державних дат, засвідчують своїм талантом цінності свободи й незалежності.

Філармонійна діяльність – це важливий фактор урбаністики, віддзеркалення людських настроїв і стосунків. І в мирний час, й у воєнний.

Список використаних джерел

1. Обласна філармонія дала безкоштовні концерти вже у 37 громадах Полтавщини. URL: https://poltava.to/news/67996/.

2. *У Полтаві та області мають запрацювати заклади культури в яких є бомбосховища або укриття.* URL: https://poltavawave.com.ua/p/u-poltavskii-oblasti-maiut-zapratsiuvati-zakladi-kulturi-621795.

3. Кодекс цивільного захисту України. URL: https://zakon.rada.gov.ua/laws/show/5403-17#Text.

4. Постанова КМУ № 138 від 10.03.2017 «Деякі питання використання захисних споруд цивільного захисту»: URL: https://zakon.rada.gov.ua/laws/show/138-2017-%D0%BF#n76.

КІБЕРБЕЗПЕКА В УКРАЇНІ В УМОВАХ ВОЄННОГО СТАНУ

Навроцький І. С.

здобувач першого (бакалаврського рівня) вищої освіти, факультету технологій та дизайну Полтавського національного педагогічного університету імені В. Г. Короленка

Відколи Росія почала широкомасштабне вторгнення в Україну, кібербезпека стала одним із ключових фронтів у цій війні. Російські хакери безперервно атакують інфраструктуру України, знищуючи важливі об’єкти, викрадаючи дані та намагаючись спричинити хаос.

Зіткнувшись із зростаючою загрозою кібербезпеці, Україна, як і багато інших країн, стикається з необхідністю зміцнення можливостей кіберзахисту, особливо в умовах воєнного стану. Воєнний стан у країні підвищує ризик кібератак та інших форм кіберзагроз, які можуть мати серйозні наслідки для національної безпеки. Саме тому Україна має відповісти на ці виклики шляхом вдосконалення заходів кібербезпеки.

Одним із головних викликів для кібербезпеки України в умовах воєнного стану є збільшення кількості кібератак з боку ворогів країни.

Агресія Росії проти України, зокрема окупація територій та підтримка військових дій проти українських сил, також супроводжується активною кібервійною. Хакерські угруповання за підтримки російських військових і спецслужб активно здійснюють кібератаки на інформаційні системи та мережі

України, займаючись шпигунською діяльністю, завдаючи якісних матеріальних збитків і викликаючи соціальну нестабільність.

За даними українських служб кібербезпеки, ці кібератаки здійснюються різними способами та формами.

Серед них розповсюдження шкідливих програм (шкідливого програмного забезпечення), атаки на критично важливі системи та інфраструктуру, втручання у роботу телекомунікаційних мереж, а також кібершпигунство та кібервимагання.

Крім того, українські експерти з кібербезпеки відзначають збільшення кількості атак соціальної інженерії, коли зловмисники користуються довірою людей і дезінформацією для несанкціонованого доступу до інформації та обману користувачів. Такі атаки є більш складними, і їх важче виявити системами захисту, що ускладнює виявлення та захист від кібератак.

У зв'язку з цим, захист важливих інформаційних систем і мереж стає найважливішим завданням українських організацій, які працюють у сфері кібербезпеки.

У цьому контексті важливо не лише вдосконалювати технічні засоби захисту та спостереження, але й підвищувати обізнаність громадян та експертів щодо того, як захиститися від кіберзагроз.

Усім українцям важливо знати основні загрози кіберпростору та як від них захиститися [1]. Такими кіберзагрозами є:

- кібератака на критичну інфраструктуру (електростанції, водопроводи, транспортні системи). Ці атаки можуть призвести до серйозних збоїв у критично важливих системах, завдати шкоди економіці та поставити під загрозу життя;

- крадіжка даних: особисті, комерційні та державні дані українців. Ця інформація може бути використана для шантажу, вимагання, розпалювання ненависті та підриву довіри до уряду;

– дезінформація та пропаганда: поширює неправдиву інформацію, розпалює ненависть і підриває довіру до уряду. Це може призвести до соціальних заворушень, громадських безладів і неправильних рішень;

– фішинг і кібершахрайство: запитує особисті та банківські дані, розповсюджує зловмисне програмне забезпечення. Ці дії можуть завдати фінансових збитків українському народу та призвести до втрати конфіденційної інформації.

Україна зробила кроки для посилення кібербезпеки в умовах воєнного стану, але потрібні додаткові зусилля та інвестиції. Лише спільними зусиллями української влади, приватного сектору та міжнародних партнерів Україна

зможе забезпечити ефективний захист кіберпростору в умовах воєнного стану.

Науковці пропонують такі методи безпеки:

- використовуйте надійні паролі: використовуйте надійні унікальні паролі для всіх облікових записів. Це ускладнить доступ зловмисників до даних;

- увімкнути двофакторну автентифікацію: покращує захист облікового запису. Навіть якщо зловмисник знає ваш пароль, він не зможе увійти у ваш обліковий запис без коду авторизації, надісланого на ваш мобільний телефон або електронною поштою;

– оновлення програмного забезпечення: регулярно оновлює вашу операційну систему, браузер та інші програми. Розробники програмного забезпечення регулярно випускають оновлення, які виправляють уразливості, якими можуть скористатися хакери;

- встановіть антивірусне програмне забезпечення: встановіть надійне антивірусне програмне забезпечення та брандмауери для захисту від шкідливих програм. Антивірусне програмне забезпечення допомагає виявляти та видаляти шкідливі програми з комп'ютера.

- будьте обережні, натискаючи посилання та відкриваючи вкладення: не відкривайте посилання та вкладення з невідомих джерел. Ці посилання та вкладення можуть містити зловмисне програмне забезпечення, яке може пошкодити ваш комп'ютер або викрасти дані;

- резервне копіювання даних: регулярно створюйте резервні копії важливих даних [2].

Таким чином, у контексті військового стану, кібербезпека стає ключовим елементом національної безпеки для України. Зростання кібератак з боку противника, зокрема підтримуваних російським агресором, створює серйозні загрози для інформаційних систем та мереж країни. Ці атаки можуть мати різні форми та методи, включаючи у себе використання шкідливого програмного забезпечення, соціальну інженерію, а також кібершпигунство та кібершантаж.

Для забезпечення ефективного захисту під час військового стану Україна повинна посилити свої заходи з кібербезпеки. Це включає у себе підвищення свідомості громадськості та фахівців щодо кіберзагроз, розвиток технічних засобів захисту та моніторингу, а також активізацію співпраці з міжнародними партнерами. Тільки шляхом спільних зусиль усіх зацікавлених сторін Україна зможе забезпечити ефективний захист свого кіберпростору та зберегти національну безпеку в умовах військового конфлікту [3].

Список використаних джерел

1. Кібербезпека під час війни: базові заходи з кіберзахисту для українських організацій. URL: https://www.kmu.gov.ua/news/kiberbezpeka-pid-

chas-viiny-bazovi-zakhody-z-kiberzakhystu-dlia-ukrainskykh-orhanizatsii

2. Кібербезпека під час війни: як надійно захистити ваші пристрої і дані на них. URL: https://koda.gov.ua/kiberbezpeka-pid-chas-vijny-yak-nadijno-zahystyty-vashi-prystroyi-i-dani-na-nyh/.

3. Кібербезпека. URL: https://moz.gov.ua/kiberbezpeka.

ПРОБЛЕМИ ФОРМУВАННЯ КУЛЬТУРИ БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ УЧНІВСЬКОЇ ТА СТУДЕНТСЬКОЇ МОЛОДІ У ПТНЗ

Дуброва Ю. А.
майстер виробничого навчання
Регіонального центру професійно-технічної освіти м. Зіньків

Нещодавні події в нашій країні спричинили глибокі зміни у всіх сферах суспільного життя. Зростання технічних можливостей та збільшення випадків техногенних та екологічних катастроф акцентують необхідність у висококваліфікованих спеціалістах, які забезпечуватимуть дотримання державних стандартів і законодавчих вимог у сфері безпеки.

Фахівці з безпеки праці, робота яких включає управління складними взаємодіями між людьми та технікою, набувають особливого значення. З цієї причини роль системи вищої освіти у підготовці молоді до питань безпеки життєдіяльності та вироблення безпечної поведінки стає все більш значущою і відповідальною. Ключове завдання університетів полягає у формуванні у студентів свідомого ставлення до власної безпеки, що має велике значення для їх здоров'я та безпеки оточуючих.

Дисципліни, пов’язані з безпекою, є важливими для підготовки майбутніх педагогів та професійних фахівців, зосереджуючись на необхідних знаннях і вміннях у сферах охорони праці, фізіології, гігієни праці, виробничої санітарії, безпеки процесів праці, та пожежної безпеки, які регулюються державними освітніми стандартами.

Наукові дослідження та публікації, що стосуються навчання дисциплінам безпеки в університетах України згідно з кредитно-модульною системою, представлені у роботах Я. Семчука, О. Малишевської та Р. Борисюка. Процес покращення підготовки студентів у цій сфері аналізується у дослідженнях В. Жидецького, Є. Желібо, Н. Заверухи та В. Зацарного.

Метою цієї статті є дослідження поточного стану, проблем і законодавчих основ викладання безпекознавства у вищих навчальних закладах України. Основна частина роботи фокусується на аналізі взаємозв’язку між