можуть неусвідомлено порушити законодавство про приватність, захист даних або інтелектуальну власність, якщо будуть використовувати неавторизовану інформацію з відкритих джерел.

Для забезпечення інформаційної безпеки необхідно, в першу чергу уникати формалізму проходження освітніх програм та тренінгів для посадових осіб щодо інформаційної (кібер) гігієни та захисту персональних даних. Необхідно постійно здійснювати моніторинг та аналіз відкритих джерел на предмет наявності персональних даних або іншої чутливої інформації. Забезпечити запровадження чітких політик і процедур щодо використання відкритих джерел та взаємодії з медіа. Інформаційна безпека посадових осіб при взаємодії з відкритими джерелами є багатогранною проблемою, яка потребує постійного контролю, навчання і технологічної підтримки, щоб мінімізувати ризики для національної і організаційної безпеки.

Список використаних джерел:

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII : станом на 28 черв. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 15.10.2024).

DOI https://doi.org/10.36059/978-966-397-444-6-54

Данькевич Ю. В.,
кандидат філологічних наук, доцент,
доцент кафедри комп'ютерних та інформаційних технологій
Таврійського національного університету імені В. І. Вернадського
м. Київ, Україна

БЕЗПЕКА ПЕРЕДАЧІ СЛУЖБОВОЇ ІНФОРМАЦІЇ В ЕЛЕКТРОННИХ ДОКУМЕНТАХ ПІДПРИЄМСТВ ДЕРЖАВНОЇ ФОРМИ ВЛАСНОСТІ У ВОЄННИЙ ПЕРІОД

Одним із головних завдань безпечного функціонування систем електронного документообігу підприємств державної форми власності у воєнний час є дотримання нормативно-правових вимог, що регулюють передачу конфіденційної та службової інформації. Особливістю конфіденційної інформації є те, що вона має обмежений доступ як для фізичних, так і юридичних осіб. У статті 7 Закону України «Про доступ до публічної інформації» (далі – Закон) обґрунтовано, хто є «суб'єктами владних повноважень», та як саме конфіденційна інформація

«може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов» [2]. Ця ж стаття Закону визначає, що конфіденційною не є інформація між «суб'єктами владних повноважень при здійсненні ними своїх функцій, а також на відносини у сфері звернень громадян, які регулюються спеціальним законом» [2].

У свою чергу, службова інформація у статті 9 Закону розуміється як така, що «міститься в документах суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень». До службової інформації належить і та, що була «зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці» [2]. Документам, що містять службову інформацію «присвоюється гриф "для службового користування"» [2]. Подальший доступ до таких документів надається відповідно до умов, визначених статтею 6 Закону.

Особливого посилення захисту на сьогодні потребує службова інформація, вміщена у документах, які функціонують на рівні державних підприємств. За офіційною статистикою, поданою Державною службою спеціального зв'язку та захисту інформації України, з лютого 2022 року кількість кібератак на державні інформаційні системи та об'єкти критичної інформаційної інфраструктури зросла втричі. 90% атак здійснювали військові хакери з росії та білорусі, діяльність яких фінансувалася владою. Основна мета російських хакерів зосереджена на атаках на цивільну інфраструктуру з метою завдання шкоди через різноманітні засоби (ракетні та кібератаки) [3]. Важливо наголосити, що під час воєнного стану «вимоги щодо захисту інформації в інформаційно-комунікаційних системах не змінюються». Вимоги визначені у Наказі № 93 «Про затвердження Положення про державну експертизу у сфері технічного захисту інформації» [4].

За офіційними джерелами, «російські військові хакери намагаються отримати доступ до персональних даних українців, а також завдати шкоди українським інформаційним системам. Ці атаки координуються з атаками на критичну інфраструктуру і є частиною воєнної агресії рф» [3]. Зрозуміло, що витік чутливих даних (наприклад, персональних) загрожує роботі органів влади та критичної інфраструктури, якщо він буде використаний ворогом для подальших атак. Через це, на державних підприємствах посилені технічні та організаційні заходи захисту у вигляді технічних (програмно-апаратних та програмних) засобів, налаштувань, так у вигляді розпоряджень, планів, інструкцій, методик тощо. Для захисту інформаційних систем, в яких не обробляється

інформація з обмеженим доступом, але захист яких вимагає українське законодавство, може бути також використана альтернативна система інформаційної безпеки відповідно до європейських стандартів ISO/IEC 27 серії [3].

Система захисту службової інформації на підприємстві повинна врахувати три необхідні складові: юридичні, організаційно-економічні й технологічні. Розробкою заходів у кожній із трьох груп займаються відповідні фахівці, які застосовують свої способи і методи для досягнення заданих цілей, що враховують: аналіз і узагальнення потенційних загроз і таких, що реалізувалися, причин порушень вимог інформаційної безпеки. Аналіз ступеня забезпечення безперервності бізнес-процесів, що використовують ІТ, з точки зору інформаційної безпеки. Пошук нових загроз і вразливостей, пов'язаних з інформаційною взаємодією. Побудова методик оцінки інформаційних ризиків. Інформаційне обстеження підприємства та інформаційних ресурсів, розробка методів захисту інформації та ІТ і методик їх упровадження в діяльність підприємства. Заходи посилення повинні включати й розробку та модифікацію концепції і політики забезпечення інформаційної безпеки. Створення локальної нормативної бази із цих питань з урахуванням комплексного підходу до економічної безпеки [1].

Отже, за останніми опублікованими даними, фахівцями Держспецзв'язку України було впроваджено CSET (Cybersecurity Evaluation Tool). CSET було перекладено українською мовою та адаптовано до потреб українських організацій у межах Меморандуму про співробітництво між Держспецзв'язком та Агентством з кібербезпеки та безпеки інфраструктури Сполучених Штатів (CISA) [1].

Список використаних джерел:

1. Вимоги до захисту інформації в інформаційних системах у воєнний час: роз'яснення Держспецзв'язку. Державна служба спеціального зв'язку та захисту інформації України від 19.07.2022. URL: https://cip.gov.ua/ua/news/vimogi-do-zakhistu-informaciyi-v-informaciinikh-sistemakh-u-voyennii-chas-roz-yasnennya-derzhspeczv-yazku (дата звернення: 02.10.2024).

2. Закон України «Про доступ до публічної інформації» станом на 08.10.2023, документ 2939-V. URL: https://zakon.rada.gov.ua/laws/show/2939-17?find=1&text=%D1%81%D0%BB%D1%83%D0%B6%D0%B1%D0%BE%D0%B2%D0%B0+%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%8F#w1_1 (дата звернення: 01.10.2024).

3. Зміцнюємо цифровий захист: Держспецзв'язку презентувала інструмент оцінки кібербезпеки. Державна служба спеціального зв'язку та захисту інформації України від 30.09.2024. URL: https://cip.gov.ua/ua/

news/zmicnyuyemo-cifrovii-zakhist-derzhspeczv-yazku-prezentuvala-instrument-ocinki-kiberbezpeki (дата звернення: 03.10.2024)
4. Наказ № 93 «Про затвердження Положення про державну експертизу у сфері технічного захисту інформації» станом на 11.10.2022, документ z0820-07. URL: https://zakon.rada.gov.ua/laws/show/z0820-07#Text

DOI https://doi.org/10.36059/978-966-397-444-6-55

Деркач В. В.,
студентка ІІ курсу магістратури ОП «061 Журналістика»
Таврійського національного університету імені В. І. Вернадського
Науковий керівник: **Досенко А. К.,**
кандидат наук із соціальних комунікацій, доцент,
завідувач кафедри журналістики
Таврійського національного університету імені В. І. Вернадського
м. Київ, Україна

ФЕЙКОВІ НОВИНИ: МЕДІАГРАМОТНІСТЬ ТА БЕЗПЕЧНІСТЬ ЗМІ

Якщо брехня повторена більше тисячі разів,
вона стане правдою.
Й. Геббельс

Сотні років війн, конфліктів, міждержавних зіткнень змінили стан справ, погляди, організації, позиції світової спільноти. Науково-технічний прогрес, який не припиняється ні на мить, є характерною рисою як сучасності, так і тих відносно далеких часів. Це явище супроводжується бурхливим розвитком як інформаційних технологій, які використовуються в повсякденному житті, так і технічних відкриттів на міжнародному рівні, зокрема, у зовнішній політиці.

Комплексне вивчення такого чинника як фейк дає безцінний досвід, який може бути використаний і потрібний не тільки в наукових колах, а й в інших, більш практичних сферах – наприклад, спеціалістам із сучасної зовнішньої політики для впровадження антифейків у обіг та глобальної протидії інформаційним загрозам. Розгляд феномену фейку в сучасній літературі дозволить краще зрозуміти його анатомію та прослідкувати всі негативні чинники, до яких це явище призводить Україну та світ. Саме тому питання поширення фейкових новин у контексті медіаграмотності, а особливо медіабезпеки, є значущим