Міністерство освіти і науки України
Національний університет
«Полтавська політехніка імені Юрія Кондратюка»
Університет Ауреля Влайку (Румунія)
Центральна бібліотека Болгарської академії наук (Болгарія)
Коледж Санта-Фе (США)
Державний університет Сан-Паулу(Бразилія)
Університет Метрополітен Лондон (Великобританія)
Західноукраїнський національний університет (Тернопіль)
Державний архів Полтавської області
Центральна бібліотека Полтавської міської територіальної громади

Документно-інформаційні комунікації в умовах глобалізації: стан, проблеми і перспективи

МАТЕРІАЛИ
VIII МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

23 листопада 2023 року

Полтава

необхідності дотримуватися правил кібергігієни. Україна вже кілька років поспіль підтримує цю ініціативу.

Отже, інформаційна агресія, яка є складовою воєнних дій росії проти України, містить значну загрозу, оскільки спрямована на дестабілізацію суспільства. Тому громадянам України слід бути готовими до інформаційного спротиву та забезпечення захисту від ворожої агресії, аби перемогти в боротьбі за свої цінності та власне майбутнє.

Джерела та література

1. Радутний О.Е. Поняття та ознаки інформаційної агресії на законодавчому рівні в кримінально-правовій сфері. *Інформація і право*. №2(14)/2015. С. 58 – 63.

2. Курило В.С., Савченко С.В. Інформаційна агресія в контексті гібридної війни на сході України. *Education and Pedagogical Sciences («Освіта та педагогічна наука»)* / Ред. В. С. Курило; ДЗ «Луганський національний університет імені Тараса Шевченка». 2017. № 2 (167). С. 5 – 13.

3. Кулеба Д. Війна за реальність: як перемагати у світі фейків, правд і спільнот. Київ : Книголав, 2022. 384 с.

Руслана Охріменко
Наук. керівник – к. філол. н., доцент Акіншина І. М.
м. Полтава

ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ ТА ЗАХИСТУ В СИСТЕМІ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ В УНІВЕРСИТЕТІ

У високотехнологічному сучасному світі у закладах вищої освіти важливо забезпечувати конфіденційність та захист даних у системі електронного документообігу. З ростом кількості цифрової інформації та

кіберзагроз забезпечення безпеки стає завданням першочергового значення для збереження конфіденційності даних університетської спільноти.

Отже, метою дослідження є опис технічних засобів, що сприяють збереженню конфіденційності й безпеки використання персональних даних працівників закладу вищої освіти й студентів у системі документообігу університету.

Система електронного документообігу (СЕД) – це організаційно-технічна система, яка забезпечує процес створення, управління доступом і розповсюдження електронних документів у комп'ютерних мережах, а також забезпечує контроль над потоками документів у закладах вищої освіти.

Сучасні університети активно використовують електронний документообіг для зручності обміну документами та інформацією. Це дозволяє зменшити паперовий обіг, спростити процеси та підвищити продуктивність. Однак цей підхід вимагає уваги до питань конфіденційності та захисту даних.

Конфіденційність важливо забезпечити так, щоб особисті дані студентів та співробітників були надійно захищені від несанкціонованого доступу. Потрібно встановити строгі політики доступу та шифрування інформації.

З погляду захисту даних важливо мати резервні копії електронних документів, щоб уникнути втрати інформації внаслідок технічних неполадок чи кібератак. Також важливо проводити навчання персоналу та студентів з питань кібербезпеки [1].

Очевидно, що електронний документообіг принесе багато користі, але потребує систематичного підходу до забезпечення конфіденційності та захисту даних університетської спільноти.

Потенційні загрози та ризики, пов'язані з електронним

документообігом в університетах, можуть включати:

1. *кібератаки* (університети можуть бути об'єктом кібератак, включаючи віруси, троянських коней, різновиди шкідливого програмного забезпечення та DDoS-атаки. Ці атаки можуть призвести до втрати доступу до важливих документів і даних);

2. *несанкціонований доступ* (несправедливі користувачі можуть намагатися отримати несанкціонований доступ до систем університету, щоб отримати конфіденційну інформацію або змінити дані. Це може порушити конфіденційність і цілісність даних);

3. *витоки інформації* (недбале оброблення даних або несанкціоновані дії можуть призвести до витоку конфіденційної інформації, такої як особисті дані студентів і співробітників, а також інформацію про дослідження та інтелектуальну власність) [2, с. 47].

Отже, наслідки таких порушень конфіденційності та витоку даних можуть включати фінансові втрати, втрату репутації та порушення законодавства про захист даних. Університети повинні приділяти особливу увагу кібербезпеці та використовувати ефективні заходи захисту для запобігання таким ситуаціям.

Завдяки швидкому розвитку технологій, електронний документообіг стає невід'ємною частиною функціонування університетів. Він спрощує обмін інформацією та покращує продуктивність. Але разом з перевагами приходить важлива відповідальність – забезпечення конфіденційності та захисту даних [3].

Для забезпечення конфіденційності та захисту даних у системі електронного документообігу університети можуть використовувати різні технологічні та організаційні заходи. включаючи:

1. *шифрування даних* (університет може вимагати шифрування всіх даних, що передаються через мережу та зберігаються на серверах. Наприклад, використання шифрування TLS для захисту даних під час

передачі);

2. *багатофакторна аутентифікація (MFA)* (за впровадження багатофакторної аутентифікації, де користувачі зобов'язані підтверджувати свою ідентичність за допомогою двох або більше методів, таких як пароль та мобільний токен);

3. *контроль доступу* (встановлення системи контролю доступу до документів і даних на основі ролей і прав користувачів. Це означає, що кожен користувач має доступ лише до інформації, яка необхідна для його ролі);

4. *аудит і моніторинг* (регулярний моніторинг системи для виявлення незвичайної активності та створення журналів аудиту для відстеження дій користувачів);

5. *захист від фішингу* (проведення навчання для користувачів щодо розпізнавання фішингових атак та імплементація заходів для захисту від них);

6. *резервне копіювання* (регулярне створення резервних копій даних, які зберігаються в офсайтових архівах для відновлення в разі втрати даних внаслідок аварій чи кібератак);

7. *строга політика паролів* (вимагання від користувачів створювати складні паролі та їх регулярну зміну);

8. *заборона зберігання конфіденційних даних на особистих пристроях* (закріплення правил, що забороняють зберігання чутливої інформації на особистих смартфонах або комп'ютерах);

9. *політика видалення даних* (розроблення процедур для безпечного видалення даних, коли вони більше не потрібні) [4, с. 35].

Отже, такі заходи спільно допоможуть забезпечити надійний рівень конфіденційності та захисту даних у системі електронного документообігу в університетах.

Університети активно впроваджують заходи для забезпечення

конфіденційності та захисту даних у системі електронного документообігу. Наприклад, деякі університети встановлюють системи шифрування для захисту конфіденційної інформації, подібно до того, як банки захищають фінансові транзакції. Інші впроваджують багатофакторну аутентифікацію, вимагаючи від користувачів підтверджувати свою ідентичність не лише паролем, але й додатковим підтвердженням, таким як відбиток пальця або мобільний код.

Деякі університети також встановлюють системи контролю доступу, що дозволяють обмежити права користувачів на рівні окремих документів чи папок. У такий спосіб кожен користувач має доступ лише до інформації, яка необхідна для його ролі в університеті.

Ці приклади демонструють, як університети вдосконалюють свої системи електронного документообігу, щоб забезпечити високий рівень захисту даних та зберегти конфіденційність інформації [5].

Захист даних у системі електронного документообігу – це важливий аспект сучасного університетського управління. Завдяки впровадженню технологічних та організаційних заходів, таких як шифрування, багатофакторна аутентифікація та контроль доступу, університети забезпечують конфіденційність та захист даних від потенційних загроз. Такий підхід допомагає зберегти довіру спільноти та забезпечити безпеку важливої інформації [6, с. 82].

Покращення захисту даних у системі електронного документообігу – це нагадування про важливість забезпечення конфіденційності та захисту даних у сучасних університетах. За допомогою технологічних та організаційних заходів, таких як шифрування, багатофакторна аутентифікація та контроль доступу, університети можуть надійно захищати конфіденційну інформацію від потенційних загроз.

Отже, забезпечення конфіденційності та захисту даних є необхідним для збереження довіри спільноти та партнерів, а також для виконання

законодавства про захист даних. Недбалість у цих питаннях може призвести до фінансових втрат та пошкодження репутації університету.

Тому важливо продовжувати вдосконалювати заходи безпеки, надавати пріоритет захисту даних і забезпеченню конфіденційності, і надійно працювати в електронному документообігу.

Джерела та література

1. Пономаренко В.М., Черненко К.О., Цись І.Д. Електронний (безпаперовий) документообіг. *Економіка. Управління. Інновації. Рекомендації.* 2017. № 1 (26). URL: http://dspace.pdaa.edu.ua:8080/xmlu(дата звернення: 07.11.2023).

2. Кухарін О.М., Грицяк Н.В., Назаренко К.Б. Електронний документообіг та захист інформації. Київ : НАДУ, 2020. 84 с.

3. Копняк К.В., Костунець Т.А. Аналіз сучасного стану використання електронного документообігу в університетах та конфіденційність і захист даних. *Економіка, фінанси, менеджмент: актуальні питання науки та практики*. 2019. № 57. URL: http://www.kbuapa.ua/e-book/db/2019-1/doc/1/57.pdf (дата звернення: 04.11.2023).

4. Чукут С.А., Буряченко К.Л., Сорока Н.Б. Технологічні та організаційні заходи для забезпечення конфіденційності та захисту даних у системі електронного документообігу. *Інвестиції: практика та досвід*. 2018. № 493. 56 с.

5. Сташевська О.А., Поліщук Н.В. Перспективи впровадження електронного документообігу вищих навчальних закладів. Впровадження заходів для забезпечення конфіденційності та захисту даних. 2021. № 460. URL: https://doi.org/ (дата звернення: 09.11.2023).

6. Павлюк Д.О. Конкретні приклади впровадження заходів для забезпечення конфіденційності та захисту даних в університеті. *Електронний документообіг. Конфіденційність*. 2019. № 327. 114 с.