isu-conference.com

ISU

INTERNATIONAL SCIENTIFIC UNITY

COLLECTION OF SCIENTIFIC PAPERS

ISSUE №21

3RD INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE

RESEARCH IN SCIENCE, TECHNOLOGY AND ECONOMICS

MAY 28-30, 2025
LUXEMBOURG, LUXEMBOURG

INTERNATIONAL SCIENTIFIC UNITY

3rd International Scientific and Practical Conference

«Research in Science, Technology and Economics»

Collection of Scientific Papers

May 28-30, 2025
Luxembourg, Luxembourg

UDC 01.1

Research in Science, Technology and Economics: Collection of Scientific Papers with Proceedings of the 3rd International Scientific and Practical Conference. International Scientific Unity. May 28-30, 2025. Luxembourg, Luxembourg. 566 p.

ISBN 979-8-89704-985-1 (series)
DOI 10.70286/ISU-28.05.2025

The conference is included in the Academic Research Index ReserchBib International catalog of scientific conferences.

The collection of scientific papers presents the materials of the participants of the 3rd International Scientific and Practical Conference "Research in Science, Technology and Economics" (May 28-30, 2025).

The materials of the collection are presented in the author's edition and printed in the original language. The authors of the published materials bear full responsibility for the authenticity of the given facts, proper names, geographical names, quotations, economic and statistical data, industry terminology, and other information.

ISBN 979-8-89704-985-1 (series)

Official site: https://isu-conference.com/

5. National CIO Review. (2024, March 16). Cybersecurity in 2025: The trends reshaping security strategies. Retrieved from https://nationalcioreview.com/articles-insights/cybersecurity-in-2025-the-trends-reshaping-security-strategies/
6. Otava. (2024). 2025 Trends in Edge Computing Security. Retrieved from https://www.otava.com/2025-trends-in-edge-computing-security/
7. Palo Alto Networks. (2024). Cybersecurity in 2025: How One Year Will Reshape the Industry. Retrieved from https://www.paloaltonetworks.com/why-paloaltonetworks/cyber-predictions
8. Splunk. (2024). Cybersecurity Trends. Retrieved from https://www.splunk.com/en_us/blog/learn/cybersecurity-trends.html
9. Strobes.co. (2024). 10 Cybersecurity Trends to Watch in 2025 and How to Prepare. Retrieved from https://strobes.co/blog/10-cybersecurity-trends-to-watch-in-2025-and-how-to-prepare/

ІНФОРМАЦІЙНА БЕЗПЕКА В ІНТЕРНЕТІ: ЗАГРОЗИ, ЗАХИСТ, КУЛЬТУРА ТА ПРАВО

Деркач Тетяна
к.т.н., доцент
Гринюк Данило
здобувач вищої освіти
Національний університет «Полтавська політехніка імені Юрія Кондратюка», Україна

У сучасному цифровому світі інтернет став невід'ємною частиною повсякденного життя. Він відкриває безліч можливостей – від спілкування та розваг до банківських операцій і дистанційної роботи. Однак поряд із перевагами виникають серйозні загрози, пов’язані з інформаційною безпекою. Уразливість персональних даних, шахрайство, віруси та атаки хакерів – усе це створює виклики, з якими стикається як окрема людина, так і суспільство в цілому. Інформаційна безпека – це сукупність заходів, спрямованих на захист інформації від несанкціонованого доступу, модифікації, знищення або розголошення. Вона охоплює не лише технічні аспекти, такі як шифрування чи захист від вірусів, а й організаційні та правові заходи.

Забезпечення інформаційної безпеки передбачає дотримання принципів конфіденційності, цілісності та доступності інформації [3].

Сучасна концепція інформаційної безпеки включає також питання етики в цифровому середовищі, дотримання прав користувачів на приватність, а також створення безпечного інформаційного простору для всіх учасників мережі.

Основні загрози в мережі. Сучасний Інтернет надає великі можливості, але водночас є джерелом численних кіберзагроз.

Шкідливе програмне забезпечення (віруси, трояни, програми-шпигуни) здатне збирати інформацію без відома користувача.

Фішингові атаки часто маскуються під надійні сервіси, щоб виманити у користувачів конфіденційні дані.

Кібербулінг, шантаж, соціальна інженерія – це не лише технічні, а й психологічні загрози, що впливають на психіку та соціальну поведінку людини.

Також небезпеку становлять вразливості в програмному забезпеченні, неправильне налаштування систем безпеки та використання застарілих протоколів.

Все частіше зловмисники використовують штучний інтелект для проведення більш складних атак, що робить питання кіберзахисту ще актуальнішим.

Захист. Найефективніший спосіб захисту – це поєднання технічних рішень та обізнаності користувача. Слід регулярно оновлювати операційну систему та додатки для усунення відомих вразливостей. Антивірусне програмне забезпечення та фаєрволи допомагають виявити і блокувати загрози в режимі реального часу. Використання складних, унікальних паролів для кожного сервісу разом із двофакторною автентифікацією значно ускладнює несанкціонований доступ. Також важливо користуватися лише перевіреними Wi-Fi мережами, уникати відкритих публічних точок доступу або користуватися VPN для захисту переданої інформації. Копіювання важливих даних на зовнішні носії або у хмарні сховища з належним захистом є ключем до збереження інформації у разі атаки або збою системи.

Культура поведінки в Інтернеті. Інформаційна гігієна – це основа безпечного цифрового життя. Не варто передавати особисту або фінансову інформацію через неперевірені канали або підозрілі сайти. У соцмережах доцільно обмежити публічний доступ до особистих даних та уникати додавання незнайомих осіб. Користувачі мають бути обережними при відкритті електронної пошти — не варто відкривати підозрілі вкладення або переходити за сумнівними посиланнями. Також важливо регулярно проводити цифрову «чистку»: переглядати дозволи додатків, видаляти непотрібні акаунти та змінювати паролі.

Правові аспекти. В Україні діє Закон «Про захист персональних даних», який регламентує збір, зберігання та обробку приватної інформації [2]. Кіберзлочини підлягають кримінальній відповідальності згідно зі статтями Кримінального кодексу України. У міжнародній практиці діють норми, як-от GDPR у Європейському Союзі, які забезпечують високий рівень захисту приватності користувачів. Крім того, міжнародні організації, такі як ENISA та Interpol, активно працюють над створенням глобальної системи реагування на кіберзагрози [1].

Знання своїх прав і обов’язків у цифровому середовищі – основа правової безпеки кожного користувача.

У сучасному цифровому світі користувач несе не лише персональну відповідальність, а й стає учасником глобальної системи кіберзахисту. Інформаційна грамотність повинна стати частиною освітньої програми починаючи зі школи. Саме усвідомлення ризиків і розуміння основ кібербезпеки

дозволяє уникати більшості загроз. Також важливо ділитися знаннями з близькими — допомагати літнім людям або дітям налаштувати безпечне середовище для користування Інтернетом. Кожен крок до відповідального цифрового громадянства формує більш безпечний онлайн-простір.

Інформаційна безпека в інтернеті – це не лише технічна, а й соціальна проблема. Кожен користувач має нести відповідальність за свою поведінку онлайн, а держава й бізнес – створювати умови для безпечного цифрового середовища. Тільки спільними зусиллями можна подолати виклики, що постають у світі кіберзагроз.

Список використаних джерел

1. Європейське агентство з кібербезпеки ENISA. URL: https://www.enisa.europa.eu
2. Закон України «Про захист персональних даних». URL: https://zakon.rada.gov.ua/laws/show/2297-17 (дата звернення 20.05.2025)
3. Кіберпростор: аналіз загроз та методи захисту/Деркач Т.М., Лавренко М.//L International scientific and practical conference «Innovative Education: Problems and Prospects of Scientific Research» Stuttgart, Germany. International Scientific Unity, 2024. 112-115 p.

СУЧАСНІ БІЗНЕС-ПРОЦЕСИ ОРГАНІЗАЦІЇ ВІДПУСТОК В АУТСОРС-КОМПАНІЯХ

Кузнєцов Дмитро Олександрович
здобувач вищої освіти
Євланов Максим Вікторович
професор кафедри ІУС
Харківський національний університет радіоелектроніки, Україна

Потреба у впорядкованому процесі відпусток зростає разом із масштабом компанії. Коли число співробітників перетинає позначку у кількасот людей, паперові заяви та розрізнені електронні листи стають джерелом помилок, подвійних бронювань і фінансових втрат. Це особливо актуально для аутсорс-компаній, де команди рідко перебувають в одному часовому поясі та працюють над кількома клієнтськими проєктами паралельно. У такому середовищі важливо забезпечити прозору та автоматизовану систему оформлення відпусток, щоб зберегти темп роботи й довіру замовників. Організація бізнес-процесів відпусток стає не лише адміністративним завданням, а й критичним елементом управління ресурсами, який запобігає перевантаженню та допомагає уникати зривів у графіках поставок [1].

Запропонована BPMN-модель на рисунку 1 є ефективною тому, що поєднує миттєву фіксацію наміру працівника відпочити з багатоетапним цифровим контролем навантаження: дані про дедлайни, заплановані релізи та вже