3. Документно-інформаційні комунікації в умовах глобалізації: стан, проблеми та перспективи: матеріали VII Міжнар. наук.-практ. конф., 24 листоп. 2022 р. / редкол.: І.Г. Передерій [та ін.]. Полтава, 2022. 295 с.

4. ДСТУ 4163:2020. Уніфікована система організаційно-розпорядчої документації. Вимоги до оформлення документів. [Чинний від 01-09-2021]. Вид. офіц. Київ: ДП «УкрНДНЦ», 2020. 37 с.

УДК [35:004]:004.056.5(043.2)

Сергій ГОРЄВ
Національний авіаційний університет, Київ

ІНФОРМАЦІЙНА БЕЗПЕКА В СИСТЕМІ ЕЛЕКТРОННОГО УРЯДУВАННЯ: СУТНІСТЬ, ЗАГРОЗИ, ЗАСОБИ ЗАБЕЗПЕЧЕННЯ

Інформаційна безпека в системі електронного урядування є важливим аспектом забезпечення безпеки держави та її громадян. Інформаційну безпеку визначають як стан захищеності інформації від несанкціонованого доступу, використання, розголошення, модифікації або знищення. У свою чергу, електронне урядування є формою організації державного управління, яка використовує інформаційно-телекомунікаційні технології (ІКТ) зокрема для надання державних послуг громадянам та бізнесу. До головних цілей забезпечення інформаційної безпеки в системі електронного урядування в Україні належать: захист конфіденційності інформації, яка використовується або створюється в процесі надання державних послуг; захист доступності інформації для авторизованих користувачів; захист цілісності інформації від змін, які можуть призвести до втрати, перекручення або спотворення її значення. Відповідно, у контексті електронного урядування інформаційну безпеку можна визначити як стан захищеності інформаційних систем і мереж, що використовуються для надання державних послуг, від несанкціонованого доступу, використання, розголошення, модифікації або знищення, а також від інших дій, які можуть призвести до втрати, перекручення або спотворення інформації [1, с. 44].

Відповідно до Концепції розвитку електронного урядування в Україні, серед іншого, управління розвитком електронного урядування передбачає захист телекомунікаційних систем, зокрема, «мережі передачі даних, у тому числі національної системи конфіденційного зв'язку»; захист електронної пошти, центрів обробки даних; безпечне

функціонування кіберпростору; «забезпечення захисту інформації в державних електронних інформаційних ресурсах»; «надійний захист персональних даних та прав на приватність особи з метою зміцнення довіри до он-лайн середовища» [3].

Основні загрози інформаційній безпеці складаються з поєднання умов і факторів, що створюють небезпеку життєво важливим інтересам особистості, суспільства й держави в інформаційній сфері. Виокремлюють три групи зазначених загроз. Першу групу становлять загрози впливу на особистість, суспільство, державу неякісної інформації (недостовірної, фальшивої, дезінформації). Друга група пов'язана з низкою загроз несанкціонованого та неправомірного впливу сторонніх осіб на інформацію, інформаційні ресурси та інформаційні системи (їх виробництво, використання). Третя група об'єднує загрози інформаційним правам і свободам особистості, до яких належать право на виробництво, поширення, пошук, одержання, передавання та використання інформації; право на інтелектуальну власність на інформацію [2, с. 333]. До загроз інформаційній безпеці у інформаційній сфері також відносять «викрадення інформації, відомостей, які становлять таємницю, що охороняється законом; знищення інформації, програмних засобів, які забезпечують опрацювання даних або функціонування технічних засобів і систем; неправомірне «перехоплення» інформації; модифікація інформації, програмних засобів; неправомірне використання інформації, програмних засобів порушення функціонування або виведення з ладу комп'ютерів і мереж; приховування (неповідомлення) інформації, яка торкається інтересів людини, громадянина, суспільства; збирання, накопичення і використання даних про особу та інші дії, які порушують основні права людини і громадянина [2, с. 333–334]. Поширений спосіб викрадення персональних даних пов'язаний з перехопленням інформації з комп'ютера службової особи за допомогою атаки «men-in-the-middle». Наслідком такої атаки є перенаправлення зловмиснику інформації з Wi-Fi роутера службовця перед тим, як вона потрапить до вірного адресата. Таким чином відбувається викрадення особистих даних, логінів та паролів [4].

На думку Н. І. Логінової, несанкціонований доступ до інформаційних ресурсів сьогодні здобув найбільше поширення серед інших видів інформаційних загроз. Суть несанкціонованого доступу полягає в тому, що користувач, який не має дозволу відповідно до політики безпеки, отримує доступ до того чи іншого об'єкта. На запобігання такій загрозі в системах електронного урядування має використовуватись ідентифікація

та аутентифікація. Національна програма «Держава в телефоні» містить одним з своїх ключових елементів систему цифрової ідентифікації громадян. Відсутність єдиної системи цифрової ідентифікації в Україні здійснює негативний вплив на розвиток електронного урядування [5, с. 51].

Для забезпечення інформаційної безпеки в системі електронного урядування необхідно використовувати комплексний підхід, який включає технічні, організаційні та правові заходи.

Важливим елементом інформаційної безпеки в системі електронного урядування є нормативно-правове забезпечення. До нормативно-правових документів, що створюють умови для реалізації державної політики в сфері протидії внутрішнім та зовнішнім загрозам інформаційній безпеці, зокрема й в процесі здійснення електронного урядування, належать Закони України «Про інформацію», «Про захист інформації в інформаційно-теле-комунікаційних системах»; Стратегія національної безпеки України, Стратегія кібербезпеки України та Стратегія інформаційної безпеки України до 2025 року, затверджені Указами Президента України відповідно від 14 вересня 2020 р., 26 серпня 2021 р. та 28 грудня 2021 р.

Підходи і засоби забезпечення інформаційної безпеки в електронному урядуванні, зокрема, під час надання громадянам електронних послуг, передбачають створення відкритого, «прозорого», інформаційного середовища; використання віртуалізації і хмарних обчислень, забезпечення виконання особливих вимог до ідентифікації і автентифікації; інтеграцію різних інформаційних систем, різних технологій інформаційної безпеки під час вирішення завдань; широке використанням мобільних інформаційно-комунікаційних технологій; взяття до уваги як необхідності забезпечення інформаційної безпеки системи, так і інформаційної безпеки кінцевого користувача; збільшення питомої ваги персональних даних в інформаційному просторі. З цією метою була запропонована концепція безпеки, що отримала назву «інформаційне середовище на основі резидентних компонентів безпеки». Вона базується на винесенні ключових операцій із забезпечення безпеки в ізольоване апаратне середовище, що дозволяє, не порушуючи цілісності засобу захисту інформації, перевірити її і прошивки управління. Такий засіб отримав назву «резидентний компонент безпеки» [4, с. 85]. З метою забезпечення інформаційної безпеки в електронному урядуванні використовується й резервне копіювання даних. Також до засобів безпеки можна віднести розвиток цифрової грамотності громадян, спрямованої на дотримання ними правил безпеки в системі електронного

урядування. Вони передбачають, зокрема, застосування двофакторної автентифікації під час кожної реєстрації; використання біометричних даних для активації пристроїв і застосунків; використання складних комбінацій для створення паролів, їх регулярне оновлення та використання різних паролів для різних сервісів і застосунків; використання електронного цифрового підпису [4, с. 87].

Отже, інформаційна безпека в електронному урядуванні розуміється як стан захищеності інформаційних систем і мереж, що використовуються для надання державних послуг, від несанкціонованого доступу, використання, розголошення, модифікації або знищення, а також від інших дій, які можуть призвести до втрати, перекручення або спотворення інформації. До основних загроз в системі електронного урядування належать загрози впливу на особистість, суспільство, державу неякісної інформації; загрози несанкціонованого та неправомірного впливу сторонніх осіб на інформацію, інформаційні ресурси та інформаційні системи; загрози інформаційним правам і свободам особистості. Виявлення та запобігання цим загрозам є надзвичайно важливим завданням, вирішення якого вимагає використання комплексного підходу, що поєднує правові, організаційні і технічні заходи.

Список літератури

1. Гайдученко С. О. Електронне урядування : конспект лекцій для студентів усіх форм навчання спеціальності 281 – Публічне управління та адміністрування / С. О. Гайдученко ; Харків. нац. ун-т міськ. госп-ва ім. О. М. Бекетова. Харків : ХНУМГ ім. О. М. Бекетова, 2019. 54 с. URL: http://surl.li/qrzsm (дата звернення: 17.02.2024).

2. Конопліцька О. І. Інформаційна безпека у системі електронного урядування. *Україна в умовах реформування правової системи : сучасні реалії та міжнародний досвід* : матеріали ІІ Міжнар. наук.-практ. конф. Тернопіль : Економічна думка, 2017. С. 333–335. URL: http://dspace.wunu.edu.ua/bitstream/316497/21451/1/333-335.pdf (дата звернення: 17.02.2024).

3. Концепція розвитку електронного урядування в Україні : Розпорядження Кабінету Міністрів України від 20 вересня 2017 р. № 649-р. База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/649-2017-р#Text (дата звернення: 16.11.2023).

4. Кузь Т. Нормативно-правове забезпечення інформаційної безпеки в процесі організації та надання адміністративних послуг в Україні. URL:

http://confuf.wunu.edu.ua/index.php/confuf/article/view/858/847 (дата звернення: 17.02.2024).

5. Логінова Н. І. Інформаційна безпека в електронному урядуванні. *Кібербезпека в сучасному світі* : матеріали ІІ Всеукраїнської науково-практичної конференції (м. Одеса, 20 листопада 2020 р.) / за ред. О. В. Дикого ; уклад.: Н. І. Логінова, В. Д. Бойко, М. О. Флюнт. Одеса : Видавничий дім «Гельветика», 2020. С. 50–53. URL: https://dspace.onua.edu.ua/server/api/core/bitstreams/66b22a51-80ff-434e-8ac9-98c08a20f68f/content (дата звернення:17.02.2024).

Науковий керівник: Леся ХАЛЕЦЬКА,
канд. іст. наук, доцент

УДК 316.77(043.2)

Дарина ГРУЗИНСЬКА
Національний авіаційний університет, Україна

ДОКУМЕНТНА ІНФОРМАЦІЯ У СИСТЕМІ СОЦІАЛЬНОЇ КОМУНІКАЦІЇ

У сучасному світі, який вражає своєю швидкістю і обсягом інформації, роль документної інформації у системі соціальної комунікації стає надзвичайно важливою. Документи виступають не лише як засіб фіксації подій і фактів, а й як засіб передачі цієї інформації між людьми, групами, спільнотами. У процесі тривалого історичного розвитку соціуму, сформувалися різні форми соціокомунікативної діяльності індивідів, найбільш ефективними із яких стала комунікація, опосередкована документами. Документи можуть приймати різні форми, такі як текстові документи, фотографії, відеозаписи, аудіозаписи тощо. Кожен з цих форматів має свої унікальні особливості щодо збереження та передачі інформації. По-перше, текстові документи є одним із найпоширеніших і ефективних засобів передачі інформації, вони можуть бути використані для створення документів різних видів, таких як електронні листи, наукові статті, літературні твори, різноманітна службова документація тощо. Проте текстові документи мають свої обмеження. Вони не завжди здатні передати емоційний стан співрозмовників або візуальні аспекти комунікації. Також текст може бути сприйнятий по-різному різними людьми, що може призвести до непорозумінь або спотворення змісту, тому у таких випадках, фотографії або відеозаписи можуть виявитися більш ефективними засобами