number of neurons is set with a certain margin. "Superfluous" neurons, whose weights will change chaotically during the learning process, can be removed at the end of this process.

Literature

1. Semenov, S. ., Liqiang, Z., Weiling, C., & Davydov, V. (2021). Development a mathematical model for the software security testing first stage. Eastern-European Journal of Enterprise Technologies, 3(2 (111), 24–34. https://doi.org/10.15587/1729-4061.2021.233417.

2. Zongyuan Zhao, Shuxiang Xu, Byeong Ho Kang, Mir Md Jahangir Kabir, Yunling Liu, Rainer Wasinger, Investigation and improvement of multi-layer perceptron neural networks for credit scoring, Expert Systems with Applications, Volume 42, Issue 7, 2015, Pages 3508-3516, ISSN 0957-4174, https://doi.org/10.1016/j.eswa.2014.12.006.

3. . W. Zaki et al., "A Novel Sigmoid Function Approximation Suitable for Neural Networks on FPGA," 2019 15th International Computer Engineering Conference (ICENCO), 2019, pp. 95-99, doi: 10.1109/ICENCO48310.2019.9027479.

4. Kleyko D., Rosato A., Paxon F. E., Panella M., Sommer F. T. Perceptron Theory for Predicting the Accuracy of Neural Networks https://arxiv.org/pdf/2012.07881.pdf.

Одержано 14.04.2022

УДК 65.012.8+004

МАНЖАЙ Олександр Володимирович,
кандидат юридичних наук, доцент,
завідувач кафедри протидії кіберзлочинності факультету № 4
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0001-5435-5921
МАНЖАЙ Ірина Андріївна,
завідувач навчального відділу Харківського університету

СУЧАСНІ ТЕНДЕНЦІЇ У ВІТЧИЗНЯНОМУ СЕКТОРІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЇ

У новому українському законодавстві на теперішній час формується розуміння термінології у сфері безпеки інформації, яке дещо відрізняється від класичного. Серед іншого це пов’язано з низкою серйозних викликів в інформаційному просторі держави, які посилилися у 2014 році і тривають донині. Водночас, залишені старі нормативні документи, продовжуючи класичні традиції формування безпеки інформації, можуть утворювати деяку плутанину та неузгодженість. Серед іншого це стосується таких категорій як «інформаційна безпека» та «кібербезпека».

Ще не так давно термін «інформаційна безпека» був узагальнюючим до тієї ж «кібербезпеки» та/або «захисту інформації». Саме такий стан речей випливає із все ще чинного Закону України, яким визначено основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки. Зокрема у п. 13 розділу ІІІ цього закону зазначено, що під ***інформаційною безпекою*** розуміється стан захищеності життєво важливих інтересів людини, суспільства і держави, за якого запобігається нанесення шкоди через: неповноту, невчасність і невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.

Водночас прийняття нової Доктрини інформаційної безпеки засвідчило, що у вищих органах державної влади інформаційна безпека асоціюється радше з протидією дезінформації, забезпеченням безпеки інформаційного простору, як середовища впливу на світосприйняття людини, але аж ніяк не з кібербезпекою чи технічним захистом інформації.

У розумінні значення «кібербезпеки» також досі не простежується єдиного підходу. Так, у 2015 році запровадження нової спеціальності 125 «Кібербезпека» розпочало процес об’єднання дещо різних за змістом напрямів підготовки: «Системи технічного захисту інфор-

мації», «Безпека інформаційних та комунікаційних систем», «Управління інформаційною безпекою». Водночас на законодавчому рівні кібербезпека стосується переважно безпеки у кіберпросторі та аж ніяк не охоплює технічний захист інформації фізичних об'єктів. Отже, питання змісту термінології у сфері безпеки інформації наразі лишається відкритим.

Паралельно зі зміною підходів до розуміння термінологічного апарату у сфері безпеки в Україні простежується новий підхід до побудови системи безпеки на об'єктах інформаційної діяльності. Так, у 2020 р. на законодавчому рівні було запроваджено альтернативу досі монопольній комплексній системі захисту інформації (КСЗІ), а саме унормовано порядок впровадження системи управління інформаційною безпекою (СУІБ).

Відповідно до ч. 4 ст. 8 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 державні інформаційні ресурси та інформація з обмеженим доступом, крім державної таємниці, службової інформації та державних і єдиних реєстрів, створення та забезпечення функціонування яких визначено законами, можуть оброблятися в системі ***без*** *застосування комплексної системи захисту інформації* у разі виконання **всіх** таких умов:

– підтвердження відповідності *системи управління інформаційною безпекою* за результатами процедури з оцінки відповідності національним стандартам України щодо систем управління інформаційною безпекою, яка проведена *органом з оцінки відповідності*, акредитованим національним органом України з акредитації чи національним органом з акредитації іншої держави, якщо і національний орган України з акредитації, і національний орган з акредитації такої держави є членами міжнародної або регіональної організації з акредитації та/або уклали з такою організацією угоду про взаємне визнання щодо оцінки відповідності;

– використання для захисту інформації в системі *засобів криптографічного захисту інформації, які мають позитивний експертний висновок* за результатами державної експертизи у сфері криптографічного захисту інформації;

– жоден з елементів системи не може бути *розташований на територіях* України, на яких органи державної влади України тимчасово не здійснюють своїх повноважень, на територіях держав, визнаних Верховною Радою України державами-агресорами, на територіях держав, щодо яких застосовані санкції відповідно до Закону України «Про санкції», та на територіях держав, які входять до митних союзів з такими державами;

– *виконання особливих вимог*, встановлених Кабінетом Міністрів України до забезпечення захисту інформації в системах залежно від категорії державних інформаційних ресурсів або інформації з обмеженим доступом (вимога щодо захисту якої встановлена законом, що обробляються.

Етапи побудови СУІБ дещо відрізняються від аналогічного процесу щодо КСЗІ. У загальному вигляді їх можна представити так:

– *визначення сфери дії* СУІБ;

– *попередня перевірка відповідності* системи безпеки організації вимогам стандарту ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги. На цьому етапі можуть бути застосовані й інші стандарти, у тому числі ДСТУ ISO/IEC 27004:2018 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Моніторинг, вимірювання, аналізування та оцінювання;

– *оцінка ризиків*, де основою для вибору відповідної методики є стандарт ДСТУ ISO/IEC 27005:2019 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки;

– *опис процедур та їх документування*. На цьому етапі описуються процеси у сфері управління та забезпечення безпеки, які потрібно виконати, а також формується відповідна документація;

– *впровадження процедур та відповідної документації*;

– *дослідна експлуатація* СУІБ;

– *сертифікація*, яка проводиться у формі аудиту, за результатами якого організація має отримати сертифікат про відповідність СУІБ вимогам ДСТУ ISO/IEC 27001:2015.

Отже, нормативно-правова база кібернетичної та інформаційної безпеки на теперішній час перебуває в процесі становлення. Для убезпечення державних ресурсів в інформаційних системах можуть бути створені або комплексна система захисту інформації, або система управління інформаційною безпекою. Вимоги до обох видів систем та порядок їх побудови є недостатньо визначеними на законодавчому рівні та потребують удосконалення. СУІБ є певною альтернативою КСЗІ, її запровадження обумовлене тенденціями у світових процесах з безпеки. Проте в Україні СУІБ є досить новим механізмом і на законодавчому рівні унормований лише в червні 2020 року.

Одержано 07.04.2022

УДК 65.012.8+004
МОГІЛЕВСЬКИЙ Леонід Володимирович,
доктор юридичних наук, професор,
заслужений юрист України,
проректор Харківського національного університету внутрішніх справ
https://orcid.org/0000-0002-6994-6086

ІНСТРУМЕНТИ ВИЯВЛЕННЯ НЕПРАВДИВИХ ПОВІДОМЛЕНЬ

Для перевірки повідомлень та інших матеріалів на предмет їх актуальності та достовірності можуть бути використані різні аналітичні методи. Для полегшення цього процесу також варто застосовувати і низку технічних рішень. Серед подібних інструментів можна виділити розширення Fake Profile Detector (Deepfake, GAN) – інструмент, який працює у браузерах на базі Chrome або Chromium і дає змогу ідентифікувати заображення, створені з використанням штучного інтелекту (рис. 1). Саме тому, якщо обличчя реальної людини додано до іншого зображення, воно теж визначатиметься як справжнє. Розширення доступне за посиланням https: //chrome.google.com/webstore/detail/fake-profile-detectordee/jbpcgcnnhmjmajjkgdaogpgefbnokpcc/related?hl=en-US.

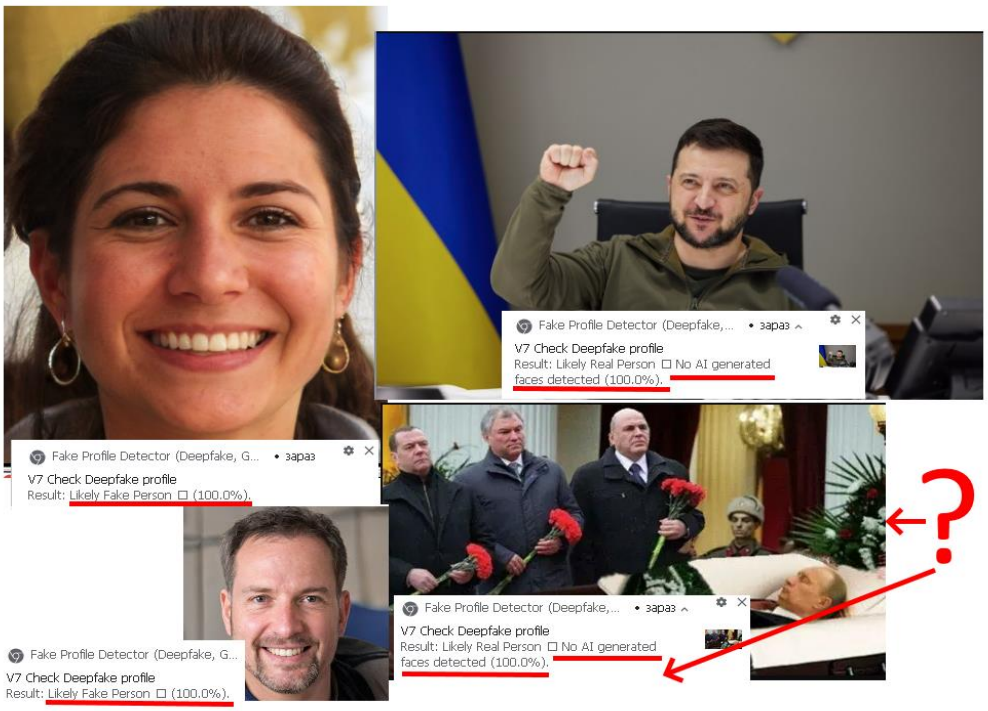

Рис. 1. Результат роботи розширення з виявлення діпфейків