УДК 004.056:378

АНАЛІЗ ІНФОРМАЦІЙНИХ РИЗИКІВ, ПОВ'ЯЗАНИХ ІЗ ПУБЛІЧНИМ РОЗМІЩЕННЯМ СТИПЕНДІАЛЬНИХ РЕЙТИНГІВ СТУДЕНТІВ

Горохов Я. А.
e-mail: yaroslav.horokhov@nure.ua
Науковий керівник – проф. Радівілова Т.А.
Харківський національний університет радіоелектроніки, каф. ІКІ імені В.В. Поповського,
м. Харків, Україна

This article examines the risks associated with personal data exposure in open-access scholarship ratings. Publicly available information, including full names and academic grades, allows attackers to easily locate students' emails and photos for targeted social engineering. Students receiving scholarships often become priority targets for cybercriminals due to their verified financial activity. The research highlights how this information enables highly convincing spear phishing campaigns by exploiting institutional trust. The study highlights that insufficient data protection necessitates improved university security protocols and data anonymization to effectively mitigate the risks of successful social engineering attacks by scammers.

У сучасному світі знайти інформацію про людину стає все легше завдяки розвитку пошукових систем. Це несе за собою збільшення ризиків реалізації атаки на цю людину, тому необхідністю стає фільтрування інформації про себе перед оприлюдненням у публічному просторі. Але навіть якщо ми можемо контролювати власні дії щодо поширення інформації про себе, то витоком інформації може бути державна установа, наприклад, заклад вищої освіти, який публікує інформацію про студентів.

Університети надають стипендіальні рейтинги у відкритому доступі, що є дуже зручно, так як можна швидко отримати інформацію про оцінки, наявність стипендії та конкуренцію серед студентів. Але за цією зручністю стоїть розкриття інформації про студентів. Відповідно до закону "Про захист персональних даних", персональні дані – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована [1]. Отже, наявність у списках студентів прізвищ, імен та по-батькові (ПІБ) вже ідентифікує людину.

У багатьох організаціях прийнято стандартний спосіб створення електронної пошти для користувача у вигляді ім'я.прізвище@gmail.com, університети можуть мати власні домени [2]. З цього виходить, що з'являється можливість отримати канал зв'язку зі студентом, через який зловмисник може вести комунікацію. Також, акаунт пошти студента може мати фото профілю, за яким можна ідентифікувати вигляд студента.

За стипендіальним рейтингом можна дізнатися чи отримує студент стипендію. Частина кафедр одразу виокремлює студентів із стипендією, але

і без цього можна легко дізнатися кількість стипендіатів, обравши перші 40-45% від усіх бюджетників списку. На основі цієї інформації стає зрозумілим, що студент отримує дохід, а отже може стати пріоритетною ціллю для шахраїв.

Проаналізувавши стипендіальний список студентів зловмисник може отримати дані щодо ПІБ, електронної пошти, фото профілю, наявності доходу. Отримана інформація окремо одна від одної не несе ризиків, але вся разом агрегована інформація допомагає створити портрет людини та використати ці дані для майбутніх атак. Також варто зазначити, що для отримання цих даних необхідна мінімальна кількість знань, а отже коло потенційних зловмисників збільшується за рахунок людей з низьким рівнем навичок.

Отримані дані зловмисник може використати для різних цілей. Першою ціллю може бути заволодіння банківськими даними та паролями студентів. Це звичайна практика шахраїв, які шляхом обману хочуть нажитися на довірливих особах.

Другою ціллю є отримання інформації з обмеженим доступом (ІзОД), якою може володіти студент або мати до неї доступ. Здобувач освіти може бути частиною команди, яка займається реалізацією новітніх розробок, інформація про які має цінність для конкурентів, іноземних держав або окремих осіб.

Третьою ціллю може бути сам студент, який має успіхи у навчанні, та який потенційно як майбутній фахівець може нести загрозу країнам-агресорам або мати на них вплив. Такими є студенти, які навчаються за напрямками інформаційної безпеки, військових наук, оборонної інженерії, міжнародних відносин, економічної та енергетичної безпеки, а також аналізу даних і штучного інтелекту – адже їхні професійні компетентності спрямовані на зміцнення обороноздатності та стійкості держави до зовнішніх загроз. Зловмисники можуть розглядати способи зниження ефективного навчання таких студентів через атаки на інфраструктуру навчальних закладів або навіть виконати фізичну ліквідацію.

Варто розглянути методи соціальної інженерії та їх можливі реалізації через отримані дані для досягнення цілей зловмисником. Першим методом є імперсоналізація, через яку зловмисник видає себе за іншого [3]. Наприклад, зловмисник видає себе за працівника кафедри і під приводом зміни оцінок за семестр надсилає файл, який містить шкідливе програмне забезпечення.

Другим методом є фішинг – поширення електронних листів з метою отримання банківських даних або паролів користувача. Наприклад, зловмисник пише студенту, що його переведено зі звичайної стипендії на підвищену, але дані його карти для виплат застарілі та потребують оновлення, тому необхідно перейти за посиланням та надати актуальну інформацію.

Третім методом є претекстинг, який побудований на створенні детальної вигаданої ситуації з метою входження в довіру протягом тривалого часу, від кількох тижнів до місяців. Наприклад, зловмисник може написати студенту, який володіє ІзОД щодо розробок кафедри, від імені одного з працівників цієї кафедри з пропозицією підвищити його оцінку за семестр, якщо той підтвердить свою наукову активність документами про розробки.

Зручність використання відкритих списків студентів та їх рейтингових балів на противагу має ризики компрометації як студентів, так і службової інформації, якою вони володіють. Цю проблему можливо вирішити двома способами. Першим способом є використання авторизації та автентифікації перед отриманням доступу до перегляду стипендіального рейтингу. Наприклад, використовувати сайт для дистанційного навчання, де поміж матеріалів навчальних дисциплін буде знаходитися окремий список.

Другим способом є використання анонімізації студентів шляхом заміни їх ПІБ на певний числовий ідентифікатор, який буде унікальним для кожного студента. Наприклад, це може бути номер залікової книжки або номер студентського квитка. Таким чином, стипендіальні рейтинги залишаться у відкритому доступі, але ідентифікація студентів буде неможливою, якщо не мати інформацію щодо номеру та його власника.

Відкритість стипендіальних рейтингів є лише частиною того, що може дізнатися зловмисник про людину, використовуючи відкриті джерела інформації. ПІБ студента можна пов’язати з його банківським рахунком, знайти у соціальних мережах, переглянути інформацію у державних реєстрах тощо. В епоху інтернету людство живе у такий час, коли людині може написати особа, яку він не може ідентифікувати, в той час коли ця особа вже ідентифікувала його.

Список використаних джерел:

1. Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI: станом на 18 лютого 2026 р. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text.

2. Professional Email Address Examples. VitaMail Blog. URL: https://vitamail.vitanur.com/blogs/professional-email-address-examples (дата звернення: 18.02.2026).

3. Соціальна інженерія. ESET: Енциклопедія загроз. URL: https://www.eset.com/ua/support/information/entsyklopediya-zahroz/sotsialna-inzheneriya/ (дата звернення: 18.02.2026).