особливості функціоналу частини для адміністраторів. Перелік даних статей дає вичерпний матеріал із сучасних технологій створення веб-сайтів та по основних тенденцій розвитку галузі веб-програмування, що дозволяє об'єктивно оцінити свій сайт перед його публікацією у всесвітній мережі. Також детально описанні нові можливості мови розмітки HTML5 і таблиці каскадних стилів CSS3.

У процесі дослідження розроблено сайт для Міжнародного тренінгового центру «Освітня інноватика» для підвищення кваліфікації вчителів інформатики, який виконаний за допомогою HTML5 і CSS3 з використанням PHP, на порталі є 4 сторінки з важливою інформацією про курси, сторінки «Про нас», «Корисні посилання» (для тих хто проходить курси), «Головна», де зібрана інформація про курси і їх організаторів і «Контакти» для зв'язку із організаторами.

У моєму досліджені описано основні проблеми розробки дизайну сайту і його функціоналу, особливості частини для адміністратора, форми реєстрації нових учасників, а також детальна інформація про кожен розділ інформаційного порталу. Досліджено нові можливості HTML5 і CSS3 для створення правильного функціоналу сайту. Оцінено можливості PHP I Javascript для створення інтерактивного сайту, що дозволяють створювати власні плагіни для обслуговування сайту і подання інформації у коректному і цікавому вигляді.

Найважливішим дослідженням є кросплатформенність і кросбраузерність для коректного представлення сайту на усіх пристроях під управлінням різних операційних систем, на даний час CSS3 (система каскадних стилів) дозволяє оптимізувати відображення сайту на різних девайсах.

Найкращим виходом для організації кросплатформенності є мова програмування JAVA, що працює на усіх пристроях під управлінням усіх популярних на даний момент операційних систем. Вона дозволяє правильно інтерпретувати код для поставлених задач, не витрачаючи ресурсів сервера, адже JAVA є мовою програмування, яка має свій інтерпретатор вмонтований у браузер і зменшує навантаження на систему.

У ході виконання завдання було розроблено веб-портал із власною частиною адміністрування сайту і можливістю реєстрації користувачів адміністратором, що забороняє несанкціонований доступ до ресурсів. Реєстрація користувачів на курси організована за допомогою бази даних MySQL і мови програмування PHP, що надсилає запити до бази і отримує відповіді про правильність авторизації користувачів і відповідає за реєстрацію користувачів на курси. У перспективі розвитку поставлено завдання для проведення невеликих опитувань для покращення роботи сайту і завдання до деяких курсів.

Проаналізувавши дані, можна сказати, що технології розробки веб-сайтів розвивається стрімкими темпами і надає нових можливостей для створення і наповнення інформаційних порталів. На даний час для створення сучасного веб-сайту потрібно знати багато аспектів програмування і оптимізації сайту що дозволяє збільшити цільову аудиторію і зробити свій сайт більш інтерактивним. У моїй роботі досліджується аспекти програмування на мові HTML5, CSS3 I PHP. Основні аспекти кращої оптимізації сайту залежать від потреб і призначення порталу, а також від користувачів, які будуть ним користуватись.

### ЛІТЕРАТУРА


1. Засоби створення Web-сайтів [Електронний ресурс]. — Режим доступу:
2. http://pidruchniki.com/1970070547797/informatika/zasobi_stvorennya_web-saytiv
3. Веб-розробка [Електронний ресурс]. — Режим доступу:
4. https://uk.wikipedia.org/wiki/%D0%92%D0%B5%D0%B1-%D1%80%D0%BE%D0%B7%D1%80%D0%BE%D0%B1%D0%BA%D0%B0
5. Яркие решения.[Електронний ресурс]. — Режим доступу: http://webstudio2u.net
6. Як створити сайт з нуля самому[Електронний ресурс]. — Режим доступу: http://poradumo.pp.ua/kompyter-i-internet/15847-yak-stvoriti-sayt-z-nulya-samomu.html
7. Як створюємо сайт на HTML [Електронний ресурс]. — Режим доступу: http://ruszura.in.ua/html/yak-stvoryujemo-sajt-na-html.html
8. Як створити свій сайт ? [Електронний ресурс]. — Режим доступу: http://sseo.pp.ua


*Куліковський І.*

*Науковий керівник – доц. Карабін О. Й.*

## СПОСОБИ ЗАХИСТУ БЕЗПЕКИ ПРИВАТНИХ ДАНИХ У ВІРТУАЛЬНИХ СЕРЕДОВИЩАХ ТА МЕТОДИ ЇХ ЗАХИСТУ

**Постановка проблеми**. Згідно статистичних даних розвиток технологій відбувається безперервно і з плином часу все більше з'являються нові концепції їх розвитку. Нині технологічні інновації характеризуються різноманітними середовищами, одним із яких є віртуальне. Саме тому на ринку технологій популярним є факт, що дані зберігаються у віртуальних середовищах. Відтак однією з проблем, яка постає з цього — є захист та безпека приватних даних у віртуальних середовищах.

**Метою статті** є дослідження загроз захисту приватних даних у віртуальних середовищ та методів їх захисту.

Для досягнення постановленої мети необхідно вирішити такі завдання:

1. Охарактеризувати способи захисту безпеки приватних даних у віртуальних середовищах.
2. Дослідити основні методи захисту приватних даних.

**Виклад основного матеріалу.** Для початку розглянемо поняття та основні загрози віртуального середовища. *Віртуальне середовище* — система, створена для підтримки процесу дистанційного керованого доступу до того, чи іншого середовища управління, доступом Збереження даних у віртуальному середовищі на сьогоднішній день є дуже актуальним, оскільки це не тільки спрощує роботу власника цих даних, тому що все зберігається в одному місці, і дозволяє на будь якому іншому комп'ютері мати доступ до цих даних. Одним із фактором є те, що проблеми з носіями або з випадковими втратами інформації не вплинуть на результат і пророблену роботу, яка збереглась у віртуальному середовищі [1].

Розгляд безпеки віртуальних середовищ та їх приватних даних доцільно почати з аналізу існуючих загроз. Контроль і управління середовищами є проблемою безпеки, оскільки немає гарантії, що всі ресурси підраховані і в неї немає неконтрольованих віртуальних машин, не запущених зайвих процесів і не порушена взаємна конфігурація елементів управління. Це небезпечний тип загроз, тому що він пов'язаний з керованістю середовищ, як єдиною інформаційною системою і для неї загальних захист потрібно будувати індивідуально. Для цього необхідно використовувати модель управління ризиками для захисту приватних даних у віртуальних середовищах [7].

Дослідження IDC Predictions [6] дозволяють стверджувати, що сьогодні існує значно ширший набір інструментів для забезпечення безпеки ніж раніше, робота далека від завершення. У деяких випадках для виведення на IT-ринок тієї або іншої технології, що допомагає вирішити нове завдання, проходить деякий час, навіть незважаючи на те, що вона вже розроблена. Наприклад, дані з вбудованим захистом (саме захищені дані) і довірені монітори.

Найбільш ефективні способи захисту в галузі безпеки віртуальних середовищ опублікувала організація Cloud Security Alliance (CSA):

*Збереження даних.* Шифрування — один з найефективніших способів захисту даних. Провайдер повинен шифрувати інформацію клієнта, яка зберігається в ЦОД, а також безповоротно видаляти у випадку необхідності.

*Захист даних при передачі.* Зашифровані дані при передачі повинні бути доступні тільки після аутентифікації. Дані не будуть розкриті або модифіковані, навіть при доступі через ненадійні вузли. Такі технології використовуються провайдерами: алгоритми та протоколи AES, TLS, IPsec тощо [8].

*Аутентифікація.* Для забезпечення більш високої надійності, використовують токени та сертифікати. Для прозорої взаємодії з провайдером при авторизації рекомендується використовувати протоколи LDAP (Lightweight Directory Access Protocol) і SAML (Security Assertion Markup Language).

*Ізоляція користувачів.* Віртуальні мережі повинні бути розгорнуті із застосуванням таких технологій, як VPN (Virtual Private Network), VLAN (Virtual Local Area Network) і VPLS (Virtual Private LAN Service).

Аналіз існуючих систем управління безпекою показав, що сучасні системи повинні включати в себе коректний аналіз ймовірних вторгнень і можливість оперативної реакції на потенційні атаки. Тому актуальним є підвищення ефективності методів і засобів управління безпекою, особливо в застосуванні їх для розподілених комп'ютерних систем.

На рисунку 1 зображено трирівневу модель захисту приватних даних у віртуальному середовищі [4]. Вона складається з трьох основних рівнів: аутентифікація, шифрування даних та швидке відновлення.


*Рис. 1. Трирівнева модель захисту приватних даних [2]*

Перший рівень відповідає за аутентифікацію користувача шляхом перевірки його цифрового сертифікату. На другому рівні відбувається шифрування даних і визначення прав доступу даного користувача. На третьому рівні — швидке відновлення інформації у разі її пошкодження або втрати [2].

Перед початком роботи опишемо основні поняття моделі. *Модель* — опис об'єкта (предмета, явища або процесу) на якій-небудь формалізованій мові, складений з метою вивчення його властивостей. Такий опис особливо корисний у випадках, коли дослідження самого об'єкта ускладнене або фізично неможливе. Також модель буде за змістом частково формальною. *Формальні інформаційні моделі* (числення висловлювань) — це моделі, створені формальною мовою (тобто науковою,

професійною або спеціалізованою, наприклад мовою програмування). Приклади формальних моделей: всі види формул, таблиці, графи, карти, схеми тощо [3].

Для забезпечення більш високого рівня безпеки необхідно комплексно вирішувати дане завдання:

— скерувати виконання завдання забезпечення безпеки інформаційного середовища Web–сервера хостинг-провайдеру або data-центру;

— регулярно використовувати спеціальні засоби для моніторингу захищеності інформаційного середовища Web-сервера;

— періодично проводити незалежний комплексний аудит безпеки інформаційного середовища Web-сервера.


*Рис. 2. Модель загроз віртуального середовища*

Для вирішення цього завдання на етапі проектування моделі захисту приватних даних було запропоновано модель загроз віртуального середовища, яку подано на рисунку 2.

**Висновки.** Проаналізувавши основні загрози та методи захисту віртуального середовища з'ясовано, що ці дослідження є перспективними для подальшого розвитку віртуальних середовищ. Після застосування цих рішень кількість загроз приватних даних істотно знижується. Але багато проблем, пов'язаних із захистом віртуалізації, вимагають ретельного аналізу і опрацьованого рішення.

## ЛІТЕРАТУРА


1. Гнатюк С. Л. Актуальні питання захисту персональних даних у віртуальному середовищі (на прикладі технологій та сервісів «ного» обчислення) : аналіт. зап. / С. Л. Гнатюк. [Електронний ресурс]. — Режим доступу : http://www.niss.gov.ua/articles/1090/.
2. Марреро А. Прогноз: к 2015 году треть украинских компаний будут использовать облачные технологии / Антон Марреро // [Електронний ресурс]. — Режим доступу : http://www.marrero.com.ua/oblachnye-tekhnologii/149-prognoz-k-2015-godu-tret-ukrainskikh-kompanij-budut-ispolzovat -oblachnye-tekhnologii.
3. Морозов А. В. Проблема правовой защиты персональных данных / А. В. Морозов // [Електронний ресурс]. — Режим доступу : http://www.kiev-security.org.ua/box%20/4/136.shtml.
4. Права человека и защита персональных даннях. — Харьков: Фолио-ХПГ, 2000. — 280 с.
5. IDC Predictions 2013. Competing on the 3rd Platform : Opportunities at the Intersection of Mobile, Cloud, Social, and Big Data. [Електронний ресурс]. — Режим доступу до ресурсу: http://clck.ru/8aXZM.
6. International Working Group on Data Protection in Telecommunications (IWGDPT). [Електронний ресурс]. — Режим доступу : http://clck.ru/8aXVe.
7. Symantec Avoiding the Hidden Costs of the Cloud. [Електронний ресурс]. — Режим доступу : http://www.symantec.com/connect/blogs/avoiding-hidden-costs-cloud.
8. Working Paper on Cloud Computing. Privacy and data protection issues («Sopot Memorandum»). [Електронний ресурс]. — Режим доступу : http://clck.ru/8aJ9c.


*Цимбаляк М.*