НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

28 листопада 2025 року

КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ

МАТЕРІАЛИ VI МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Одеська юридична академія»
Факультет кібербезпеки та інформаційних технологій
Кафедра кібербезпеки

КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ

МАТЕРІАЛИ VI МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

28 листопада 2025 року, м. Одеса

Одеса, 2025

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
National University «Odesa Law Academy»
Faculty of Cybersecurity and Information Technologies
Department of Cybersecurity

CYBERSECURITY IN TODAY'S WORLD: ACTUAL CHALLENGES

MATERIALS OF THE VI INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE

November 28, 2025, Odesa

Odesa, 2025

УДК 004.056

Відповідальній редактор:

О. В. Дикий, декан факультету кібербезпеки та інформаційних технологій, кандидат юридичних наук, доцент

Матеріали видано в авторській редакції.
Повну відповідальність за достовірність та якість поданого матеріалу несуть учасники конференції, їхні наукові керівники, які рекомендували ці матеріали до друку.

Рекомендовано до друку
Вченою радою Національного університету
«Одеська юридична академія»
(протокол №3 від 29.11.2025 р.)

Матеріали Міжнародної науково-практичної конференції «Кібербезпека в сучасному світі: актуальні виклики» (м. Одеса, 28 листопада 2025 р.). Одеса, 2025. 287 с.

У конференції взяли участь студенти, аспіранти, молоді вчені, викладачі та науковці. Конференція проводиться на базі Національного університету «Одеська юридична академія».

UDC 004.056

Editor-in-chief:

O. V. Dykyi, Dean of the Faculty of Cybersecurity and Information Technologies,
Candidate of Law, Associate Professor

The materials were published in the author's edition.
Full responsibility for the reliability and quality of the submitted material
bears the participants of the conference, their scientific supervisors,
who recommended these materials for publication.

Recommended for printing
by the Academic Council of the National University
«Odesa Law Academy»
(Minutes No. 3 dated 11/29/2025)

Materials of the International Scientific and Practical Conference «Cybersecurity in the Modern World: Current Challenges» (Odessa, November 28, 2025). Odesa, 2025. 287 p.

The conference was attended by students, postgraduates, young scientists, teachers and researchers. The conference is held at the National University «Odesa Law Academy».

VI Міжнародна науково-практична конференція

«Кібербезпека в сучасному світі: актуальні виклики»

28 листопада 2025 року

ТЕМАТИЧНІ НАПРЯМКИ КОНФЕРЕНЦІЇ:

Секція 1. Алгоритмічні та технічні аспекти кібербезпеки

Секція 2. Штучний інтелект та інформаційні технології

Секція 3. Управлінські, соціальні та психологічні аспекти взаємодії з кіберпростором

Секція 4. Нормативно-правові засади кібербезпеки та захисту інформації

E-mail: kiberprostirconf@gmail.com (Для питань та тез)

VI International Scientific and Practical Conference

«Cybersecurity in today's world: actual challenges»

28 November 2025 year

THEMATIC DIRECTIONS OF THE CONFERENCE:

Section 1. Algorithmic and technical aspects of cybersecurity

Section 2. Artificial intelligence and information technologies

Section 3. Management, social and psychological aspects of interaction with cyberspace

Section 4. Regulatory and legal principles of cybersecurity and information protection

E-mail: kiberprostirconf@gmail.com (Для питань та тез)

обґрунтованих рішень на інтелектуальному рівні. Їх інтеграція з машинним навчанням та штучним інтелектом відкриває нові можливості для автоматизації та аналізу даних.

На даний час проблемою залишається достатньо велика різноманітність способів і підходів до зберігання і оброблення неструктурованих даних і, тому, у кожному окремому випадку, вибір інструментарію залежить від вимог конкретного проекту, його масштабу та характеристик даних.

Список використаних джерел:

1. E. F. Codd, “A relational model of data for large shared data banks,” Communications of the ACM, vol. 13, no. 6, pp. 377–387, 1970. : https://www.seas.upenn.edu/~zives/03f/cis550/codd.pdf
2. S. Tiwari, Professional NoSQL, John Wiley & Sons, 2011. URL : https://books. google.com.ua/books/about/Professional_NoSQL.html?id=tv5iO9MnObUC&redir_esc=y
3. Miral Borad, Tejas Chauhan, Harsh Mehta. A Review on NoSQL Databases. November 2017. International Journal of Science and Research (IJSR) 6(11): 26-28. URL : https://www.researchgate.net/publication/327883334_A_Review_on_NoSQL_Databases
4. Piekos, J. (2015). SQL vs, NoSQL vs. NewSQl: finding the right solution. Retrieved June, 11, 2018. URL : https://www.researchgate.net/publication/340978543_SQL_NewSQL_and_NOSQL_Databases_A_Comparative_Survey/link/5ec46445a6fdcc90d685d608/download?_tp=eyJjb250ZXh0Ijp7Im-ZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19

Ключові слова: Системи управління базами даних, реляційна модель, хмарні технології, горизонтальне масштабування баз даних, нормалізація даних, напівструктурований формат даних.

Key words: Database management systems, relational model, cloud technologies, horizontal database scaling, data normalization, semi-structured data format.

ПРОБЛЕМА БЕЗПЕКИ ПЕРСОНАЛЬНИХ ДАНИХ У CRM-СИСТЕМАХ (НА ПРИКЛАДІ SALESFORCE)

Бойко Віктор

кандидат технічних наук, доцент кафедри кібербезпеки Національного університету «Одеська юридична академія»

Перепелиця Марія

студентка 4-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

CRM-системи стали ключовою інфраструктурою взаємодії бізнесу з клієнтами, оскільки централізують великі масиви персональних даних (ПД) –

від ідентифікаційних атрибутів до історії комунікацій і транзакцій. Саме тому безпека ПД у CRM є не лише технічною задачею, а й предметом правового регулювання, корпоративного управління ризиками та відповідальності перед клієнтами. Особливості сучасних CRM як хмарних багатокористувацьких рішень (multi-tenant), їхня широка інтегрованість через API, мобільні клієнти та маркетингові екосистеми створюють розгалужену поверхню атаки і множину сценаріїв витоків даних. У роботі розглядаються характерні загрози та організаційно-технічні механізми їхнього стримування на прикладі Salesforce, однієї з найпоширеніших CRM-платформ, з опорою на офіційні навчальні матеріали Trailhead [1], [2].

Актуальність проблеми зумовлена концентрацією ПД у CRM та зростанням залежності бізнес-процесів від цих платформ. Будь-яка помилка конфігурації доступу, некоректна інтеграція або неналежне управління життєвим циклом ПД можуть призвести до інцидентів, що мають фінансові, репутаційні й юридичні наслідки (у т.ч. штрафи за порушення GDPR та національного законодавства). Для великих організацій, де CRM інтегрує відділи продажів, підтримки, маркетингу та аналітики, вразливість одного сегмента здатна спричинити каскадні ефекти у суміжних, подовжуючи час відновлення сервісів та збільшуючи сукупні втрати – отже, міркування стійкості та швидкого відновлення мають бути невід'ємною частиною моделі захисту [9]-[14].

Проблематика безпеки ПД у CRM має декілька рівнів. Технічний рівень охоплює моделі доступу до даних і шифрування, аудит подій, сегментацію середовища та керування інтеграціями. Організаційний рівень визначає політики мінімізації даних, принцип «найменших привілеїв», контроль постачальників (включаючи додатки з маркетплейсів), навчання користувачів і процедури реагування. Правовий рівень регламентує правові підстави обробки, інформування суб'єктів, права доступу/видалення, транскордонні передачі та локалізацію даних. У хмарних CRM ці рівні взаємозалежні: наприклад, вибір регіону розміщення даних (data residency) безпосередньо впливає на можливість дотримання локальних норм та на архітектурні рішення резервування й відновлення [9]-[13], [15].

На прикладі Salesforce можна системно описати основні вектори ризику та механізми їхнього пом'якшення. Базовою умовою є правильна побудова моделі доступу: організаційні стандартні налаштування (Organization-Wide Defaults), ієрархія ролей (Role Hierarchy) та правила надання доступу (Sharing Rules) працюють разом і визначають, хто і що бачить у межах організації. Ієрархія ролей надає менеджерам видимість записів підлеглих, а правила шерингу дозволяють робити винятки та розширювати доступ поза ієрархією – у т.ч. для зовнішніх користувачів-партнерів. Правильне застосування цих механізмів, разом із контролями доступу на рівні полів (Field-Level Security) та

об'єктів (Profiles/Permission Sets), формує «базову лінію» захисту ПД та мінімізує ризики надмірних прав користувачів [1]-[4], [14].

Шифрування даних у стані спокою – ключова вимога для ПД, що зберігаються у хмарі. У Salesforce ця функція реалізується через Shield Platform Encryption, яка дозволяє шифрувати конфіденційні поля та файли з керуванням життєвим циклом ключів. Для організацій, що опрацьовують ПД високої чутливості (фінансова/медична інформація, ідентифікаційні документи), увімкнення шифрування «на місці зберігання» поряд із політиками маскування даних у непроходових середовищах (Data Mask) знижує наслідки компрометації та обмежує видимість ПД навіть для привілейованих користувачів [5], [6].

Моніторинг і аудит – ще один критичний шар захисту. Подієвий моніторинг (Event Monitoring) надає журнали дій користувачів і клієнтів API, що дозволяє виявляти аномалії (масове завантаження даних, підозрілі логіни, нетипові запити) і будувати дашборди для оперативного реагування. Реалізація моніторингу у реальному часі та застосування політик транзакційної безпеки (Transaction Security) допомагають не лише «бачити» події, а й запобігати небажаним діям (наприклад, блокувати скачування великого обсягу ПД поза графіком) [7], [8].

Проблеми безпеки ПД у CRM часто походять від інтеграцій і додатків. Salesforce як платформа підтримує численні з'єднання через API та екосистему додатків, що створює ризики поширення доступів і копій ПД за межі контрольованого периметра. Політики «need-to-know», ревізія маркерів/секретів, обмеження обсягу даних у вебхуках та регулярний перегляд дозволів додатків мають бути обов'язковими; контроль повинен підкріплюватися технічними засобами – від журналів подій API до лімітів запитів і автоматизованих сповіщень про нетипові інтеграційні патерни. З огляду на мобільні клієнти та віддалений доступ, доцільно застосовувати умовний доступ (policy-based) і обмеження експорту ПД у незахищені канали [1], [7], [8].

Важливим напрямом зниження ризиків є управління життєвим циклом ПД і мінімізація даних. Модуль Privacy Center у Salesforce дозволяє створювати політики зберігання, маскування й видалення ПД та підтримувати запити суб'єктів даних (копія, стирання, знеособлення). Коректна класифікація ПД (визначення категорій чутливості й призначення відповідних контролів доступу) покращує узгодженість політик і спрощує доведення відповідності регуляторним вимогам. У межах продуктової лінійки Salesforce також доступні засоби виявлення ПД (Data Detect) і навчальні матеріали з політик приватності, що формують методичну основу для впровадження «privacy by design» [9]-[11].

Окремо варто відзначити вимоги локалізації та резидентності даних. Ініціатива Hyperforce дає змогу обирати регіон зберігання даних і підтримувати

локальні вимоги, забезпечуючи зберігання ПД «на місці» в публічній хмарі та спрощуючи відповідність нормам (у т.ч. GDPR і національним). Для організацій із географічно розподіленою присутністю коректна стратегія резидентності зменшує юридичні ризики і спрощує моделювання відмовостійкості [12], [13].

З урахуванням наведеного, ключові групи ризиків у CRM можна структуровано подати так:

- Конфігураційні: помилки у ролях/правах, надмірні дозволи, «приватні» об'єкти без винятків, або, навпаки, надто широкі правила доступу [1].

- Інтеграційні: витоки через API/вебхуки, слабкі секрети, додатки третьої сторони, що запитують надмірні скоупи [7], [8].

- Операційні: масові експорти, відсутність журналювання, несвоєчасний аналіз подій, відсутність тригерів реального часу [7], [8].

- Дані та приватність: відсутність політик мінімізації, неточна класифікація, зберігання ПД у непотрібних середовищах, відсутність автоматизованого видалення/маскування [9]-[11].

- Юридичні: неврегульовані транскордонні передачі, відсутність прозорих підстав обробки, порушення строків відповіді на запити суб'єктів [9]-[13].

Практична модель підвищення безпеки ПД у Salesforce повинна поєднувати архітектурні та процесні заходи. На архітектурному рівні: визначити «зону довіри» для ПД, застосувати Shield Platform Encryption до чутливих полів/файлів, установити політики Data Mask у непроходових середовищах, упровадити шаблон «least privilege» з регулярними recertification-кампаніями прав доступу; окремо – уніфікувати правила шерингу, мінімізувати індивідуальні винятки. На рівні моніторингу: активувати Event Monitoring (у т.ч. реального часу) та Transaction Security, налаштувати дашборди ризикових подій (аномальні logins, великі експорти, масштабні API-виклики). На рівні даних і приватності: запровадити класифікацію ПД і політики Privacy Center для автоматизованої мінімізації, видалення та обробки запитів суб'єктів даних; підтримувати data lineage для інтеграцій. На організаційному рівні: затвердити політики екосистеми додатків, провести інвентаризацію інтеграцій, обмежити скоупи доступів, установити процеси безпечного розроблення (DevSecOps) для конфігурацій і метаданих CRM. На рівні стійкості: поєднати резервне копіювання/відновлення з репетиціями інцидент-response, щоб скорочувати час відновлення та уникати каскадних збоїв у суміжних сервісах [5]-[11], [16].

Висновки. Безпека ПД у CRM-системах – це системна задача на перетині технічних, організаційних і правових практик. На прикладі Salesforce видно, що платформа надає розвинуті механізми керування доступом,

шифрування, моніторингу подій та управління приватністю. Однак ефективність цих механізмів визначається якістю їхнього впровадження: узгодженістю ролей і правил шерингу, дисципліною в інтеграціях, наявністю політик класифікації/мінімізації даних і постійним аудитом. З огляду на зростання обсягу й цінності ПД, а також на правові вимоги, організації мають інвестувати в налаштування та періодичну перевірку захисних контролів, а також у підготовку користувачів. Для студентів і фахівців із кібербезпеки Trailhead-пісочниці (Trailhead Playgrounds) дають безпечне середовище відпрацювання цих підходів без доступу до продуктивних даних – це дозволяє формувати практичні навички без витягання коду з реальної CRM та без ризику для ПД [1], [2].

Список використаних джерел:

1. Data Security – Improve Record Access Control in Your Org. Trailhead, Salesforce. URL: https://trailhead.salesforce.com/content/learn/modules/data_security/data_security_records
2. Trailhead Playground Management – Module. Trailhead, Salesforce. URL: https://trailhead.salesforce.com/content/learn/modules/trailhead_playground_management
3. Define Sharing Rules. Trailhead, Salesforce. URL: https://trailhead.salesforce.com/content/learn/modules/data_security/data_security_sharing_rules
4. Communities & External Users – Sharing Rules. Trailhead, Salesforce. URL: https://trailhead.salesforce.com/content/learn/projects/communities_share_crm_data/sharing_rules
5. Shield Platform Encryption. Trailhead, Salesforce. URL: https://trailhead.salesforce.com/content/learn/modules/spe_admins
6. Shield Platform Encryption – Quick Look. Trailhead, Salesforce. URL: https://trailhead.salesforce.com/content/learn/modules/shield-platform-encryption-quick-look2/get-to-know-shield-platform-encryption2
7. Event Monitoring – Module. Trailhead, Salesforce. URL: https://trailhead.salesforce.com/content/learn/modules/event_monitoring
8. Real-Time Event Monitoring – Module. Trailhead, Salesforce. URL: https://trailhead.salesforce.com/content/learn/modules/realtime-event-monitoring
9. Privacy Center – Module. Trailhead, Salesforce. URL: https://trailhead.salesforce.com/content/learn/modules/privacy-center
10. Prepare for Privacy Center. Trailhead, Salesforce. URL: https://trailhead.salesforce.com/content/learn/modules/privacy-center/prepare-for-privacy-center
11. Create a Data Management Policy in Privacy Center. Trailhead, Salesforce. URL: https://trailhead.salesforce.com/content/learn/modules/privacy-center/create-a-data-management-policy-in-privacy-center
12. Hyperforce – Data Residency. Salesforce Help. URL: https://help.salesforce.com/s/articleView?id=000795008
13. Introducing Hyperforce – General Information & FAQ. Salesforce Help. URL: https://help.salesforce.com/s/articleView?id=000388902

14. Create a Role Hierarchy. Trailhead, Salesforce. URL: https://trailhead.salesforce.com/content/learn/modules/data_security/data_security_roles
15. Cybersecurity Challenges in Cloud-based CRM. SSRN Working Paper, 2024. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5005031
16. Best Practices for Protecting Your CRM Data. National Cybersecurity Alliance (StaySafeOnline), 2025. URL: https://staysafeonline.org/articles/best-practices-for-protecting-your-crm-data

Ключові слова: CRM, персональні дані, конфіденційність, доступ на основі ролей, правила шерингу, шифрування, моніторинг подій, Privacy Center, Hyperforce, резидентність даних.
Keywords: CRM, personal data, confidentiality, role-based access, sharing rules, encryption, event monitoring, Privacy Center, Hyperforce, data residency.

ЗАХИСТ ІГРОВИХ РЕСУРСІВ У СУЧАСНИХ ВІДЕОІГРАХ: КОНЦЕПЦІЯ ТА ПРАКТИЧНА РЕАЛІЗАЦІЯ В ГРІ «HONEY & MOLD»

Дяченко Аріна

студентка 4 курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Соколов Артем

доктор технічних наук, професор кафедри кібербезпеки Національного університету «Одеська юридична академія»

Сфера відеоігор є однією з найдинамічніших і фінансово потужних галузей цифрової індустрії: щороку ігровий ринок залучає мільярдні інвестиції та забезпечує значні прибутки розробникам, видавцям і сервісним платформам. В умовах такої конкуренції успіх ігрового продукту значною мірою залежить від ефективності механізмів захисту внутрішніх ресурсів [1, 2]. Порушення цілісності ігрових даних, втручання у збереження, маніпуляції з внутрішньою економікою чи обхід механік прогресу можуть не лише руйнувати баланс гри, але й завдавати прямих фінансових збитків.

Сучасні відеоігри давно вийшли за межі традиційних розваг і перетворилися на складні програмні системи, в яких поєднуються елементи кібербезпеки, управління даними, штучного інтелекту та мережевої інфраструктури. Тому захист внутрішніх ігрових ресурсів стає критично важливим завданням і для великих студій, і для розробників. Особливо актуальним це є у проєктах, де економічний баланс визначає динаміку геймплею й безпосередньо впливає на користувацький досвід.

Метою цієї роботи є проєктування системи безпеки ресурсів гри «Honey & Mold».

ЗМІСТ