2. Командровська В., Кривицька Н., Назаренко О. Управління діджиталізацією hr-процесів в бізнесі. *Економіка та суспільство*. 2024. № 69. DOI: 10.32782/2524-0072/2024-69-102.

3. Огляд популярних систем для HR: BambooHR, Zoho People, CakeHR і Hurma. *WORK.ua*. 22.05.2020. URL: https://www.work.ua/articles/employer/2308/ дата звернення: 05.04.2025).

4. Тур О., Петренко Д. Використання діджитал-технологій в кадровому адмініструванні та в документообігу. *Економіка та суспільство*. 2024. № 61. DOI: 10.32782/2524-0072/2024-61-33.

5. Що таке електронний кадровий документообіг та як впровадити його в компанії? *SmartPoint DMS*. 17.08.2023. URL: https://dms.smart-it.com/blog-post/what-is-hr-document-management/ (дата звернення: 05.04.2025).

УДК 004.9

Гненюк Ангеліна Олегівна
(наук. керівник – канд. екон. наук, доцент Потапова Н. А.)
Донецький національний університет імені Василя Стуса, м. Вінниця

КІБЕРБЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ ПІДПРИЄМСТВА: СУЧАСНІ ВИКЛИКИ І МЕТОДИ ЗАХИСТУ

Анотація. Обґрунтовується ключова роль кібербезпека у захисті інформаційних процесів, які активно розвиваються в умовах цифровізації та глобалізації. Аналізуються елементи кібератак, як-от фішинг, зловмисне програмне забезпечення та експлуатація вразливостей у програмному забезпеченні. Обумовлюється зв'язок між такими загрозами та значними фінансовими втратами, витоками конфіденційної інформації, порушеннями роботи компаній і серйозними репутаційними ризиками.

Ключові слова: інформаційні технології, комплексний підхід, кібербезпека, кіберзагрози, дані.

Забезпечення ефективного кіберзахисту вимагає комплексного підходу, що передбачає аналіз вразливостей, впровадження сучасних протоколів безпеки, навчання персоналу та використання новітніх технологій, зокрема штучного інтелекту та машинного навчання, для виявлення аномалій і попередження атак. Однак навіть найсучасніші системи не гарантують абсолютного захисту, тому важливим є постійний моніторинг, виявлення загроз у режимі реального часу та оперативне реагування на кіберінциденти.

Кібербезпека – це комплекс принципів, технологій і процесів, що забезпечують захист комп'ютерних систем, мереж і даних від несанкціонованого доступу, атак і пошкоджень. Вона охоплює такі ключові аспекти: фізичний захист, управління доступом, шифрування даних, а також моніторинг і реагування на інциденти. Загрози постійно еволюціонують, що вимагає комплексного підходу до забезпечення інформаційної безпеки. Основними складниками кібербезпеки є конфіденційність – запобігання несанкціонованому доступу до даних; цілісність – гарантує, що інформація не буде змінена без належного дозволу; доступність – інформація та системи повинні бути доступні для авторизованих користувачів у будь-який час; автентифікація – підтвердження облікових даних користувачів, що

контролює доступ. Серед основних методів захисту можна виділити шифрування, яке забезпечує безпеку чутливої інформації як під час зберігання, так і під час передачі. Також важливими є брандмауери та антивірусне програмне забезпечення, які захищають від зовнішніх загроз [1].

Традиційні методи захисту вже не забезпечують достатній рівень безпеки, тому необхідні адаптивні та проактивні стратегії. Швидкий розвиток технологій, зокрема хмарних обчислень та Інтернету речей, створює нові вразливості. Важливо не лише впроваджувати нові технології, але й формувати культуру кібербезпеки серед співробітників. До того ж підприємства повинні дотримуватись законів щодо захисту персональних даних, щоб уникнути фінансових і репутаційних втрат. Тільки комплексний підхід, що поєднує технологічні рішення, навчання і правові норми, забезпечить ефективний захист інформаційних систем.

Методи захисту інформаційних систем є важливою частиною стратегії кібербезпеки підприємств, оскільки сучасні загрози вимагають комплексного підходу. Одним із найефективніших методів є впровадження багаторівневої архітектури безпеки, яка включає комбінацію технологій і процесів для виявлення, запобігання та реагування на інциденти безпеки. Основними елементами цієї архітектури є периметральний захист, контроль доступу, шифрування даних і системи виявлення вторгнень (IDS) [3]. Периметральний захист забезпечується через використання брандмауерів, які контролюють вхідний і вихідний трафік, блокуючи несанкціонований доступ до внутрішніх даних організації. Брандмауери можуть бути як апаратними, так і програмними, і виконують критичну роль у захисті мережі. Контроль доступу охоплює механізми автентифікації та авторизації, які дають доступ лише авторизованим користувачам. Багатофакторна автентифікація є важливим елементом цього процесу, забезпечуючи додатковий рівень перевірки користувачів і знижуючи ризик несанкціонованого доступу. Шифрування даних відіграє ключову роль у захисті конфіденційності інформації. Воно забезпечує захист даних не лише під час їх передачі, а й у стані спокою, що знижує ризик витоків інформації навіть у разі її перехоплення зловмисниками [4]. Системи виявлення вторгнень (IDS) активно моніторять трафік у реальному часі, виявляючи аномалії, які можуть свідчити про потенційні загрози. Вони допомагають своєчасно виявити і реагувати на вторгнення або інші небезпечні ситуації. Ці методи є невід’ємною частиною захисту інформаційних систем, забезпечуючи високий рівень безпеки та мінімізуючи ризики для підприємств.

Щоденно підприємства стикаються з новими викликами, які виникають в умовах швидко змінюваного інформаційного ландшафту. Проведений аналіз показує, що основними загрозами для інформаційних систем є кібератаки, внутрішні зловживання, а також вразливості, що виникають внаслідок недостатньої грамотності співробітників. Актуальність впровадження надійних методів захисту, зокрема використання сучасних технологій шифрування, антивірусних програм та систем виявлення вторгнень, зростає з кожним днем [6].

Основною метою цих заходів є не лише захист даних, а й забезпечення цілісності й доступності інформації. Розробка детальної стратегії управління ризиками передбачає регулярний аудит інформаційних систем, навчання персоналу та

розробку політик реагування на інциденти. Продовження досліджень у цій галузі та активна співпраця з фахівцями з кібербезпеки дають змогу розробити ще ефективніші механізми захисту.

Список використаних джерел

1. Дубовий В. І. Дослідження взаємозв'язку між цифровою грамотністю та кібербезпекою суспільства: кваліфікаційна робота, спец. 125 «Кібербезпека та захист інформації». Поліський нац. ун-т, каф. комп'ютерних технологій і моделювання систем. Житомир, 2024. 46 с.

2. Кіберборотьба в умовах збройного протистояння: аналіз, стратегії та виклики / В. В. Машталір, О. М. Гук, Р. К. Мурасов, С. І. Фараон, В. В. Лоза. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2024. № 1. С. 93–104.

3. Сімаков С. Г., Чаплик О. В., Інформаційна безпека як основа надійності кредитування: управлінські стратегії для банківських установ в Україні. *Дослідження та інновації.* 2024. № 1. С. 29–36.

4. Даник Ю. Г., Воробієнко П. П., Чернега В. М. Основи кібербезпеки та кібероборони: підручник. Одеса: ОНАЗ ім. О. С. Попова, 2019. 320 с.

5. Інформаційна та кібербезпека: соціотехнічний аспект. В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа. Львів: Видавництво «Магнолія 2006», 2024. 320 с.

6. Гребенюк А. М., Гребенюк Л. В. Основи управління інформаційною безпекою: навч. посібник. Дніпро: Дніпропетровський державний університет внутрішніх справ, 2020. 144 с.

7. Панасюк В. М. Інформатизація та цифровізація: тенденції та напрями розвитку в Україні. *Інтелект XXI*. 2020. № 1. С. 160–165.

УДК 004.65:35.077.3

Дебелий Антон Васильович
(наук. керівник – канд. філол. наук, доцент Мізіна О. І.)
Національний університет «Полтавська політехніка імені Юрія Кондратюка», м. Полтава

ІННОВАЦІЙНІ ТЕХНОЛОГІЇ МОДЕРНІЗАЦІЇ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ В ОРГАНАХ ДЕРЖАВНОЇ ВЛАДИ

Анотація. У роботі досліджено ключові напрями цифрової трансформації електронного документообігу в органах державної влади України. Проаналізовано функціональні можливості та перспективи розвитку сучасних СЕД у контексті національної цифрової політики.

Ключові слова: документообіг, цифрова трансформація, система електронного документообігу, державне управління.

Збільшення обсягів інформаційних потоків, потреба в оперативному ухваленні управлінських рішень, а також актуальність забезпечення відкритості та прозорості діяльності органів влади обумовлюють необхідність переходу від традиційного паперового до цифрового документообігу. Електронний документообіг є інноваційною технологією, яка реалізує високу швидкість і надійність передавання інформації у формі документів між органами державної влади, громадянами та державними структурами, всередині організацій, а також на міждержавному рівні. Саме завдяки впровадженню електронного документообігу досягаєть-