі проектних рішень слід враховувати потребу в спорудах цивільного захисту, необхідність підтримання їх у постійній

готовності та майбутню пропускну спроможність споруд.

Література

1. Алімпієв А.М., Пєвцов Г.В. Особливості гібридної війни рф проти України. Досвід, що отриманий Повітряними Силами Збройних Сил України. Наука і техніка Повітряних Сил Збройних Сил України. 2017. № 2. С. 19-25.

2. Мосов С.П., Хорошилова С.Й. Особливості застосування тактичної безпілотної розвідувальної авіації у воєнних конфліктах. Збірник наукових праць Центру воєнно-стратегічних-досліджень Національного університету оборони України ім. І. Черняховського, 2018, № 1(62).- С. 90-96.

3. Ільяшов О.А., Мосов С.П. Розвідка у сучасних воєнних конфліктах за досвідом іноземних країн.- Київ: РУМБ, 2011.- 280 с.

4. Корсунов С.І., Волков А.Ф., Оборонов М.І., Орєхов С.В. та ін, Трансформація завдань безпілотної авіації: від створення до застосування у воєнних конфліктах сучасності. Наука і техніка Повітряних Сил Збройних Сил України, 2021, № 3(44).- С. 66-81.

5. Безпілотна авіація у військовій справі: монографія / Мосов С. П. та ін. Київ : Інтерсервіс, 2019.- 324 с.

6. Корсунов С.І., Левагін Г.А., Коротій В.О. Застосування засобів повітряного нападу провідних країн світу у збройних конфліктах і локальних війнах // Збірник наукових праць.- Х: ХУПС, 2016, № 3(140).- С. 131-135.

ПЛАН-СХЕМА
використання матеріалів в лекціях, практичних заняттях та лабораторних роботах навчальних дисциплін

№ з/п	Тема заняття з робочої програми, силабуса навчальної дисципліни	Номер теми до заняття									
		1	2	3	4	5	6	7	8	9	10
	ОК Прикладні інформаційні технології в сфері пожежної безпеки										
1	Лекція 1. Сервіси Інтернет, принципи побудови web-ресурсів	×									
2	Лекція 2. Мережі, обладнання, протоколи			×							
3	Практичне заняття 2. Робота в мережі, мережні команди					×					
4	Практичне заняття 3. Сервіси та програми віддаленого доступу								×		
5	Лекція 5. Законодавство сфери інформаційних технологій в діяльності ДСНС України		×								
6	Семінар 2. Альтернативне офісне програмне забезпечення						×				
7	Практичне заняття 8. Простий пошук інформації за ключовими словами та розширений пошук з використанням символів, знаків та операторів							×			
	ОК Основи інформаційних технологій										
1	Лекція 1. Загальні відомості про табличний процесор Microsoft Excel.	×									
2	Лабораторна робота 7. Рішення прикладних та науково-технічних задач у середовищі MS Excel.									×	
3	Лекція 5. Загальні поняття про комп'ю-терні мережі. Всесвітня мережа					×					
	ОК Інформаційні технології в практиці наукових досліджень										
1	Лекція 1. Інформаційні системи. Локальні та глобальні комп’ютерні мережі.	×									
2	Лекція 3. Інтернет технології. Принципи створення та розміщення інформації на web-сторінках						×				
3	Практичне заняття 1. Пошук релевант-ної інформації в мережі Internet								×		
4	Лекція 7. Обробка та аналіз даних за допомогою електронних таблиць									×	
5	Практичне заняття 9. Логічне та фізичне проектування інформаційних систем										×