КОНФІДЕНЦІЙНІСТЬ ПРИ ЗБИРАННІ ДАНИХ У СИСТЕМІ ДИСТАНЦІЙНОГО НАВЧАННЯ

[1]Шапран О.О., [2]Судніков Є.О., [3]Прокопенко А.А.
Національний університет оборони України імені Івана Черняховського
[1]*o.shapran@nuou.org.ua,* [2]*vestix@ukr.net,* [3]*allicka7@gmail.com*

У багатьох навчальних системах контроль конфіденційності є другорядним – це ряд налаштувань конфіденційності, що супроводжуються складною політикою конфіденційності. На відміну від цього, система дистанційного навчання повинна використовувати філософію конфіденційності згідно з моделлю [1], яка дасть змогу розробникам і дослідникам таких систем вибирати характеристики, які найкраще впораються з побоюваннями користувачів. Більш того, реалізація конфіденційності, адаптованої під запити користувача, допоможе системам моделювати проблеми конфіденційності учнів і надавати їм адаптивну підтримку у прийнятті рішень щодо конфіденційності [2].

Це може номінально подовжити цикл розроблення, але при цьому запобігатиме виникненню ситуації, коли система має безліч складних налаштувань конфіденційності та складну політику конфіденційності, у якій учні не можуть орієнтуватися, або, що ще гірше, повну відсутність захисту конфіденційності.

Різноманітні персональні дані можуть бути зібрані через систему дистанційного навчання, включаючи активність учня під час навчання, його компетенції та умови навчання. Такі дані можуть бути зібрані анонімно або з прив’язкою до профілю учня. Практика збирання даних у системі дистанційного навчання може мати унікальні наслідки для конфіденційності залежно від типу зібраних даних, їх джерела та потенційної можливості їх

ідентифікувати. Тож критично важливо враховувати ці аспекти під час визначення та розроблення методів збирання даних у системі дистанційного навчання.

Один з найбільш послідовних висновків досліджень конфіденційності полягає в тому, що люди сильно відрізняються у поглядах на розкриття інформації. Часто використовувана концептуалізація свідомих рішень людей щодо розкриття інформації – це "розрахунок конфіденційності", який передбачає, що люди приймають рішення про конфіденційність, врівноважуючи передбачувані ризики і переваги доступних варіантів вибору. Однак люди не завжди раціональні у прийнятті рішень щодо конфіденційності. Системи дистанційного навчання повинні опитувати своїх користувачів, щоб дізнатися більше про евристичні процеси прийняття рішень, які можуть негативно вплинути на розкриття інформації.

Соціальну мережу Інтернет-користувачі також вибирають залежно від стилю спілкування, якому вони надають перевагу. Системи дистанційного навчання, які використовують або реалізують компоненти соціальних мереж, повинні адаптувати свої функції забезпечення конфіденційності до різних стилів управління конфіденційністю.

Використання і поширення персональних ідентифікаційних даних учнів заслуговує на особливу увагу, оскільки створює ризик розкриття особистості учнів іншим сторонам. Проблеми конфіденційності, пов'язані з персональними ідентифікаційними даними, можна пом'якшити, дозволивши користувачам системи дистанційного навчання залишатися повністю анонімними. Повністю анонімна взаємодія означає, що з користувачем не пов'язані постійні ідентифікатори. Однак це складно виконати у системах дистанційного навчання, оскільки більшість навчальних дій передбачає численні взаємодії, а

це означає, що система повинна бути здатна розпізнавати учня в ході цих взаємодій. Реалістичнішим є варіант, згідно з яким користувачам можна буде взаємодіяти із системою дистанційного навчання під псевдонімом. Однак ефективність псевдонімів і інших засобів деідентифікації особистих даних була поставлена під сумнів, оскільки такі дані також можуть піддаватися ризику повторної ідентифікації, особливо у системах дистанційного навчання, які збирають дані у багатьох вимірах та з різних джерел. Незважаючи на це, дослідники стверджують, що деідентифікація даних сервера все ще є гарною практикою безпеки, оскільки, навіть якщо сервер буде зламаний, знадобляться значні зусилля для повторної ідентифікації всіх користувачів.

Також системи цифрового навчання мають можливість збирати широкий спектр даних про своїх користувачів. Безперервне відстеження може створити цифровий паноптикум, що обмежує свободу користувача. Отже, користувачам потрібно надати прості у використанні механізми повідомлення і контролю для управління межею між дозвіллям і навчанням. Крім того, активність користувачів під час виконання завдань має бути ретельно захищена за допомогою комбінації суворого контролю доступу, деідентифікації, обфускації, шифрування і (або) персоналізації з боку клієнта.

Занепокоєння учнів щодо конфіденційності може також бути викликане висновками, зробленими про них системою дистанційного навчання. Передбачається, що майбутні системи дистанційного навчання будуть повсюдними, з використанням кількох пристроїв. Кожен з цих пристроїв має унікальні обмеження конфіденційності. Саме тому процес навчання на таких пристроях повинен бути структурований так, щоб не турбував учнів і не розкривав інформацію про них неконтрольованим чином.

Список використаних джерел

1. Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

2. Knijnenburg, B. P. (2015). A user-tailored approach to privacy decision support (Doctoral dissertation, UC Irvine).