Таким чином OSINT-розвідка в соціальних мережах, що спрямована на пошук і добування інформації з доступних через мережу інтернет відкритих джерел дає можливість автоматизувати оцінку ЦА для виготовлення матеріалів психологічного впливу та планування психологічних операцій.

Література:

1. Про Стратегію кібербезпеки України: Указ Президента України від 15 березня 2016 року № 96/2016.
2. Грищук Р. В. Основи кібернетичної безпеки : монографія / Р. В. Грищук / за заг. ред. Ю. Г. Даника – Житомир : ЖНАЕУ, 2016. – С. 216-224
3. Світова гібридна війна: український фронт : монографія / за заг. ред. В. П. Горбуліна. – К. : НІСД, 2017. – 496 с.
4. Мелешко Є.В Дослідження методів визначення центральності акторів у соціальних мережах для задач інформаційної безпеки/ Є.В. Мелешко, В.С. Гермак, С.М. Охотний // Системи управління, навігації та зв'язку Кіровоград: Кіровоградський національний технічний університет , 2016 № 4(40) с.67-70 ISSN 2073-7394

Перспективи використання інноваційних інформаційних технологій штучного інтелекту у складі технічних засобів моніторингу як складової системи охорони (оборони) берегових і прибережних споруд державного значення

Симоненков В.М.
старший науковий співробітник;
Науково-дослідний центр ЗС України «Державний океанаріум»
Литвин М.А.
студентка Національного авіаційного університету
Коновець В.І.
кандидат технічних наук, с.н.с.
провідний науковий співробітник;
Науково-дослідний центр ЗС України «Державний океанаріум»

Аналізуючи проблеми безпеки прибережної держави, корисно поглянути на морську сферу через призму просторового ландшафту її розміщення:

95% телекомунікацій світу проходять по підводних кабелях;

90% світової торгівлі переміщується морем;

50% нафти транспортують морським шляхом;

понад 40% населення світу мешкає в межах 100-150 км від узбережжя.

За останні десять-п’ятнадцять років у провідних країнах світу в галузі робототехніки відбулися кардинальні зміни, які пов’язані з масовим виробництвом і випробуваннями у реальних умовах бойових робототехнічних комплексів, у тому числі безпілотних літальних апаратів, наземних мобільних роботів та безекіпажних напівзанурених або підводних апаратів.

Ще вчора завдання створення робототехнічних комплексів, здатних нести бойовий заряд, була прерогативою держав з потужною технологічною базою, але зараз доступність технологій і можливість анонімного замовлення складних компонентів на глобальному комерційному ринку дозволяють виготовляти зразки такої техніки навіть інженерам середнього рівня. Фінансово така робота цілком під силу навіть невеликій групі кіберзлочинців у морський сфері.

Враховуючи те, що такі загрози носять складний та комплексний характер, питання побудови ефективної системи охорони (оборони) об’єктів необхідно вирішувати із застосуванням більш досконалих сучасних та перспективних технічних засобів моніторингу, в першу чергу, у складі відповідних стаціонарних та мобільних робототехнічних комплексів різного призначення.

На думку провідних фахівців світу, перспективні дослідження в області військової робототехніки спрямовані на поетапне нарощування можливостей дистанційно-керованих машин з поступовим виключенням функцій управління і контролю з боку людини-оператора.

З інформаційної точки зору, систему моніторингу обстановки із застосуванням перспективних роботизованих засобів можливо розглядати у вигляді програмно-апаратного комплексу, який призначений для виявлення вторгнень на об’єкти охорони (оборони) або спроб неправомірного доступу.

Зазвичай, до складу такого комплексу, входять:

сенсорна підсистема, яка відповідає за відстеження подій;

підсистема інтелектуального аналізу та виявлення вторгнень, що безпосередньо визначає чи є дана подія загрозою, чи ні;

консоль оператора управління, яка служить для конфігурації робототехнічного комплексу, перегляду виявлених загроз, а також спостереження за функціонуванням системи моніторингу в цілому.

Найважливішою, на наш погляд, є підсистема інтелектуального аналізу та виявлення вторгнень.

Тому зараз доцільно використовувати методи аналізу та виявлення загроз на основі технологій штучного інтелекту, а саме експертні системи та нейронні мережі або їх комбінації. Головною перевагою штучних нейронних мереж є можливість виявлення нових та невідомих видів загроз, що підвищує захищеність усієї системи охорони (оборони) берегових і прибережних споруд державного значення.

До питання вдосконалення державних механізмів боротьби з кіберзлочинністю

Скачкова Т.Ю.
кандидат юридичних наук., доцент
доцент кафедри спеціально-правових дисциплін
Донецького державного університету управління

У своїх дослідженнях Фурашев В.М. надає наступне визначення поняття “інформаційна безпека”: “інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства і держави, за якого запобігається завдання шкоди через:

1. негативний інформаційний вплив за допомогою, в першу чергу, несанкціонованого створення, розповсюдження, використання свідомо спрямованої за визначеною метою неповної, невчасної, невірогідної та упередженої інформації;
2. негативні наслідки застосування інформаційних технологій;
3. несанкціоноване порушення режиму доступу до інформації з подальшим її розповсюдженням та використанням [1, с. 162-169]. Безпеку та захищеність громадян гарантує держава. У ст. 17 Конституції України зазначається, що забезпечення інформаційної безпеки України є найважливішою функцією держави, справою всього Українського народу.

Відкритий та вільний кіберпростір сприяв політичній та соціальній інтеграції в усьому світі. Він знищив бар’єри між країнами, громадами та громадянами, дозволяючи взаємодіяти та обмінюватись інформацією та ідеями по всьому світі. Це забезпечує свободу виразу думки та здійснення основних прав, надаючи сили людям в їхньому прагненні створити більш демократичне суспільство.

Для забезпечення прозорості та свободи використання кіберпростору необхідно, щоб норми права, якими ЄС користується повсякденно, також було застосовано і до кібернетичного простору. Основні права, демократія і верховенство закону повинно бути максимально захищено в кіберпросторі.

Наші свобода та успіх усе більше залежать від надійності та розвитку кіберпростору, який надалі процвітатиме, якщо розвиватимуться приватний сектор і громадянське суспільство. Проте свобода онлайн також вимагає охорони та безпеки. Кіберпростір повинно бути захищено від випадків зловмисних дій та від зловживань, уряди держав відіграють значну роль у забезпеченні вільного та безпечного кіберпростору. Уряди повинні здійснювати захист доступу та відкритості, поважати і захищати основні права в Інтернеті та підтримувати надійність і безпечність Інтернету.

Нині приватний сектор володіє та оперує значною частиною кіберпростору, і тому будь-яка ініціатива в цій сфері може бути успішною тільки при визнанні приватного сектора головним її учасником. Незважаючи на те, що в останні роки цифровий світ надає значну користь, він не став безпечнішим. Випадки вразливості Інтернету, будь то від навмисних чи випадкових дій, зростають тривожними темпами і можуть порушити постачання основних послуг, які ми сприймаємо як належне, наприклад, постачання води, електрики, послуг охорони здоров’я або мобільного зв’язку. Загрози можуть мати різне походження, у тому числі кримінальне, політично вмотивоване, терористичне, у вигляді проплачених певною державою атак, а також природних лих ненавмисних помилок. Отже, ефективний контроль негативних явищ у кібепросторі, таких як злочинність, вимагає набагато інтенсивнішої міжнародної співпраці, ніж заходи боротьби з будь-якими іншими формами транснаціональної злочинності. Проте світова спільнота поки не має в розпорядженні ані міжнародного органу, що спеціально займається інтернет-злочинністю, ані загальносвітового правового інструменту,