УДК 65.011.05: 004.056.53

Т.Ю. Приходько
керівник відділу технічної підтримки клієнтів
(ТОВ Інтернет Інвест, Україна)
кандидат технічних наук, доцент
(Національний авіаційний університет, Україна)

OSINT у кібербезпеці цивільної авіації

Кібербезпека в авіації має велике значення через все більше покладання організаціями цивільної авіації на мережеві технології та інформаційні системи для управління польотами, зв'язку, навігації, та підтримки операцій в них. OSINT у контексті кібербезпеки відіграє важливу роль у виявленні потенційних загроз і вразливостей, які можуть вплинути на критичні системи авіаційної інфраструктури.

OSINT (Open Source Intelligence) у сфері цивільної авіації включає збір, аналіз і використання відкритих джерел інформації для виявлення і моніторингу подій, що пов'язані із повітряним транспортом. Це можуть бути дані, отримані з різноманітних відкритих джерел, таких як сайти, публічні бази даних, соціальні мережі, боти в месенджерах типу Telegram та інші.

Джерела OSINT у цивільній авіації

Можна виділити наступні джерела OSINT у цивільній авіації:

Регуляторні органи:

Офіційні сайти, такі як FAA (Federal Aviation Administration) у США або EASA (European Union Aviation Safety Agency) в Європі, надають дані про безпеку, інциденти та авіаційні новини.

Flight Tracking Platforms:

Сайти для відстеження польотів, такі як Flightradar24, FlightAware, Plane Finder або ADS-B Exchange, надають інформацію про рух літаків у режимі реального часу. Ці дані можуть містити реєстраційні номери, типи літаків і авіакомпанії, маршрути.

Авіаційні новини та блоги:

Авіаційні новинні сайти (наприклад, Aviation Herald, Simple Flying, Aviation Week) регулярно публікують оновлення про авіаційні події, інциденти, катастрофи та нові розробки у сфері. Статті та огляди, здебільшого, стосуються комерційної авіації, авіаліній, літаків, космонавтики, оборони та авіаційних технологій.

Бази даних авіакомпаній і літаків:

Відкриті бази даних, як Planespotters, ch-aviation, Airfleets, можуть надавати інформацію про реєстрації літаків, історії літаків і авіакомпанії. Такі бази містить інформацію про авіапарки авіакомпаній, включаючи типи літаків, серійні номери, виробників і статуси (в експлуатації, списані, зберігання).

Сайти аеропортів:

Інформація про заплановані або поточні рейси, стан злітних смуг і умови польотів надається на сайтах аеропортів.

Огляди і дослідження ринку авіації:

Аналітичні звіти щодо комерційної авіації та тенденцій галузі можуть бути публічно доступними через звіти та прес-релізи.

Соціальні медіа:

Платформи на зразок Twitter, Facebook або Instagram часто є джерелами інформації, коли очевидці діляться фотографіями та відео аварій або незвичайних подій.

Використання OSINT

Використання OSINT для потреб в напрямку кібербезпеки в цивільній авіації та авіаційній галузі загалом:

- Безпека: Моніторинг безпеки польотів, виявлення можливих ризиків, спостереження за підозрілими рухами літаків.
- Розслідування інцидентів: Збір інформації про авіаційні інциденти або катастрофи.
- Економічний аналіз: Оцінка тенденцій авіакомпаній, аеропортів і ринків.
- Підтримка авіаційної розвідки: Використання для військових або урядових розвідок.

Напрями OSINT у кібербезпеці цивільної авіації

Можна виділити основні напрями OSINT у кібербезпеці цивільної авіації:

Виявлення вразливостей у системах авіації:

OSINT може використовуватися для вивчення публічно доступної інформації про програмне забезпечення та апаратні системи, які використовуються авіакомпаніями, аеропортами та виробниками літаків. Це може включати пошук відомих вразливостей (наприклад, через бази даних CVE — Common Vulnerabilities and Exposures) або відстеження оновлень для систем навігації, управління польотами тощо.

Моніторинг кіберзагроз та атак:

Використовуючи дані з відкритих джерел, таких як форуми хакерів, соціальні медіа та новини про кіберінциденти, можна отримувати інформацію про потенційні загрози або атаки на авіаційну інфраструктуру. Це допомагає авіакомпаніям та організаціям вчасно реагувати на нові атаки або вразливості. OSINT може виявляти загальнодоступні дані про критичну авіаційну інфраструктуру, такі як відкриті порти, слабкі сервери або застарілі програмні рішення, які можуть стати ціллю для хакерів.

Відстеження атак на інфраструктуру аеропортів:

Системи аеропортів, такі як служби бронювання, реєстрації, управління рейсами та навігація, є потенційними мішенями для кібератак. Використовуючи OSINT, можна ідентифікувати зловмисні дії, такі як фішингові атаки, DDoS-атаки, або злом систем управління.

Розслідування інцидентів у кіберпросторі:

Коли відбувається кібератака на авіаційну компанію або інфраструктуру, OSINT може допомогти зібрати інформацію про хакерські угруповання, методи атак та інші технічні деталі для розслідування інцидентів. Це може включати збір даних із темних веб-ресурсів, де хакери обговорюють свої цілі чи діляться

інструментами для атак. То ж після того як кіберінцидент стався, OSINT допомагає розслідувати джерела атаки, методи та потенційних зловмисників.

Оцінка репутації авіакомпаній та аеропортів:

Моніторинг думок клієнтів: Аналізуючи публічні обговорення у соціальних мережах, форумах, новинних ресурсах і блогах, OSINT може допомогти виявити негативні відгуки або можливі інформаційні кампанії, спрямовані на підрив репутації авіакомпаній.

Відстеження шахрайства: OSINT також може використовуватися для виявлення шахрайських дій щодо продажу квитків або підроблених вебсайтів, що можуть завдати шкоди як репутації, так і кібербезпеці компанії.

Моніторинг регуляторних змін:

Регуляторні вимоги: За допомогою OSINT можна відстежувати зміни в нормативно-правових актах та вимогах щодо кібербезпеки в авіаційній галузі, що допоможе забезпечити дотримання нових стандартів (наприклад, GDPR, FAA регуляції тощо).

Нові стандарти та рекомендації: Постійний моніторинг міжнародних рекомендацій з безпеки, таких як стандарти ICAO або IATA щодо авіаційної безпеки.

Інформація про інциденти з кібербезпеки:

Спеціалізовані платформи, такі як Recorded Future, Shodan, Censys або VirusTotal, дозволяють отримувати інформацію про інциденти з кібербезпеки в реальному часі. Наприклад, за допомогою Shodan можна знаходити відкриті мережеві пристрої, пов'язані з авіаційною інфраструктурою, які можуть бути вразливими до атак.

Фізична і кібернавігація:

Навігаційні системи літака, такі як ADS-B (Automatic Dependent Surveillance–Broadcast) та ACARS (Aircraft Communications Addressing and Reporting System), часто передають незашифровані дані, які можуть бути перехоплені зловмисниками для кібератак або підроблення сигналів.

Приклади кіберзагроз у цивільній авіації

DDoS-атаки: Атаки на вебсайти авіакомпаній або аеропортів можуть призвести до затримок рейсів, скасування польотів або порушень у роботі систем бронювання.

Злом навігаційних систем: Маніпуляція даними ADS-B або ACARS може дозволити зловмисникам змінювати інформацію про місцезнаходження літаків, що ставить під загрозу безпеку польотів.

Атаки на системи управління повітряним рухом: Кібератаки на інфраструктуру управління повітряним рухом можуть впливати на здатність контролерів керувати літаками, що призводить до небезпечних ситуацій.

Висновки

Активне впровадження цифрових технологій для покращення ефективності та конкурентоспроможності своєї роботи у авіаційній галузі призводить до збільшення кількості цифрових пристроїв, точок доступу та ін., які потенційно можуть бути використані для кібератак. Один із напрямків у контексті кіберзахисту є OSINT (Open Source Intelligence), який стає важливим інструментом у попередженні та мінімізації кіберзагроз у цивільній авіації,

дозволяючи оперативно виявляти та реагувати на загрози, попереджати атаки та підвищувати безпеку інфраструктури.

References

1. Dmytro Lande, Ellina Shnurko-Tabakova. OSINT as a part of cyber defense system. Theoretical and Applied Cybersecurity, 2019. – Iss. 1. – pp. 103-108.
2. D. Lande, O. Puchkov, I. Subach, M. Boliukh, D. Nahornyi OSINT investigation to detect and prevent cyber attacks and cyber security incidents // Information Technology and Security, 2021. Vol 9 (2). – pp. 209-218.
3. ATP 2-22.9. Army Techniques Publication No. 2-22.9 (FMI 2-22.9). Open-Source Intelligence. Headquarters Department of the Army Washington, DC, 10 July 2012
4. Yong-WoonHwang,Im-Yeong Lee, Hwankuk Kim, Hyejung Lee, and Donghyun Kim. Current Status and Security Trend of OSINT. Wireless Communications and Mobile Computing, vol. 2022, Article ID 1290129, 14 pages, 2022