КУДРЯ А.Р.,
слухач магістратури 1 курсу навчально-наукового інституту № 1
КАЛЄНІЧЕНКО, Л.І.,
д.ю.н., професор,
завідувач кафедри інформаційних систем та технологій ННІ 4 ХНУВС,
Харківський національний університет внутрішніх справ

РОЛЬ КІБЕРБЕЗПЕКИ В ІНФОРМАЦІЙНОМУ ПРОСТОРІ

Анотація: Зроблено висновок про те, що забезпечення кібербезпеки є ключовим фактором стабільного розвитку цифрового суспільства та економіки України, побудова ефективної системи кібербезпеки вимагає комплексного підходу, що охоплює технічні, правові та освітні аспекти.

Abstract: It was concluded that ensuring cyber security is a key factor in the stable development of the digital society and economy of Ukraine, building an effective cyber security system requires a comprehensive approach covering technical, legal and educational aspects.

Ключові слова: кіберзагрози, кіберпростір, механізм кібербезпеки.

Keywords: cyber threats, cyber space, cyber security mechanism.

Кібербезпека передбачає захист важливих інтересів громадян, суспільства та держави від загроз у кіберпросторі. Захист кіберпростору, у свою чергу, передбачає перевірку, запобігання та нейтралізацію кіберзагроз, які можуть зруйнувати національну безпеку України. В нашій державі формування механізму кібербезпеки знаходиться на етапі становлення, і цілком логічно, що ефективність його функціонування в умовах стрімкого розвитку цифрових технологій певною мірою залежить від його досконалості, а отже потребує своєчасних науково-обґрунтованих законодавчих змін.

Одним із важливих аспектів кібербезпеки є управління доступом до інформаційних ресурсів. Він забезпечує захист доступу користувачів до електронних послуг, а також моніторинг і контроль їх дій у відповідній системі. Управління доступом включає процедури ідентифікації, автентифікації, авторизації та моніторингу, які дозволяють отримати надійний контроль над доступом до критично важливих даних.

Для забезпечення надійного рівня кібербезпеки України необхідно не лише впроваджувати технічні рішення, але й формувати стратегію розвитку кіберпростору [1].

Особливу увагу у даному контексті, на нашу думку, слід приділити захисту критичної інфраструктури, яка забезпечує життєдіяльність нашої країни. І в умовах дії воєнного стану в Україні потребує додаткового захисту з боку держави. До таких об'єктів належать енергетична система, фінансовий сектор, транспортні мережі, медичні та інші системи, що функціонують на основі цифрових технологій. Критична інфраструктура є вразливою до кіберзагроз, і будь-яке порушення її роботи може призвести до значних збитків для держави та суспільства. А інколи навіть паралізувати роботу певної сфери діяльності суспільства.

Сучасні кіберзагрози спрямовані не лише на злом певної системи, а й на збір і використання особистих даних, що може призвести до негативних наслідків як для приватних осіб, так і для державної безпеки в цілому. Зважаючи на зазначене, на нашу думку, розробка єдиних стандартів зберігання, обробки та захисту персональних даних, а також предбачення їх як обов’язкової складової в механізмі кібербезпеки, є кроком як для формування довіри громадян до електронних послуг, так і кібербезпеки в цілому.

Ще одним засобом механізму кібербезпеки, на наш погляд, є впровадження у кіберпростір технологій, які забезпечують можливість ефективного моніторингу, прогнозування та реагування на кіберзагрози. Наприклад, автоматизовані системи встановлення вторгнень і аномалій у поведінці користувачів можуть допомогти у швидкому виявленні та нейтралізації наявних загроз [2, с.118-121].

Інтеграція України у світовий кіберпростір також забезпечує обмін досвідом і технологіями з іншими країнами, особливо в рамках їх європейських ініціатив. Налагодження міжнародного співробітництва у сфері кібербезпеки, на нашу думку, дозволить отримати доступ до найкращих практик, підвищити рівень захисту національних інформаційних систем та сприяти гармонізації українських стандартів із загальноприйнятими світовими нормами [3, с.145-148].

Таким чином, забезпечення кібербезпеки є ключовим фактором стабільного розвитку цифрового суспільства та економіки України. Побудова ефективної системи кібербезпеки вимагає комплексного підходу, що охоплює технічні, правові та освітні аспекти, спрямовані на формування безпечного інформаційного простору та підвищення рівня захищеності державних, суспільних та приватних даних.

Список використаних джерел:

1. Швець Д. В. Механізми забезпечення кібербезпеки в інформаційному просторі. URL: https://dspace.univd.edu.ua/server/api/core/bitstreams (дата звернення 05.11.2024).
2. Зінченко Д. А. Аналіз ризиків і стратегій захисту від кібератак у сучасному цифровому світі. Протидія кіберзлочинності та торгівлі людьми : зб. матеріалів міжнар. наук.-практ. конф. МВС України. Харків. нац. ун-т внутр. справ, Наук. парк «Наука та безпека». Вінниця : ХНУВС. 2023. С. 118-121.
3. Бережна Є. В. Актуальні питання становлення та розвитку сучасної поліцеїстики (кібербезпека в сучасному безпековому середовищі). Проблеми сучасної поліцеїстики : тези доп. наук.-практ. конф. МВС України, Харків. нац. ун-т внут. справ, Ф-т № 6, Каф. правоох. діяльності та поліціїстики, Наук. парк «Наука та безпека». Харків, 2022. С. 145-148.

КУЛІШ С.П.,
ТКАЧЕНКО О.М.
Вінницький національний технічний університет

ВИЗНАЧЕННЯ ВИМОГ ДЛЯ ПОБУДОВИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ СИСТЕМИ МАРКУВАННЯ АУДІО- ТА ВІДЕОРЯДІВ РЕКЛАМИ В СОЦІАЛЬНИХ МЕРЕЖАХ

Актуальність досліджень та розробки методів побудови програмного забезпечення системи маркування аудіо та відео рядів реклами в соціальних мережах підтверджується активним розвитком соціальних мереж, електронної комерції в такому мережевому середовищі, необхідністю позиціонування та просування брендів за допомогою рекламних компаній. Маркування аудіо та відео рядів реклами передбачає запровадження спеціальних технологій генерації маркерів для визначення об'єктів, процесів, окремих фрагментів, що можуть вплинути на ефективність реклами в соціальних мережах. Створення програмного забезпечення систем маркування з подальшим аналізом і представленням даних реклами, формування автоматичних рекомендацій щодо запровадження змін в рекламі є основою для прийняття рішення щодо удосконалення відео та аудіо реклами для соціальних мереж [1; 2]. Відповідно до міжнародного стандарту SWEBOK [3] першим етапом для побудови програмного забезпечення (ПЗ) є збір даних для визначення вимог до ПЗ. Програмна інженерія за цим стандартом визначається як «застосування систематичного, дисциплінованого, кількісно вимірюваного підходу до розробки, експлуатації та обслуговування програмного забезпечення; тобто, застосування інженерії до програмного забезпечення)". Вимоги до процесів і результатів маркування аудіо та відео рядів реклами в соціальних мережах визначаються за такими напрямами – відповідно до законодавства, потреби замовників (власників) реклами в соціальних мережах та технічні можливості маркування, відповідно до яких можуть змінюватись або/і деталізуватись вимоги замовника.

Загальні вимоги до ПЗ маркування аудіо- та відеореклами полягають в процесах отримання аналітичних даних для прийняття рішення щодо удосконалення та розвитку реклами. Маркування реклами – це процес додавання спеціальних тегів, ключових слів та інших метаданих до відеоролика, щоб зробити його більш помітним для користувачів та пошукових систем. Це важливий крок у процесі просування відеоконтенту, який дозволяє підвищити його релевантність, охоплення аудиторії та ефективність рекламних кампаній. Маркування дозволяє оптимізувати користувацький пошук за допомогою ключових слів, визначити цільові аудиторії, аналізувати поведінку аудиторії. Процеси маркування дозволяють виділяти заголовок, опис, включати теги, визначати категорії, формувати субтитри. Для маркування використовують вбудовані інструменти та правила соціальних мереж, а також спеціальні платформи маркування та аналітики.