7. Developing and implementing cyber defense technologies: it is necessary to actively develop and implement cyber defense technologies, such as systems for detecting and preventing cyber attacks, encrypting data, and identifying anomalous activity.

These priorities and strategies will help Ukraine strengthen its cybersecurity and preserve national security in the face of armed aggression and bring the country closer to victory.

1. Peculiarities of anti-Ukrainian informational (cyber) influence on Ukraine - Oleksandr Vitaliyovych Levchenko, Volodymyr Vasyliovych Okhrimchuk - Protection of information. – 2022. – Vol. 24, No. 4.

URL: https://odnb.odessa.ua/view_post.php?id=4361

2. Koterlin I.B., Actual problems of domestic jurisprudence No. 1.

URL: http://apnl.dnu.in.ua/1_2022/25.pdf

3. Manulov Y.S., Ensuring cyber security of critical infrastructure objects in the conditions of cyber war

УДК 004.738.5:681.5
DOI: 10.31733/15-03-2024/2/353-354

Марія ЗАВ`ЯЛОВА
студентка ННІ права
та інноваційної освіти

Ігор ЧОБОТЬКО
старший викладач кафедри
фізичного виховання
та тактико-спеціальної підготовки
Дніпропетровського державного
університету внутрішніх справ

ДИСКУРС ЩОДО РОЗУМІННЯ ОКРЕМИХ АСПЕКТІВ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Сучасний прогрес людства визначається швидким розвитком інформаційних новацій, зокрема комп'ютерних технологій, які є невід'ємною складовою сучасності. Інтернет, безперечно, став неодмінною частиною нашого життя [1]. Однак у кіберпросторі поширені різноманітні загрози, такі як маніпуляції, дезінформація, пропаганда фізичного чи сексуального насилля, поширення заборонених товарів, підбурювання до самогубства та інші. Суспільство усвідомлює потребу у впровадженні передових заходів кібербезпеки, але варто зауважити, що лише свідомість не є достатньою. Кібербезпека постійно обговорюється, оскільки суспільство ще не має достатньої медіаграмотності для повного розуміння загроз. Зростання кількості кримінальних правопорушень у кіберпросторі підкреслює важливість цього питання як на національному, так і на міжнародному рівнях [2].

Будь-який стрімкий розвиток супроводжується як позитивними, так і негативними явищами. Згідно з програмними документами ООН, універсальне підвищення кібербезпеки передбачає врахування різних аспектів, таких як інформованість, відповідальність, етика, демократія, оцінка ризиків, впровадження засобів безпеки та управління ними, а також переоцінка [3]. Націленими напрямами забезпечення безпеки в кіберпросторі є інформаційна безпека, безпека мережі, безпека Інтернету та захист критичних інфраструктур [4].

Одним із недостатньо вивчених аспектів боротьби з цією злочинністю є соціальний план щодо формування глобальної культури кібербезпеки, зокрема в галузі освіти та науки загалом. Комп'ютерна безпека має у своєму складі широкий спектр проблем у сфері телекомунікацій та інформатики, пов'язаних з контролем та оцінкою ризиків, що виникають при використанні комп'ютерів, гаджетів та комп'ютерних мереж [5].

Згідно з Законом України «Про основні засади забезпечення кібербезпеки України», кібербезпека визначається як захист інтересів людини, суспільства та держави в кіберпросторі. Особливу увагу слід звернути на правові, моральні та суспільні аспекти

культури кібербезпеки, а також на індивідуальний розвиток навичок та використання засобів безпеки в кіберпросторі. Також слід відзначити, що соціальна інженерія в наш час є поширеною, інформація, яка базується на особистих даних особи, її психологічних та інших індивідуальних особливостях, може використовуватися для отримання важливої інформації.

Основні форми соціальної інженерії можна класифікувати наступним чином:

– Претексінг: це вчинення певних дій за попередньо складеним планом. Під час використання цієї техніки особа, що здійснює протиправні дії, намагається зібрати особисті дані жертви, такі як ім'я, місце роботи або навчання, шляхом реальних запитів, зроблених в ім'я жертви.

– Фішинг: це форма інтернет-шахрайства, спрямована на отримання конфіденційної інформації користувачів різних систем шляхом надсилання підроблених листів, що містять запити про особисті дані, такі як логіни та паролі, або навіть посилання на фальшиві веб-сайти.

– Qui pro quo: ця техніка полягає у відправці протиправних запитів через електронну пошту від імені особи, яка виглядає як співробітник технічної підтримки. Зловмисник повідомляє про виникнення проблем на робочому місці та намагається змусити жертву виконати певні команди для вирішення неіснуючих проблем.

– Дорожнє яблуко: ця техніка полягає у розповсюдженні CD-дисків або флеш-накопичувачів у громадських місцях, які можуть містити віруси або шкідливе програмне забезпечення.

– Вішинг: це обманні дії, спрямовані на отримання особистої інформації, такої як банківські реквізити, шляхом мобільних звернень або електронної пошти.

– Контактна соціальна інженерія: це розповсюдження спаму від імені друзів або знайомих з метою отримання доступу до їхніх акаунтів у соціальних мережах [6].

Ці методи соціальної інженерії широко використовуються в політиці, бізнесі та освітній сфері. Найбільш ефективними засобами протидії цим загрозам є освітні та попереджувальні заходи, спрямовані на учнів і студентів щодо ризиків розголошення особистої інформації.

Для боротьби з соціальною інженерією в освітньому середовищі можна застосовувати такі закони:

– Встановлення облікових записів, які належать навчальному закладу.

– Попередження співробітників, учнів та студентів про те, що їхні логіни та паролі не можна ділитися з іншими особами.

– Встановлення вірусного захисту на комп'ютерах користувачів.

– Використання систем запобігання розголошенню особистої інформації.

– Підвищення уважності стосовно запитів на особисту інформацію через телефон або електронну пошту.

Узагальнюючи вище сказане, боротьба з кіберзагрозами в освітньому середовищі вимагає комплексного підходу, що включає технічні, правові та організаційні заходи [7].

---

1. Про основні засади забезпечення кібербезпеки України : Закон України № № 2163-VIII від 05.10.2017 р. Відомості Верховної Ради (ВВР). 2017. № 45. Ст. 403.

2. Кириченко І. О. Чинник м'якої сили у стратегіях національної інформаційної безпеки США //Актуальні проблеми міжнародних відносин. 2011. №. 102 (1). С. 209-218.

3. Бєлєвцева В. В. До питання застосування правових режимів забезпечення кібербезпеки в Україні //Інформація і право. 2020. №. 4 (35). С. 106-112.

4. Чоботько І.І. Як впливає російська пропаганда на мозок людини // Міжнародна науково-практична конференція «Сектор безпеки і оборони України на захисті національних інтересів: актуальні проблеми та завдання в умовах воєнного стану», 24 листопада 2022 року. С. 1042-1043.

5. Чоботько І.І. Роль спеціально фізичної підготовки в діяльності правоохоронця // Міжнародний форум «З проблем фізичного виховання та здоров'я молоді у сучасному освітньому середовищі», 18 травня 2023 р. С. 246-248.

6. Чоботько М.А. Методи покращення тренувань співробітників силових структур // IV Міжнародної науково-практичної конференції «Сучасні тенденції та перспективи розвитку фізичної підготовки та спорту Збройних Сил України, правоохоронних органів, рятувальних та інших спеціальних служб на шляху євроатлантичної інтеграції України», Київ, Національний університет оборони України імені Івана Черняховського, НУОУ, 19 листопада 2020 р., С.263-265.

7. Чоботько І.І. Особливості фізичного виховання здобувачів вищої освіти та способи його вдосконалення у сучасних реаліях // Міжнародний науково-практичний круглий стіл «Службово-бойова підготовка як основа професійної діяльності поліцейських», 30 листопада 2023 р. С. 157-159.