ОСОБЛИВОСТІ ВИВЧЕННЯ ТЕХНОЛОГІЙ OSINT СТУДЕНТАМИ СПЕЦІАЛЬНОСТІ 125 КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

Чалий І.В., канд. техн. наук, доц.
Левкін А.В., канд. техн. наук, доц.
Бутенко Т.А., канд. екон. наук, доц.
Державний біотехнологічний університет

OSINT (Open Source INTelligence, розвідка за відкритими джерелами) – це потужний інструмент для виявлення та аналізу інформації про кіберзагрози, яка міститься у відкритих джерелах. Завдяки OSINT можна отримати цінні дані для прийняття ефективних заходів з кібербезпеки.

Сучасний інформаційний простір насичений великою кількістю даних, включаючи експертні оцінки щодо кіберзагроз. Ці оцінки, опубліковані у відкритих джерелах, можуть бути використані для виявлення нових загроз, аналізу діяльності кіберзлочинців та розробки ефективних стратегій захисту інформаційних систем. Методи розвідки за відкритими джерелами (OSINT) дозволяють систематично збирати, аналізувати та інтерпретувати цю інформацію для прийняття обґрунтованих рішень у сфері кібербезпеки. Однак, варто зазначити, що аналіз даних з відкритих джерел є складним завданням, яке вимагає застосування спеціальних методів та інструментів [1].

У воєнний час OSINT стає незамінним інструментом для збору розвідувальних даних. Завдяки аналізу відкритих джерел можна отримати критично важливу інформацію для ефективного планування та проведення операцій.

При проведенні OSINT-досліджень у сфері кібербезпеки ми прагнемо отримати відповіді на такі ключові питання:

– Суб'єкт атаки: Хто стоїть за атакою?
– Мотивація: Які причини спонукали здійснити атаку?
– Механізм атаки: Як саме була здійснена атака?
– Структура: Як організована група, що здійснює атаку?
– Інструменти та методи: Які засоби використовують зловмисники?
– Ресурси: Які ресурси залучені до атаки?
– Хронологія подій: Які дії передували та супроводжували атаку?
– Наслідки: Які наслідки мала атака?

Додаткові аспекти, які можна розглянути:

– Тіньова інфраструктура: Які ресурси та сервіси використовують зловмисники для приховування своєї діяльності?

– Взаємозв'язки між різними атаками: Чи є зв'язок між даною атакою та іншими інцидентами?

– Потенційні цілі: Хто може стати наступною жертвою?

Відомо багато публікацій присвячених дослідженню питань OSINT. Серед більш докладних робіт [2-4] виділимо перш за все навчальний посібник Д.В. Ланде "OSINT у кібербезпеці", що вийшов у 2024 році [2]. Він дає повне та докладне розкриття застосуванню OSINT саме у кібербезпеці.

Тематику, що пов'язана з OSINT у кібербезпеці, зараз розглядають у більшості вишів, що готують фахівців з захисту інформації. Ця тема вивчається при вивченні різних дисциплін, інколи матеріал дається в межах спеціальної дисципліни (зазвичай як дисципліна за вибором).

Сучасна вища освіта все активніше використовує для навчання потенціал цифрових технологій. Самостійна робота студентів є невід'ємною частиною навчального процесу, а онлайн-ресурси значно розширюють можливості для її організації. Зокрема вони стають невід'ємною частиною навчального процесу, забезпечуючи студентам широкі можливості для самостійного вивчення дисциплін. Використання онлайн-платформ, електронних бібліотек, навчальних відео та інших інтерактивних ресурсів сприяє розвитку навичок самоорганізації, критичного мислення та пошуку інформації. Це дозволяє студентам більш глибоко зануритися в матеріал, закріпити теоретичні знання та розвинути практичні навички [5,6].

Звернемо увагу, перш за все, на вітчизняний портал HackYourMom. Він цілковито відкритий і містить структуровану й агреговану інформацію для/та від фахівців у галузі інформаційної безпеки, які самі й фінансують власне навчання через Patreon.com/HackYourMom. [7].

Його розділ OSINT Mastery: Навчання та Кібербезпека включає багато можливостей для самостійного навчання для студентів.

Але початківцям в цьому питанні краще розпочати своє знайомство з OSINT за допомогою освітнього серіалу «Школа OSINT» відомого порталу «Дія.Освіта» [8]. Освітній серіал створено Інститутом постінформаційного суспільства за ініціативи Мінцифри для платформи Дія.Освіта. Програма проекту складається з 6 серій та фінального тестування. Матеріал поданий в живій та яскравій формі, та, як показала практика перших використань, дуже гарно сприймається студентами.

Навички, які набувають студенти наступні [8]: «Використання Google dorks, Використання держреєстрів, Деанонімізація особи, Зворотний пошук зображення, Покрокова організація OSINT-розслідування, Пошук геолокації за зображенням, Пошук особистих даних у Google і соцмережах, Пошук погоди в минулому, Робота з Google cache, Робота з Google-мап та Street view для пошуку локації, Робота з Webarchive, Wayback machine, Фактчекінг».

Другий ресурс, який ми застосовуємо при навчанні, онлайн-курс «OSINT – розвідка з відкритих джерел та інформаційна безпека» від дуже відомого порталу «Prometheus».

«Курс розрахований на широку аудиторію, готову долучитися до інформаційної розвідки, підвищити обізнаність у методах розпізнавання дезінформації, адже в умовах війни кожен із нас має дбати про інформаційну безпеку та робити все, аби не дати ворогу перевагу необачним ставленням до даних, які ми публікуємо в мережі». Курс створили фахівці проекту Victory Drones (БФ Dignitas) спільно з партнерськими організаціями: Molfar, Лабораторія цифрової безпеки, Центр Протидії Корупції (ЦПК), YouControl Academy, Центр стратегічних комунікацій та інформаційної безпеки, Вокс Україна – незалежна аналітична платформа [9]. Його тривалість 6 годин. Він

складається з 5 модулів: OSINT, Кібербезпека, SOCMINT та HUMINT, GeoINT та ImgINT, InfoSec та OpSec.

Обидва серіали повністю безкоштовні. Відеолекції, завдання, форум доступні в будь-який час. Ці онлайн-курси розроблені таким чином, що для їх проходження не потрібні спеціальні знання чи навички. Після проходження матеріалів, при успішному тестуванні є можливість отримати сертифікат.

У сучасному світі, де інформація є одним з найцінніших ресурсів, OSINT займає важливе місце. Ця технологія дозволяє системно збирати, аналізувати та інтерпретувати дані з відкритих джерел, що є основою для прийняття обґрунтованих рішень в різних сферах діяльності. Від журналістики та бізнесу до розвідки та кібербезпеки – OSINT надає потужні інструменти для дослідження, аналізу та прогнозування. Постійний розвиток технологій та зростаюча кількість доступних даних сприяють подальшому розширенню можливостей OSINT, роблячи її незамінним інструментом для сучасного суспільства.

У контексті зростаючих кіберзагроз, OSINT став незамінним інструментом для виявлення та аналізу загроз, а також для прийняття проактивних заходів з кібербезпеки. Саме тому доцільно навчити майбутніх фахівців спеціальності 125 Кібербезпека та захист інформації його основним прийомам. Не аби яку допомогу в цьому можуть надати освітній серіал "Школа OSINT" порталу «Дія. Освіта» та онлайн-курс «OSINT – розвідка з відкритих джерел та інформаційна безпека» порталу «Prometheus».

Інформаційні джерела:

1. OSINT як частина системи кіберзахисту (Статті та презентації). URL: [https://x-scif.info/articles-and-literature/metodyka-vyyavlennya-obyektiv-kiberbezpeky-na-bazi-tehnologiyi-osint/].

2. Д.В. Ланде. OSINT у кібербезпеці : навч. пос. / Ланде Д.В. – Київ: ТОВ «Інжиніринг», 2024. – 522 с. ISBN 978-966-2344-97-4.

3. Layton R., Watters P. A. Automating Open Source Intelligence: Algorithms for OSINT. – Elsevier, 2016. — 205 p. — ISBN 9780128029169.

4. Распознавание информационных операций / А. Г. Додонов, Д. В. Ландэ, В. В. Цыганок, О. В. Андрейчук, С. В. Каденко, А. Н. Грайворонская. К. : ООО «Инжиниринг», 2017. 282 с.

5. Онлайн-освіта: як здобувати знання в епоху діджиталізації. URL: [https://bazilik.media/onlajn-osvita-iak-zdobuvaty-znannia-v-epokhu-didzhytalizatsii/].

6. Мегель Ю.Є., Чалий І.В. Використання ресурсів порталу «Дія. Цифрова освіта» для організації самостійної роботи студентів з дисциплін «Вступ до фаху кібернетичної безпеки» та «Основи кібербезпеки» // Механізми забезпечення сталого розвитку економіки: проблеми, перспективи, міжнародний досвід [Електронний ресурс] : матеріали IV Міжнар. наук.-практ. інтернет-конф., 19 травня 2023 р. / Держ. біотехнологічний ун-т. – Харків, 2023. – 344 с.

7. Портал HackYourMom. URL: [https://hackyourmom.com/pro-nas/istoriya-portalu/].

8. «Дія. Освіта». URL: [https://osvita.diia.gov.ua/courses/osint-school].

9. Онлайн-курс "OSINT – розвідка з відкритих джерел та інформаційна безпека" порталу "Prometheus" URL: [https://prometheus.org.ua/course/course-v1:Prometheus+OSINT101+2024_T3].