DOI https://doi.org/10.30525/978-9934-26-277-7-9

PROTECTION OF THE INFORMATION IN INFORMATION AND COMMUNICATION SYSTEMS IN UKRAINE

ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАТИВНИХ СИСТЕМАХ В УКРАЇНІ

Almashi I. M.
Candidate of Law Sciences, Associate Professor of the Department of Accounting and Taxation Uzhhorod Institute of Trade and Economics State University of Trade and Economics Uzhhorod, Ukraine

Алмаші І. М.
кандидат юридичних наук, доцент кафедри обліку та оподаткування Ужгородського торговельно-економічного інституту Державного торговельно-економічного університету м. Ужгород, Україна

Almashi M. M.
Candidate of Law Sciences, Associate Professor of the Department of Constitutional Law and Comparative Law Uzhhorod National University Uzhhorod, Ukraine

Алмаші М. М.
кандидат юридичних наук, доцент кафедри конституційного права та порівняльного правознавства ДВНЗ «Ужгородський національний університет» м. Ужгород, Україна

В умовах глобалізації суспільних відносин, інтеграції України до міжнародних стандартів у забезпеченні та захисті прав людини та громадянина, в тому числі права на отримання належної освіти, розвитку науки, запровадженні нових інформаційних технологій набуває важливого значення захист інформації при використанні інформаційних технологій та запровадженні нових.

На сьогоднішній день в України прийнято ряд законодавчих актів, які спрямовані на захист інформації та інформаційних технологій запроваджених як в науці та освіті, так і на увесь інформаційний простір України.

Згідно ст. 1 п. 2 Закону України «Про інформацію» захист інформації – сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї; 4. Право на інформацію, створену в процесі діяльності фізичної чи юридичної особи, суб'єкта владних повноважень або за рахунок фізичної чи

юридичної особи, Державного бюджету України, місцевого бюджету, охороняється в порядку, визначеному законом.

Цим Законом передбачено, що порушення законодавства України про інформацію тягне за собою дисциплінарну, цивільно-правову, адміністративну або кримінальну відповідальність згідно із законами України. Інформація не може бути використана для закликів до повалення конституційного ладу, порушення територіальної цілісності України, пропаганди війни, насильства, жорстокості, розпалювання міжетнічної, расової, релігійної ворожнечі, вчинення терористичних актів, посягання на права і свободи людини [1].

Згідно Закону України «Про захист інформації в інформаційно-комунікативних системах» володілець інформації – фізична або юридична особа, якій належать права на інформацію; виток інформації – результат дій, внаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї. Відповідальність за забезпечення захисту інформації в системі покладається на власника системи.

Власник системи, в якій обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, утворює службу захисту інформації або призначає осіб, на яких покладається забезпечення захисту інформації та контролю за ним [2].

Питання захисту інформації у зв'язку з неперервними процесами ускладнення суспільних відносин потребує постійного перегляду та вдосконалення. Так, Законом України «Про внесення змін да Закону України «Про захист інформації в інформаційно-комунікативних системах» передбачено способи підтвердження відповідності інформаційної системи вимогам щодо захисту інформації шляхом встановлення відповідних критеріїв.

У пояснювальній записці до вищевказаного документу зазначено, що основною метою прийняття даного закону є інтеграція європейських вимог і критеріїв оцінки захисту інформації від кіберзагроз з української законодавчою системою захисту даних. Стандарти, які регламентують питання захисту даних та кібербез-пеки – системи управління інформаційною безпекою, СУІБ (Information Security Management System, ISMS). Закон торкнувся основних тем захисту і обміну інформацією, зокрема, криптографічного захисту інформації. Законом були встановлені основні пункти та вимоги розміщення, зберігання основних інформаційних ресурсів, їх захист і інші нормативні вимоги, як загальні, так і галузеві.

Прийняття даного закону, безперечно, стало важливим кроком вперед для вдосконалення інформаційної безпеки в Україні. Впровадження міжнародних стандартів, європейських СУІБ забезпечать єдині вимоги з кібербезпеки для компаній будь-яких розмірів, завдяки єдиній незалежній базі стандартів. Також це, однозначно, полегшить порядок підтвердження відповідності систем вимогам інформаційної безпеки, а також публічні закупівлі в держорганах і організаціях, де захист інформації забезпечується законодавством [3].

Сьогодні в світі актуальним питанням є проблема захисту інформації та інформаційного простору. Її розглядають не тільки на рівні однієї країни, але і на самітах глобальних співтовариств та організацій, таких як НАТО, ЄС [4, с. 128].

На особливої уваги потребує захист персональних даних при застосуванні інформаційних технологій у освіті і науці. Згідно ст. 24 Закону «Про захист персональних даних» забезпечення захисту персональних даних здійснюється володільцями, розпорядниками персональних даних та третіми особами, зобов'язані забезпечити захист цих даних від випадкових втрати або знищення, від незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних. В органах державної влади, органах місцевого самоврядування, а також у володільцях чи розпорядниках персональних даних, що здійснюють обробку персональних даних, яка підлягає повідомленню відповідно до цього Закону, створюється (визначається) структурний підрозділ або відповідальна особа, що організовує роботу, пов'язану із захистом персональних даних при їх обробці [5].

Слід зазначити, що персональна інформація, в Сполучених Штатах розглядається відповідно до концепції «privacy». Ця концепція реалізується через Стандарт CSA, який було прийнято у 1996 році. Цей нормативно-правовий документ використовується в Америці головним чином тому, що поширюється на всі країни-члени НАТО. Стандарт CSA містить наступні принципи регулювання суспільних відносин, що виникають з приводу персональних даних: 1. Відповідальність. Організація відповідальна за ті персональні дані, що знаходяться під її контролем, і має призначати особу або осіб, які відповідають за відповідність дій організації принципам законодавства. 2. Ідентифікація мети. Мета, задля якої збирається інформація, має бути ідентифікована організацією до початку процесу збирання інформації. 3. Згода. Усвідомлення та згода особи на збирання інформації про неї

є обов'язковою умовою збирання, використання чи поширення (розкриття) персональних даних, крім випадків, де це недоречно. 4. Обмежене збирання [6].

Сьогодні в Україні, в умовах воєнного стану захист інформації є критично необхідним. У зв'язку з цим прийнято Стратегію інформаційної безпеки на строк до 2025 року, яка затверджена Указом Президента України від 15 жовтня 2021 року.

Метою Стратегії є посилення спроможностей щодо забезпечення інформаційної безпеки держави, забезпечення прав та свобод кожного громадянина. Інформаційна безпека України – складова частина національної безпеки України, стан захищеності державного суверенітету, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації. Вказана Стратегія передбачає стратегічні цілі, серед яких: забезпечення дотримання прав особи на збирання, зберігання, використання та поширення інформації, свободу вираження своїх поглядів і переконань, захист приватного життя, доступ до об'єктивної та достовірної інформації; розвиток інформаційного суспільства та підвищення рівня культури діалогу [7].

Отже, у даній доповіді проаналізовано захист інформації в інформаційно-комунікативних системах, досліджено правовий аспект обраної проблематики, звернуто увагу на проблемі захисту інформації в Україні під час воєнного стану та на необхідності подальшого вдосконалення законодавства у цій сфері.

Література:

1. Про інформацію. Закон України. *Відомості Верховної Ради України.* 1992. № 48. Ст. 650.

2. Про захист інформації в інформаційно-комунікаційних системах. Закон України від 05.07.1994 р. *Відомості Верховної Ради України.* 1994. № 31. Ст. 286.

3. Європейські стандарти захисту інформації в Україні. URL: https://nt.ua/blog/isms

4. Маслак В. І. Законодавство провідних країн світу в сфері захисту інформації. *Вісник КДУ імені Михайла Остроградського.* Вип. 2/2010(61). Ч. 1. С.128–131.

5. Про захист персональних даних. Закон України від 01.06.2010 року**.** *Відомості Верховної Ради України.* 2010. № 34. Ст. 481.

6. Климчук С. Загальна характеристика законодавства про інформаційну безпеку ЄС, США та Канади. *Юстініан*. 2006. № 11. URL: http://www.justinian.com.ua/article.php?id=2462

7. Про Стратегію інформаційної безпеки. Указ Президента України «Про рішення Ради національної безпеки і оборони України» від 15 жовтня 2021 року № 685/2021. *Офіційний вісник Президента України.* 2022. № 1. Ст. 31.

DOI https://doi.org/10.30525/978-9934-26-277-7-10

MULTILEVEL INFORMATION SYSTEM FOR RECORDING THE STUDENTS ACADEMIC PERFORMANCE

Aloshyn S.
Senior Lecturer of Computer Science Department
SHEI «Pryazovskyi State Technical University»
Dnipro, Ukraine

Piatykop O.
PhD, Docent,
Associate Professor of Computer Science Department
SHEI «Pryazovskyi State Technical University»
Dnipro, Ukraine

Fedosova I.
Doctor of Pedagogical Sciences, Professor,
Professor of Computer Science Department
SHEI «Pryazovskyi State Technical University»
Dnipro, Ukraine

Management of organizational and educational processes in a higher educational institution is a complex and important task. First in the conditions of the pandemic, and now in the conditions of martial law Universities of Ukraine were forced to switch to distance learning. In this state, the subjects of the educational process (students and teachers) are forced to use systems and distance learning, auxiliary means of video communication and conferences. One of the problems was the task of forming progress journals based on current assessments, preparing intermediate indicators of success and carrying out attestations.