

Features of forming cybersecurity in computer design development

Valentyn Diachenko

Kyiv University of Intellectual Property and Law, Kyiv

<https://orcid.org/0000-0002-0055-9256>

Nataliia Diachenko

Kyiv University of Intellectual Property and Law, Kyiv

<https://orcid.org/0000-0002-4306-7665>

Vladyslav Popolitov

Kyiv University of Intellectual Property and Law, Kyiv

<https://orcid.org/0009-0008-5404-4275>

Vladimir Konstantinov

Kyiv University of Intellectual Property and Law, Kyiv

<https://orcid.org/0009-0002-2408-5267>

Abstract. *The features and challenges of cybersecurity formation in computer design development are investigated. It is emphasized that ensuring intellectual property rights in computer design development is a priority task. The need to adhere to the basic principles of safe use of software, computer communication tools and collaboration is substantiated. The challenges of cybersecurity formation in computer design development are identified.*

Keywords: *computer design, cybersecurity, software.*

Особливості формування кібербезпеки при розробці комп'ютерного дизайну

Валентин Дяченко

Київський університет інтелектуальної власності та права, м. Київ

<https://orcid.org/0000-0002-0055-9256>

Наталія Дяченко

Київський університет інтелектуальної власності та права, м. Київ

<https://orcid.org/0000-0002-0055-9256>

Владислав Пополітов

Київський університет інтелектуальної власності та права, м. Київ

<https://orcid.org/0009-0008-5404-4275>

Володимир Константинов

Київський університет інтелектуальної власності та права, м. Київ

<https://orcid.org/0009-0002-2408-5267>

Анотація. *Досліджено особливості та виклики формування кібербезпеки при розробці комп'ютерного дизайну. Наголошено, що забезпечення права інтелектуальної власності при розробці комп'ютерного дизайну є пріоритетним завданням. Обґрунтована необхідність дотримання базових принципів безпечного використання програмного забезпечення, інструментів комп'ютерних комунікацій та співпраці. Ідентифіковано виклики формування кібербезпеки при розробці комп'ютерного дизайну.*

Ключові слова: *комп'ютерний дизайн, кібербезпека, програмне забезпечення.*

Формування кібербезпеки при розробці комп'ютерного дизайну – важлива складова сучасного креативного процесу. Більшість дизайнерських проєктів реалізується в цифровому середовищі, де існує високий ризик кіберзагроз, пов'язаних із використанням мереж, спільної роботи в хмарних сервісах, спеціалізованого програмного забезпечення та передачі конфіденційних даних. Тому безпека даних і середовища створення дизайну має вирішальне значення.

Ігнорування потреби формування кібернетичної захищеності процесів розробки комп'ютерного дизайну може призвести до серйозних наслідків, таких як витік конфіденційних даних, компрометація інтелектуальної власності чи навіть використання дизайнерських рішень для шкідливих цілей. Серед ключових особливостей формування кібербезпеки процесів розробки комп'ютерного дизайну є потреба захисту права інтелектуальної власності, обмеження доступу до файлів дизайнерського проєкту, шифрування даних тощо (табл. 1):

Таблиця 1. Ключові особливості формування кібербезпеки процесів розробки комп'ютерного дизайну

Напрямок	Заходи	Особливості
Захист інтелектуальної власності	Контроль доступу	Обмеження доступу до файлів проєкту лише авторизованим співробітникам. Використання надійних паролів та багатофакторної автентифікації.
	Шифрування даних	Шифрування файлів проєкту необхідно здійснювати як під час зберігання, так і під час передачі інформації.
	Використання систем контролю версій	Використання систем контролю версій (наприклад, Git) для відстеження змін, резервного копіювання запобігатиме втраті даних.
	Укладання договорів про нерозголошення (англ. Non-Disclosure Agreement, NDA)	Укладання угод про нерозголошення інформації з усіма, хто має доступ до конфіденційних даних проєкту сприятиме запобіганню витоку інформації

Дизайнери використовують широкий спектр програмного забезпечення (графічні редактори, CAD-системи, програми для 3D-моделювання тощо). Важливо забезпечити безпеку цих інструментів шляхом:

- використання виключно ліцензійного програмного забезпечення та його регулярне оновлення для виправлення вразливостей;
- перевірки програмного забезпечення на наявність відомих вразливостей перед його використанням;
- ізоляції середовища, зокрема здійснювати розробку дизайну в ізольованому

віртуальному середовищі, щоб мінімізувати ризики розповсюдження шкідливого програмного забезпечення.

Дизайн-процес часто передбачає тісну співпрацю з клієнтами, колегами та підрядниками. Безпека комунікацій може бути досягнута шляхом:

- використання шифрованих каналів зв'язку (VPN, захищені месенджери) для обміну файлами та обговорення проєктів;
- вибору платформ для спільної роботи, які мають надійні функції безпеки та регулярно оновлюються;
- регулярного навчання персоналу, яке передбачає проведення тренінгів з кібергігієни для всіх учасників проєкту, щоб підвищити їхню обізнаність щодо потенційних загроз (фішинг, соціальна інженерія) [1].

Незважаючи на всі заходи безпеки, збій обладнання, помилка користувача або кібератака можуть призвести до втрати даних. З метою збереження інформації важливо мати надійну систему резервного копіювання, яка б забезпечувала б:

- автоматизоване та регулярне створення резервних копій всіх проєктних файлів;
- зберігання резервних копій на різних носіях та у віддалених місцях (хмарні сховища, зовнішні диски) для захисту від локальних інцидентів;
- регулярне тестування процесу відновлення даних з резервних копій для впевненості в їх працездатності.

Забезпечення кібербезпеки при розробці комп'ютерного дизайну – це неперервний процес, який вимагає уваги на всіх етапах, від планування до завершення проєкту. Впровадження цих особливостей допоможе захистити цінні активи та зберегти репутацію.

Сучасний комп'ютерний дизайн дедалі частіше використовує інноваційні технології, зокрема хмарні сервіси, колаборативні платформи та інструменти штучного інтелекту. У зв'язку з цим постає низка викликів у сфері кібербезпеки, що безпосередньо впливають як на процес розробки, так і на збереження результатів творчої діяльності, серед яких захист конфіденційних даних і авторських прав дизайнерів. Під час спільної роботи над проєктами існує ризик несанкціонованого доступу до вихідних файлів, що може призвести до крадіжки чи спотворення дизайнерських рішень. Це зумовлює потребу впровадження сучасних методів аутентифікації користувачів, систем шифрування даних і постійного моніторингу активності.

Не менш важливий виклик пов'язаний з інтеграцією сторонніх інструментів та плагінів, що значно розширюють можливості дизайнерських програм.

Використання ненадійного або скомпрометованого програмного забезпечення може стати джерелом шкідливого коду, здатного порушити роботу системи чи скомпрометувати дані.

Головним, на наш погляд, є виклик організації безпечного середовища зберігання та передачі даних. У добу глобалізації й віддаленої співпраці виникає потреба у захищених каналах зв'язку та сервісах резервного копіювання, здатних гарантувати цілісність і доступність інформації.

Навіть найкращі технічні засоби захисту не гарантуватимуть безпеку, якщо учасники проєкту використовують слабкі паролі, завантажують файли з ненадійних джерел чи не оновлюють програмне забезпечення.

Дизайнери, які часто комунікують з клієнтами та підрядниками, можуть стати мішенню для фішингових атак, що можуть призвести до витоку важливих даних чи компрометації робочих акаунтів.

Використання штучного інтелекту та генеративних сервісів може також стати ризиком зокрема через ненавмисне завантаження конфіденційних даних у відкриті системи чи створення підроблених зображень, що можуть ввести в оману замовників.

Процеси масштабування проєктів призводять до збільшення чисельності залучених фахівців, ускладнюють контроль за їх діяльністю та збільшують ризики витоку інформації.

Використання хмарних сервісів, надаючи можливість оперативного цілодобового доступу до власної інформації, потребує особливо ретельної перевірки налаштувань доступу, щоб уникнути публічного поширення приватних даних, а відтак, розробка комп'ютерного дизайну сьогодні нерозривно пов'язана з питаннями кібербезпеки. Тільки системний підхід, що передбачає поєднання технічних рішень, правових інструментів та підвищення обізнаності фахівців [2], дозволить ефективно протидіяти сучасним кіберзагрозам і зберегти інтелектуальні здобутки дизайнерської спільноти.

Несанкціонований доступ до дизайн-файлів може призвести до втрати інтелектуальної власності або витоку конфіденційної інформації. Тому формування навичок кібербезпеки серед дизайнерів є необхідною умовою професійної діяльності в сучасному інформаційному просторі.

Список використаних джерел

1. Дяченко В. С., Дяченко Н. П. (2024). Врахування ризиків при використанні інформаційних технологій. *Information technology: computer science, software engineering and cyber security*. Вип. 4. С. 75-80. <https://doi.org/10.32782/IT/2024-4-10>.
2. Дяченко В. С., Дяченко Н. П. (2024). Особливості впровадження сучасних інформаційних технологій в освітні процеси. *Успіхи і досягнення у науці*. № 2(20). С. 347-361. [https://doi.org/10.52058/3041-1254-2024-2\(2\)-347-361](https://doi.org/10.52058/3041-1254-2024-2(2)-347-361).