УДК 004.056.55

Сауляк Я. Ю.
Кирилащук Т. Г.

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ У ЦИФРОВОМУ СЕРЕДОВИЩІ. КОНФІДЕНЦІЙНІСТЬ, GDPR, ВИТОКИ ДАНИХ, ПОЛІТИКИ БЕЗПЕКИ

Вінницький національний технічний університет

Анотація

У роботі розглянуто механізми забезпечення захисту персональних даних у цифровому середовищі з акцентом на дотримання принципів конфіденційності та нормативних вимог General Data Protection Regulation (GDPR). Проаналізовано типові сценарії витоку інформації, зокрема несанкціонований доступ, фішингові атаки та вразливості інформаційних систем.

Окрему увагу приділено практичним підходам до формування політик інформаційної безпеки, включаючи контроль доступу, шифрування даних та багатофакторну автентифікацію. Визначено ключові фактори, що впливають на рівень захищеності персональних даних, та обґрунтовано необхідність комплексного підходу до їх захисту в умовах зростання кіберзагроз.

Ключові слова: персональні дані, конфіденційність, General Data Protection Regulation (GDPR), витоки даних, інформаційна безпека, контроль доступу, шифрування, багатофакторна автентифікація.

Abstract

The paper examines mechanisms for protecting personal data in the digital environment, focusing on confidentiality principles and compliance with the General Data Protection Regulation (GDPR). Typical data breach scenarios are analyzed, including unauthorized access, phishing attacks, and system vulnerabilities.

Particular attention is given to practical approaches to developing information security policies, such as access control, data encryption, and multi-factor authentication. Key factors affecting the level of personal data protection are identified, highlighting the need for a comprehensive security strategy in the context of evolving cyber threats.

Keywords: personal data, confidentiality, General Data Protection Regulation (GDPR), data breaches, information security, access control, encryption, multi-factor authentication.

Вступ

Обробка персональних даних у цифрових системах супроводжується ризиками їх несанкціонованого доступу, витоку та зловживання. Основні загрози виникають через вразливості програмного забезпечення, помилки конфігурації, а також людський фактор. У цих умовах забезпечення конфіденційності даних вимагає не лише технічних засобів захисту, а й чіткого дотримання регуляторних вимог, зокрема General Data Protection Regulation (GDPR).

Ефективний захист персональних даних базується на поєднанні механізмів контролю доступу, криптографічного захисту та впровадженні політик інформаційної безпеки. Водночас зростання кількості кіберінцидентів демонструє, що ізольовані заходи не забезпечують належного рівня безпеки, що обумовлює необхідність комплексного підходу до управління захистом даних у цифровому середовищі.

Результати дослідження

У цифровому середовищі персональні дані обробляються в хмарних сервісах, веб-додатках та розподілених інформаційних системах, що підвищує ризик їх компрометації. Основні загрози пов’язані з витоками інформації, несанкціонованим доступом та недостатнім рівнем захисту інфраструктури. У

цих умовах забезпечення конфіденційності даних вимагає не лише технічних рішень, а й дотримання вимог General Data Protection Regulation (GDPR), які регламентують обробку та зберігання персональної інформації.

Ключову роль у захисті даних відіграють механізми шифрування, які унеможливлюють доступ до інформації без відповідних ключів навіть у випадку її перехоплення або витоку. Водночас ефективність захисту залежить від правильного управління доступом, контролю автентифікації користувачів та впровадження політик безпеки, що регулюють роботу з персональними даними.

Окрему увагу слід приділити причинам витоків даних, серед яких домінують вразливості програмного забезпечення, помилки адміністрування та фішингові атаки. Аналіз таких інцидентів показує, що більшість порушень безпеки виникає через комплекс факторів, а не через одну конкретну слабкість системи.

Ефективний захист персональних даних передбачає використання багаторівневих механізмів безпеки. До них належать багатофакторна автентифікація, сегментація доступу, шифрування даних під час зберігання і передавання, а також постійний моніторинг подій безпеки. Такий підхід дозволяє мінімізувати ризики несанкціонованого доступу та своєчасно виявляти потенційні загрози.

Практична реалізація політик інформаційної безпеки в організаціях демонструє, що поєднання технічних засобів і регуляторних вимог забезпечує більш високий рівень захисту. Застосування комплексних заходів дозволяє не лише запобігати витокам даних, а й підвищувати стійкість систем до сучасних кіберзагроз.

Висновки

У роботі проаналізовано підходи до захисту персональних даних у цифровому середовищі з акцентом на забезпечення конфіденційності та запобігання витокам інформації. Розглянуто механізми шифрування, контролю доступу та автентифікації, що використовуються для обмеження несанкціонованого доступу до даних. Особливу увагу приділено впровадженню політик інформаційної безпеки та дотриманню вимог General Data Protection Regulation (GDPR).

Запропонований підхід базується на комплексному використанні технічних і організаційних заходів, що дозволяє знизити ризики компрометації даних та підвищити стійкість інформаційних систем до кіберзагроз. Отримані результати підтверджують ефективність інтегрованих методів захисту для забезпечення безпеки персональної інформації в сучасних цифрових умовах.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Eduardo V., Erpen de Bona L. C., Zola W. M.Speculative Encryption on GPU in Cryptographic File Systems // *Proceedings of the 17th USENIX Conference on File and Storage Technologies (FAST'19)*. – Boston, USA, 2019. – P. 93–108.
2. William Stallings *Cryptography and Network Security: Principles and Practice*. – 7th ed. – Boston: Pearson Education, 2017. – 766 p.
3. Niels Ferguson, Bruce Schneier, Tadayoshi Kohno.*Cryptography Engineering: Design Principles and Practical Applications*. – Indianapolis: Wiley Publishing, 2010. – 432 p.
4. Christof Paar, Jan Pelzl. *Understanding Cryptography: A Textbook for Students and Practitioners*. – Berlin: Springer, 2010. – 371 p.

Сауляк Ярослав Юрійовича – студент групи 2БС-24б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: yarikyanvarev57@gmail.com

Науковий керівник: ***Кирилащук Тетяна Геннадіївна*** – асистент кафедри захисту інформації, Вінницький національний технічний університет, Вінниця, e-mail: kgt0998@gmail.com

Sauliak Yaroslav – student of group 2BS-24B, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: yarikyanvarev57@gmail.com

Scientific Supervisor: ***Kyrylashchuk Tatyana*** – assistant of the Information Security Department, Vinnytsia National Technical University, Vinnytsia, e-mail: kgt0998@gmail.com