НХКЗ національний хакатон з кібер–захисту

ІНФОРМАЦІЙНИЙ ПОСІБНИК

15-19 ЛИСТОПАДА 2021 РОКУ
УКРАЇНА

ПЕРЕДУМОВИ

У серпні 2021 року Президент України Володимир Зеленський затвердив Стратегію кібербезпеки України на 2021–2025 роки. Документ зазначає, що кібербезпека є одним із пріоритетів у системі національної безпеки України. Так, кіберпростір визнано одним із можливих театрів воєнних дій, тоді як кількість і складність кіберзагроз буде лише зростати і поширюватись на всі сфери життєдіяльності.

«Стратегічний оборонний бюлетень України», схвалений рішенням Ради національної безпеки і оборони України від 20 серпня 2021 року та запроваджений в дію Указом Президента України від 17 вересня 2021 року №473/2021, визначає основні напрями реалізації воєнної політики України, стратегічні цілі та очікувані результати розвитку сил оборони.

Однією зі стратегічних цілей розвитку сил оборони є інтегровані оперативні (бойові та спеціальні) спроможності сил оборони, що забезпечують стримування, стійкість і відсіч збройної агресії проти України, протидію гібридним загрозам. Реалізація стратегічної цілі досягається шляхом реалізації завдань, зокрема, досягнення спроможностей щодо провадження протиборства в кіберпросторі, створення системи кібероборони.

Очікуваний результат – використання силами оборони кіберпростору та створення системи кібероборони забезпечують запобігання виникненню воєнного конфлікту та загрози з використанням кіберпростору, підготовку та провадження кібероборони.

Передбачено такі заходи:

- Розвиток спроможностей сил оборони щодо забезпечення кіберзахисту критичної інформаційної інфраструктури держави в умовах надзвичайного і воєнного стану.
- Розширення військової співпраці з НАТО щодо забезпечення безпеки кіберпростору та спільних дій у кіберпросторі.

15–19 листопада 2021 року відбудеться перший національний хакатон з кіберзахисту на основі стандартів та формату хакатону NATO TIDE Hackathon.

Рішення про проведення заходу було ухвалене в результаті успішної участі Державної служби спеціального зв'язку та захисту інформації України в українських оборонних хакатонах та заходах NATO TIDE Hackathon.

Захід організовано Урядовим офісом координації європейської та євроатлантичної інтеграції, Офісом віцепрем'єра з питань європейської та євроатлантичної інтеграції разом з Адміністрацією Держспецзв'язку, Центром стратегічних комунікацій «СтратКом Україна», Проєктом обміну знаннями Україна-НАТО С4 та USAID.

МЕТА

Покращення спроможності складових сектору безпеки і оборони України для забезпечення ефективного кіберзахисту власної інформаційної інфраструктури (критичної інформаційної інфраструктури), проведення превентивних дій щодо виявлення, реагування на кібератаки та інциденти кібербезпеки, а також усунення їх наслідків.

ЦІЛІ

Розробка інноваційних архітектурних рішень, а також програмного забезпечення для реалізації завдань суб'єктами сектору безпеки і оборони України в контексті кіберзахисту.

Створення умов для ефективної взаємодії та подальшого обміну знаннями між талановитою молоддю, професійними експертами з IT-сектору, державних органів України та країн НАТО для знаходження інноваційних рішень, які сприяють розв'язанню нагальних питань кіберзахисту України.

ФОРМАТ.

Національний хакатон з кіберзахисту відповідає формату змагань НАТО TIDE Hackathon.

ВИДИ ЗМАГАНЬ.

Національний хакатон з кіберзахисту пропонує учасникам взяти участь у трьох типах завдань: моделювання, кодування та комбіноване змагання. Учасникам рекомендується обрати тільки одне із завдань. Нижче наведено загальний опис видів змагань, які відповідають формату завдань змагань НАТО.

Завдання на моделювання

передбачає розроблення інноваційних методів, засобів візуалізації, архітектурних моделей або прийомів під задану бізнес-ситуацію

Завдання на програмування

стосується конкретної бізнес-ситуації, що випливає з попереднього завдання на моделювання, та передбачає розроблення новітніх рішень на базі програмного або апаратного забезпечення

Комбіноване завдання –

це поєднання завдання з моделювання та програмування

УЧАСНИКИ ХАКАТОНУ

Професії та навички осіб не обмежуються формальними вимогами. У Хакатоні можуть брати участь архітектори EA / Business / ICT, операційні аналітики, системні інженери, розробники програмного забезпечення, дизайнери, управлінці.

СИНІ КОМАНДИ

Сині команди — це група програмістів-учасників конкурсу з України. Головне завдання синіх команд полягає у тому, щоб вирішувати та презентувати запропоновані конкурсні завдання.

Синя команда повинна:

- взяти участь в основному конкурсі;
- вивчити матеріали для попереднього ознайомлення;
- взяти на рішення одне завдання;
- розробити рішення (окремо окреслені для кожного із завдань);
- презентувати своє рішення.

До складу синьої команди належать:

- керівник команди;
- члени команди.

ЗЕЛЕНІ КОМАНДИ

Зелені команди — це група програмістів з України, НАТО та країн-партнерів НАТО, а також представників сектору безпеки та оборони, які не беруть участі у змаганні. Головна мета зеленої команди полягає у тому, щоб вирішувати та презентувати запропоновані завдання. Зелені команди можуть надавати технічну підтримку синім командам, а також заохочуються консультувати учасників змагань.

Зелені команди повинні:

- вивчити матеріали для попереднього ознайомлення;
- взяти на рішення одне чи більше завдань;
- розробити рішення (окремо окреслені для кожного із завдань);
- презентувати свої рішення;
- консультувати сині команди (повідомляючи білі команди про кожну таку розмову).

До складу зеленої команди належать:

- керівник команди;
- члени команди.

БІЛА КОМАНДА

Біла команда — це контрольна команда, що не бере участі у змаганні. Головним обов'язком білої команди є забезпечення ефективного проведення Хакатону та чесності конкурсу. Білій команді дозволяється обрати одне із завдань та презентувати його рішення. Серед членів цієї команди будуть розробники завдань з моделювання та програмування, відповідальні за проведення змагання, профільні спеціалісти, журналісти та блогери, проєктувальники інфраструктури та адміністратори.

Завдання білої команди:

- забезпечити чесність конкурсу;
- надати необхідну консультацію та професійну допомогу при вирішенні завдань;
- визначити критерії оцінювання та підготувати докладну рейтингову таблицю;
- розробити правила;
- підготувати формат і бланки звітності;
- відстежувати та записувати факти взаємодії між групами;
- спроєктувати, розробити та адмініструвати інфраструктуру;
- спроєктувати та адмініструвати інформаційно-комунікаційну інфраструктуру;
- розробити та виконати стратегію та план комунікацій;
- вивчити матеріали для попереднього ознайомлення;
- взяти до рішення одне чи більше завдань;
- розробити рішення (окремо окреслені для кожного із завдань);
- презентувати свої рішення.

До складу білої команди належать:

- керівник команди;
- відповідальний за проведення змагань;
- розробник конкурсних завдань;
- профільний спеціаліст;
- прес-секретар;
- адміністратори

ЖУРІ

Журі складається мінімум із трьох членів білої команди із правом голосу та її керівника. Керівник білої команди грає роль радника та не має права голосу. Члени журі Хакатону призначаються окремо.

Члени журі повинні:

- розглянути презентовані робочі рішення;
- поставити оцінки продуктам синіх команд;
- обрати переможця серед рішень завдань із програмування, моделювання та комбінованого завдання.

До складу журі належать:

- голова (із правом голосу);
- члени журі з правом голосу;
- керівник білої групи (не голосує).

ПРОГРАМА

ДЕНЬ 1

08:00–09:00
Реєстрація учасників на онлайн-платформі проведення заходу

09:00–09:30
Офіційне відкриття Національного хакатону з кіберзахисту

09:30–10:00
Спільне фото. Спілкування.

10:00–12:30
Вступна частина, презентація завдань

12:30–13:30
Обід

13:30–14:30
Брифінг команд та обговорення завдання №1

14:30–15:30
Брифінг команд та обговорення завдання №2

15:30–16:30
Брифінг команд та обговорення завдання №3

16:30–18:00
Робота над розробленням проєктів

ДЕНЬ 2-4

8:00–16:30
Робота над розробленням проєктів

10:00 – 13:00
Семінар з питань кіберзагроз, безпеки мереж, забезпечення інформації та управління інформацією

ДЕНЬ 5

09:00–11:00
Презентації команд за видами змагань (Сині команди)

11:00–12:00
Засідання журі для визначення переможців у кожному виді змагань

11:00–12:00
Презентація альтернативних рішень командою експертів із зеленої команди

12:00–13.00
Церемонія нагородження переможців та завершення заходу

ДАТА ТА МІСЦЕ ПРОВЕДЕННЯ

Національний хакатон з кібербезпеки відбудеться 15-19 листопада 2021 року в гібридному режимі (онлайн \ офлайн)

Сині, зелені та білі команди працюватимуть онлайн за допомогою відповідних інструментів онлайн-колаборації. Церемонії відкриття та закриття будуть проводитися в офлайн-режимі з прямою трансляцією події для перегляду віртуальними учасниками.

ІНФОРМАЦІЙНІ ПАКЕТИ

Учасникам хакатону буде надано два інформаційних пакети. Початковий інформаційний пакет із Посібником буде розіслано електронною поштою. Уся інформація щодо хакатону буде також доступна на веб-сайті https://nhcs.ua30.gov.ua/. Усім зареєстрованим учасникам буде надана програма семінару та деталі для онлайн-входу.

ВИСВІТЛЕННЯ У ЗМІ ТА В ІНТЕРНЕТІ

Для підтримки заходу будуть задіяні служби комунікацій, преса та спеціалісти зі зв'язків із громадськістю організаторів та складових сектору безпеки і оборони України, що беруть участь у заході, а також ЗМІ.

- На ранніх етапах уся комунікаційна діяльність (взаємодія з пресою, присутність в онлайн-ЗМІ, висвітлення на ТВ/радіо/у друкованій пресі тощо) буде узгоджена з організаціями-учасницями заходу.
- Для комунікаційної підтримки заходу створено сайт https://nhcs.ua30.gov.ua/
- Складові сектору безпеки і оборони України будуть запрошені до поширення інформації про захід через свої веб-сайти та сторінки у соціальних мережах.

ЮРИДИЧНІ АСПЕКТИ

Продукти, які розроблять під час Національного хакатону з кіберзахисту, у тому числі програмний код, візуалізації моделей, самі моделі та методи, залишаться в Open Source та мають відповідати ліцензії (на основі ліцензії Массачусетського технологічного інституту):

«Наступним безкоштовно надається дозвіл будь-якій особі, що отримала копію цих візуалізацій, моделей, методів, програмного забезпечення та супутніх файлів документації (разом «Програмне забезпечення»), поводитися з Програмним забезпеченням без обмежень, у тому числі без обмежень на право користуватися, копіювати, змінювати, об'єднувати, публікувати, розповсюджувати, надавати під субліцензією та/ або продавати копії Програмного забезпечення, а також дозволяти це робити особам, яким надано Програмне забезпечення».

ПРОЦЕС ПІДГОТОВКИ ТА УЧАСТІ У ХАКАТОНІ

Хакатон складається з трьох основних етапів:

- Етап перший — підготовка
- Етап другий — виконання
- Етап третій — завершення

ЕТАП ПЕРШИЙ — ПІДГОТОВКА

ОЗНАЙОМЛЕННЯ

У процесі підготовки всіх учасників закликають вивчити матеріали для попереднього ознайомлення, надані для кожного завдання. Якщо учасник вирішить принести власне програмне чи апаратне забезпечення, щоб поділитися з іншими учасниками, про це слід повідомити організатора Хакатону.

До того ж, учасникам треба переконатися, що їхні робочі пристрої відповідають вимогам політики BYOD (Bring Your Own Device — «принеси свій власний пристрій»).

РЕЄСТРАЦІЯ

Реєстрація команд відбувається на сайті Хакатону https://nhcs.ua30.gov.ua/. Керівник кожної синьої команди повинен зайти на сайт та надати таку інформацію:

- назва команди,
- відомство,
- обраний вид змагань,
- склад команди,
- ПІБ, звання та спеціальність членів команди.

ПІДГОТОВКА ЗАВДАНЬ

Завдання з програмування, моделювання та комбіноване завдання розкриватимуться поступово, щоб забезпечити елемент несподіваності в останні хвилини перед їх виконанням. Опис завдань в основних рисах буде опубліковано на ранньому етапі у початковому інформаційному посібнику.

В остаточному інформаційному пакеті завдання будуть описані більш докладно: буде вказано детальні критерії відбору, приклади можливих рішень та обов'язкові попередні вимоги. Наприкінці, безпосередньо у день хакатону, у завдання учасників буде привнесено елемент несподіваності.

ЕТАП ДРУГИЙ – ВИКОНАННЯ

Виконання завдань хакатону буде розподілене на три частини. Спершу для підготовки до безпосереднього вирішення завдань хакатону буде запропоновано вступні брифінги, після чого пройде основний конкурс та здача продуктів.

ВСТУПНІ БРИФІНГИ

По завершенню налаштування інформаційно-комунікаційної інфраструктури буде проведено вступний брифінг, протягом якого будуть висвітлюватися такі питання:

- офіційне відкриття Хакатону;
- роз'яснення конкурсних завдань;
- роз'яснення правил конкурсу;
- ознайомлення з інформаційно-комунікаційною інфраструктурою та інструментами колаборації;
- інша доречна інформація з логістики;
- запитання та відповіді (Q&A).

ОСНОВНИЙ КОНКУРС

Протягом основної конкурсної частини команди виконуватимуть запропоновані завдання. Під час цього процесу командам дозволено спілкуватися між собою за умови, що це не заважатиме працювати іншим командам.

Учасникам рекомендується дотримуватися «бібліотечних правил».

Організатор Хакатону виступає за таку робочу обстановку:

- Цивілізовані розмови без двозначностей, враховуючи, що учасники можуть не розмовляти чиєюсь рідною мовою.
- Прихильні, відкриті відносини у командах, що надихають кожного її члена та цінують здібності одне одного.
- Доброзичливі, дружні стосунки з іншими учасниками, в яких поважаються протилежні думки, а також цінується внесок кожного учасника.

ОСТАТОЧНА ЗДАЧА ПРОДУКТІВ

Остаточні продукти разом із презентаціями мають зберігатися на спільному сервері згідно з інструкціями, наданими координатором Хакатону.

ЕТАП ТРЕТІЙ — ЗАВЕРШЕННЯ

Після проведення основного конкурсу розпочинається заключний етап, який містить презентацію продуктів, їх оцінювання та нагородження переможців. За результатами конкурсу будуть проведені звітні та контрольні заходи.

ПРЕЗЕНТАЦІЯ ПРОДУКТІВ

Кожній з команд-учасниць буде надано однакову кількість часу на презентацію своїх продуктів. Презентація завершується сесією запитань та відповідей, під час якої кожен член журі матиме змогу поставити свої запитання.

КРИТЕРІЇ ВІДБОРУ ТА ОЦІНЮВАННЯ

Оцінювання остаточних рішень здійснюється на підставі критеріїв відбору, визначених для хакатону. Загальна сума балів, яку може отримати команда, є сумою оцінки за рішення та оцінки за презентацію. Оцінка за рішення становитиме 90% підсумкового рахунку суми балів, тоді як решта рахунку буде відведена на презентацію рішення.

Підсумкова сума балів = оцінка за рішення (90%) + оцінка за презентацію (10%)

Усі рішення оцінюються окремо в межах виду змагань (моделювання, кодування, комбіноване завдання), а переможці обираються з команд із найвищою сумою балів.

ПРИЗИ ТА НАГОРОДИ

І місце у кожному виді змагань

Участь у міжнародному заході чи навчання на курсі в тематиці завдань Хакатону

Призові місця у кожному виді змагань

Дипломи командам-переможцям

Усі учасники

Сертифікати про участь усім учасникам Хакатону

ДЕТАЛІЗАЦІЯ ЗАВДАНЬ ХАКАТОНУ

Національний хакатон із кіберзахисту пропонує учасникам взяти участь у трьох типах завдань: моделювання, програмування та комбіноване змагання. Учасникам рекомендується обрати тільки одне з-поміж завдань. Нижче наведено загальний опис видів змагань.

1. **Кіберзахист об'єктів критичної інфраструктури.** Розробити архітектурні рішення для системи інформаційної безпеки об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури.
2. **Виявлення, реагування та запобігання кібератакам на об'єкти кіберзахисту.** Удосконалити наявне або розробити нове програмне забезпечення для кіберзахисту об'єктів державного та приватного секторів шляхом збору, оброблення, анал ізу та обміну інформацією про кібератаки для оперативного реагування на них.
3. **Добування (збір), оброблення, аналіз і відображення інформації з відкритих джерел (OSINT) для виявлення та запобігання кібератакам і кіберінцидентам.** Удосконалити наявну або запропонувати нову інформаційну технологію для добування (збору), оброблення, аналізу та відображення інформації з відкритих джерел (мережі «Інтернет», соціальних мереж тощо) для виявлення, розслідування та прогнозування кібератак і кіберінцидентів.

ЗАГАЛЬНІ УМОВИ, ВИМОГИ ТА ОБМЕЖЕННЯ

Усі рішення мають використовувати програмне забезпечення з відкритим кодом (Open Source). Заборонено пропонувати загальновідомі та доступні готові рішення. Під час проведення змагань за кожним завданням будуть надані оперативні уточнення, додаткові умови та обмеження.

Командам слід визначити проблему кіберзахисту в межах обраного завдання, рішення якої вони хотіли б продемонструвати. Опис проблеми має відповідати формату:

1. Формулювання проблеми (опишіть проблему з точки зору технічних питань).
2. Негативні впливи (на що негативно впливає проблема).
3. Результати успішного рішення (ключові переваги успішного рішення).

Обмеження щодо вибору проблем:

- має бути пов'язана з кіберзахистом;
- не має бути вже вирішена за допомогою комерційних технологій.

Обмеження рішення:

- має бути інноваційним;
- має використовувати відкритий код;
- повинно мати перспективи впровадження;
- має відповідати вимогам законодавства та стандартам.

ЗАВДАННЯ 1

МЕТА

Розробити архітектурні рішення для системи інформаційної безпеки об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури.

ПОПЕРЕДНІ ВИМОГИ

Під час розроблення рішення керуватись вимогами чинного законодавства України у сфері кіберзахисту.

За основу взяти:

- «Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури», що затверджені постановою Кабінету Міністрів України від 19 червня 2019 р. № 518;
- «Порядок віднесення об'єктів до об'єктів критичної інфраструктури», що затверджений постановою Кабінету Міністрів України від 9 жовтня 2020 р. № 1109;
- Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, National Institute of Standards and Technology, April 16, 2018 (https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf);
- інші нормативні та законодавчі акти.

НАПРЯМКИ РІШЕНЬ

1. управління доступом користувачів та адміністраторів до об'єктів захисту об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури;
2. ідентифікація та автентифікація користувачів та адміністраторів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури;
3. реєстрація подій компонентами об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури та їх періодичний аудит;
4. забезпечення мережевого захисту компонентів та інформаційних ресурсів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури;
5. забезпечення доступності та відмовостійкості компонентів та інформаційних ресурсів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури;
6. перевірка умов використання змінних (зовнішніх) пристроїв та носіїв інформації на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури;
7. перевірка умов використання програмного та апаратного забезпечення об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури;
8. перевірка умов розміщення компонентів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури.

ОЧІКУВАНІ РЕЗУЛЬТАТИ

Концепція (презентація) архітектурного рішення системи інформаційної безпеки об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури.

ЗАВДАННЯ 2.

МЕТА

Удосконалити наявне або розробити нове програмне забезпечення для кіберзахисту об'єктів державного та приватного секторів шляхом збору, оброблення, аналізу та обміну інформацією про кібератаки для оперативного реагування на них.

ПОПЕРЕДНІ ВИМОГИ

Використати документи:

- «Стратегія кібербезпеки України» (запроваджено в дію Указом Президента України від 26 серпня 2021 року № 447/2021);
- Security and Privacy Controls for Federal Information Systems and Organizations, Joint Task Force Transformation Initiative, NIST Special Publication 800-53, Revision 4 (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf);
- Assessing Security Requirements for Controlled Unclassified Information NIST Special Publication 800-171A, June 2018 (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171A.pdf);
- The Inicident Handlers Handbook, SANS Institute, 2021 (https://www.sans.org/white-papers/33901/);
- Traffic Light ProtocoL (TLP) First Standards Definitions and Usage Guidance — Version 1.0 (https://www.first.org/tlp/);
- інші нормативні та законодавчі акти.

Використати стандарти опису та обміну інформацією про кібератаки.

НАПРЯМКИ РІШЕНЬ

1. моніторинг об'єктів кіберзахисту з метою виявлення кібератак;
2. візуалізація індикаторів компрометації (IP-адреси тощо) для аналізу кібератак;
3. отримання та формування даних про кібератаки;
4. виявлення кібератак та кіберінцидентів;
5. оперативний обмін інформацією про кібератаки та кіберінциденти в різнорідному децентралізованому середовищі;
6. автоматизація процедури реагування на кібератаки;
7. організація та контроль функціонування системи запобігання кібератакам на об'єкти кіберзахисту.

ОЧІКУВАНІ РЕЗУЛЬТАТИ

Оригінальне програмне забезпечення з елементами інновацій та/або удосконалене відкрите програмне забезпечення для виявлення, реагування та запобігання кібератакам на об'єкти кіберзахисту.

ЗАВДАННЯ 3 ■

МЕТА

Удосконалити наявну або розробити нову інформаційну технологію для добування (збору), оброблення, аналізу та відображення інформації з відкритих джерел (мережі «Інтернет», соціальних мереж тощо) для виявлення, розслідування та прогнозування кібератак і кіберінцидентів

ПОПЕРЕДНІ ВИМОГИ

За основу взяти:

- Reference Incident Classification Taxonomy, ENISA, January 2018 (https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy);
- NATO Open Source Intelligence Handbook, November, 2001 (http://www.oss.net/dynamaster/file_archive/030201/ca5fb66734f540fbb4f8f6ef759b258c/NATO%20OSINT%20Handbook%20v1.2%20-%20Jan%202002.pdf);
- NATO Open Source Intelligence Reader, 2002 http://www.oss.net/dynamaster/file_archive/030201/254633082e785f8fe44f546bf5c9f1ed/NATO%20OSINT%20Reader%20FINAL%2011OCT02.pdf;
- Open Source Intelligence (OSINT): Issues for Congress, Congressional Research Service, December 5, 2007 (https://fas.org/sgp/crs/intel/RL34270.pdf;
- Open Source Intelligence (OSINT): Issues for Congress, Congressional Research Service, January 28, 2008 (https://web.archive.org/web/20160304031047/http://www.osint.org/crs-report-osint.pdf);
- Open Source Center – U.S. government arm focusing on open source intelligence under the DNI (https://www.opensource.gov/);
- “Open Source Intelligence (OSINT)”. RIS Open Source Intelligence. 2018-05-29. Retrieved 2018-05-29. (http://arnoreuser.com/);
- Arthur S. Hulnick: ‘The Dilemma of Open Source Intelligence: Is OSINT Really Intelligence?’, pages 229–241, The Oxford Handbook of National Security Intelligence, 2010 (https://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780195375886.001.0001/oxfordhb-9780195375886-e-0014);
- ATP 2-22.9 Army Techniques Publication No. 2-22.9 (FMI 2-22.9) Headquarters Department of the Army Washington, DC, 10 July 2012 Open-Source Intelligence (https://irp.fas.org/doddir/army/atp2-22-9.pdf) DISTRIBUTION RESTRICTION: Unlimited Distribution;
- Heather J. Williams, Ilana Blum. Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise. NATIONAL DEFENSE RESEARCH INSTITUTE. Library of Congress Control Number: 2018943942 ISBN: 978-0-8330-9883-2 Published by the RAND Corporation, Santa Monica, Calif., 2018 (https://apps.dtic.mil/sti/pdfs/AD1053555.pdf);

- McLaughlin, Michael (June 2012). “Using open source intelligence for cybersecurity intelligence”. ComputerWeekly.com. Archived from the original on 2018-06-29 (https://www.computerweekly.com/tip/Using-open-source-intelligence-software-for-cybersecurity-intelligence);
- інші нормативні та законодавчі акти.

Використати відкриті джерела інформації для добування інформації про кібератаки та кіберінциденти.

НАПРЯМКИ РІШЕНЬ

1. збір інформації у сфері кіберзахисту (кібератаки, кіберінциденти) з відкритих джерел;
2. оброблення інформації (Text Mining, Information Extraction та ін.) про кібератаки та кіберінциденти, що зібрана з відкритих джерел;
3. аналіз інформації (формування статистики отриманих даних, динаміки публікацій тощо) про кібератаки та кіберінциденти, що зібрана з відкритих джерел;
4. візуалізація результатів аналізу для ухвалення рішення (графіки, цифрові географічні карти, графи взаємозв’язків джерел, персоналій, ключових слів тощо);
5. ранжування отриманих рішень;
6. прогнозування майбутніх кібератак і кіберінцидентів.

ОЧІКУВАНІ РЕЗУЛЬТАТИ

Оригінальне програмне забезпечення з елементами інновацій та/або адаптоване (удосконалене) відкрите програмне забезпечення для добування (збору), оброблення, аналізу та відображення інформації з відкритих джерел для виявлення та запобігання кібератакам і кіберінцидентам.

КРИТЕРІЇ УХВАЛЕННЯ РІШЕНЬ УЧАСНИКІВ

Рішення учасників приймають до розгляду та подальшого оцінювання за умов виконання всіх критеріїв:

- завершеність рішення;
- інноваційний підхід;
- можливість упровадження;
- програмне забезпечення з відкритим кодом (Open Source).

КРИТЕРІЇ ВІДБОРУ

Критерій	Опис	Максимальна кількість балів
Відповідність реальним потребам	Рішення належним чином вирішує первісно сформульовану проблему	30
Інноваційність	У рішенні використано інноваційний підхід до сформульованої проблеми	20
Завершеність та повнота	Рішення стосується одразу всієї проблеми, а не лише якоїсь її частини	20
Можливість упровадження	Рішення має перспективи впровадження в реальних умовах	20
Презентація	Рішення презентоване у зрозумілій, переконливій манері	10
Разом		100

ОРГАНІЗАТОР

Державна служба спеціального зв'язку
та захисту інформації України

СПІВОРГАНІЗАТОР

StratCom Ukraine, співвиконавець,
комунікаційний партнер

ЗА ПІДТРИМКИ

Трастовий фонд
НАТО-Україна С4

Офіс Віцепрем'єра
з питань європейської
та євроатлантичної інтеграції

Посольство США в Україні

Урядовий офіс координації
європейської та євроатлантичної
інтеграції Секретаріату Кабінету
Міністрів України

Проект USAID «Кібербезпека критичної
інфраструктури України»