УДК 004.56

КОНТЕКСТУАЛЬНІ ХАРАКТЕРИСТИКИ ЦИФРОВИХ СЛІДІВ І ЇХ ВПЛИВ НА ІНФОРМАЦІЙНУ БЕЗПЕКУ УНІВЕРСИТЕТУ

Лахно М.В., науковий керівник Шкарупило В.В

У ході досліджень щодо управління інформаційною безпекою (ІБ) інформаційно-освітнього середовища університету (ІОСУ) було показано, що ефективне використання даних, отриманих шляхом збору та аналізу різних цифрових слідів (ЦС) користувачів — студентів, викладачів і співробітників — може сприяти підвищенню рівня ІБ та ступеня її захищеності від зовнішніх і внутрішніх загроз.

Розроблено концептуальну модель модуля системи підтримки прийняття рішень (СППР), що базується на аналізі ЦС користувачів ІОСУ. Модель враховує як контекстно-залежні, так і контекстно-незалежні характеристики ЦС (відповідно КЗХ і КНХ), які впливають на стан ІБ в ІОСУ. Аналіз ЦС у межах ІОСУ надає фахівцям з ІБ університету можливість не лише визначати рівень компетентності та відстежувати індивідуальні освітні траєкторії студентів, а й розробляти відповідні керівні дії для забезпечення стійкості ІБ.

Розглядається застосування програмних продуктів, таких як Splunk та ELK Stack (що включає Elasticsearch, Logstash і Kibana), які дозволяють не лише ефективно аналізувати лог-файли, але й виявляти потенційні загрози ІБ ІОСУ. Ці інструменти забезпечують університетам високу ефективність у виявленні, відстеженні та аналізі проблем, пов’язаних із ЦС користувачів, тим самим сприяючи посиленню захисту від несанкціонованого доступу до ресурсів ІОСУ.

Наприклад, у системі дистанційного навчання (СДН) кожен студент має відповідний профіль. У найпростішому випадку кортеж, що описує такий профіль, можна представити у вигляді:

$$UP = \langle ID\_user, UP\_out, UP\_in \rangle,$$

де UP – профіль користувача; ID_user – унікальне ім’я користувача в ІОСУ (в тому числі в СДН);

UP_out, UP_in – множини контекстно-залежних і контекстно-незалежних характеристик користувача відповідно.

Очевидно, що користувач ІОСУ має як КЗХ, так і КНХ, що впливають на забезпечення його інформаційної безпеки. До КЗХ можна віднести, наприклад, рівень технічних знань користувача щодо ІБ. Насправді користувачі (зокрема студенти), які мають глибші знання в питаннях ІБ, зазвичай краще обізнані щодо ризиків і заходів безпечної роботи в мережі.

До цього набору можна також віднести ступінь обізнаності користувача про ризики ІБ, що значно впливає на поведінку користувача і часто визначає вибір заходів захисту. У цьому наборі також буде присутній стиль поведінки користувача в мережі університету – обережний користувач, наприклад, не відкриватиме небезпечні посилання або не завантажуватиме ненадійне ПЗ.

До КНХ можна віднести, наприклад: ідентифікаційні дані користувача; заходи фізичної безпеки пристроїв (наприклад, використання сканера відбитків пальців на ноутбуці чи смартфоні); своєчасне оновлення ПЗ; використання надійних паролів; усвідомлення ризиків фішингу та здатність класифікувати підозрілі повідомлення, що можуть призвести до розголошення особистої інформації; тощо.

Вказані КЗХ і КНХ, звісно, можуть варіюватися в кожному конкретному ІОСУ з урахуванням її особливостей — архітектури обчислювальної мережі, обраної стратегії захисту ІБ та інших факторів.

Для аналізу ЦС фахівці з ІБ використовують різні програмні засоби [1–4]. Один із результатів, який отримують під час аналізу ЦС в ІОСУ, – це профіль завдань, які виконував студент. Під профілем завдань мається на увазі формалізований опис процесу взаємодії здобувача освіти з елементами ІОСУ – наприклад, із сайтом СДН або інформаційною системою університету, під час виконання конкретного завдання.

Таким чином, на основі профілів завдань у контексті забезпечення ІБ ІОСУ, фахівці з інформаційної безпеки можуть визначати типи завдань, що мають значення для безпеки, і, наприклад, за допомогою лог-файлів, відстежувати рішення, прийняті користувачами.

У цьому випадку справедливим є таке представлення моделі життєвого циклу користувача в ІОСУ (*MC*) під час вирішення завдання:

$$MC = (TP, Type\_P(t_o, t_d), PA, D(t_d), R_1, R_2),$$

де $TP -$ ідентифікатор, який призначається завданню певного профілю;

$Type\_P(t_o, t_d) -$ тип (вид) завдання, яке виконує здобувач освіти, починаючи з моменту часу (t_o) і до моменту ухвалення рішення (t_d) (наприклад, завантаження виконаної роботи до системи дистанційного навчання);

$PA -$ проблемна область завдання; $D(t_d) -$ рішення, ухвалене у момент часу (t_d) ; $R_1 \in Type\_P \times PA$, $R_2 \in Type\_P \times D$.

Висновок. Проаналізовано можливості використання даних цифрових слідів (ЦС) користувачів інформаційно-освітньої системи університету (ІОСУ) для інтелектуалізації процесів прийняття рішень, спрямованих на підвищення рівня інформаційної безпеки (ІБ). Показано, що для управління ІБ в ІОСУ доцільно використовувати дані, отримані в результаті аналізу ЦС здобувачів освіти та співробітників.

Показано, що для ефективного управління ІБ в ІОСУ доцільно використовувати дані, отримані в результаті аналізу ЦС здобувачів освіти та співробітників, зокрема за допомогою спеціалізованого ПЗ – Splunk, ELK Stack (Elasticsearch, Logstash і Kibana). Такий підхід дозволяє виявити аномальні або підозрілі активності, що можуть свідчити про спроби несанкціонованого доступу до ІОСУ або інші загрози безпеці університетів. Зокрема, можна виявити порушення норм поведінки в Інтернеті, несанкціоновані спроби доступу до захищених ресурсів, а також потенційно небезпечні зміни в активностях користувачів, які потребують додаткового моніторингу або втручання.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Лахно, В., Волошин, С., Мамченко, С., Кулініч, О., & Касаткін, Д. (2024). Кластерний аналіз для дослідження цифрових слідів студентів закладів освіти. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(23), 31–41.

2. Пічкур, М. О., Полудень, Л. І., Демченко, І. І., & Сотська, Г. І. (2023). Моніторинг цифрових слідів образотворчої підготовки здобувачів вищої мистецької освіти. Інформаційні технології і засоби навчання, 2(94), 128–149.

3. Morze, N., Kuzminska, O., & Mazorchuk, M. (2019). Attitude to the digital learning environment in Ukrainian universities. In ICT in Education, Research, and Industrial Applications. Proc. 15th Int. Conf. ICTERI 2019. Volume II: Workshops. (Vol. 2393, pp. 53–67). Zaporizhzhia National University Department of Computer Science.

4. J. Hedman, N. Srinivisan and R. Lindgren, “Digital Traces of Information Systems: Sociomateriality Made Researchable,” Thirty-fourth International Conference on Information Systems Milan 2013, vol. 38, pp. 809–830, 2013.

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ТЕОРЕТИЧНІ ТА ПРИКЛАДНІ АСПЕКТИ РОЗРОБКИ КОМП'ЮТЕРНИХ СИСТЕМ

ЗБІРНИК НАУКОВИХ ПРАЦЬ ЗА МАТЕРІАЛАМИ
VII ВСЕУКРАЇНСЬКОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ
СТУДЕНТІВ І АСПІРАНТІВ
24 квітня 2025 року

Київ 2025

УДК 004

Відповідальна за випуск: М.І. Лендєл

Збірник наукових праць за матеріалами VII Всеукраїнської науково-практичної конференції студентів і аспірантів «ТЕОРЕТИЧНІ ТА ПРИКЛАДНІ АСПЕКТИ РОЗРОБКИ КОМП'ЮТЕРНИХ СИСТЕМ '2025», 24 квітня 2025 року, НУБіП України, Київ. – 452 с. (електронне видання)

Відповідальність за зміст публікацій несуть автори.