Одеський державний університет внутрішніх справ
Кафедра кібербезпеки та інформаційного забезпечення
Факультет підготовки фахівців для підрозділів кримінальної поліції

КІБЕРБЕЗПЕКА В УКРАЇНІ: ПРАВОВІ ТА ОРГАНІЗАЦІЙНІ ПИТАННЯ

International scientific-practical conference
"Cybersecurity in Ukraine: Legal and Organization Issues"

Матеріали
Міжнародної науково-практичної конференції
19 листопада 2021 року

Одеса 2021

Рекомендовано до друку рішенням кафедри кібербезпеки та інформаційного забезпечення
Одеського державного університету внутрішніх справ
(протокол № від грудня 2021 року)

Всі матеріали надані в авторській редакції та виражають
персональну позицію учасника конференції

Кібербезпека в Україні: правові та організаційні питання: матеріали міжн. наук.
К38 практ. конф., м. Одеса, 26 листопада 2020 р. Одеса : ОДУВС, 2021. _____ с.
ISBN 678-717-7020

У збірнику представлено стислий виклад доповідей і повідомлень, поданих на міжнародну науково-практичну конференцію «Кібербезпека в Україні: правові та організаційні питання», яка відбулася на базі кафедри кібербезпеки та інформаційного забезпечення Одеського державного університету внутрішніх справ 19 листопада 2021 року.

У матеріалах конференції приділено увагу актуальним теоретичним та практичним проблемам забезпечення інформаційної безпеки в Україні. Висвітлюється широкий спектр питань, пов'язаних з удосконаленням правового регулювання та адміністративно-правового забезпечення кібербезпеки в Україні. Розглянуто використання інформаційних систем, технологій та інформаційно-аналітична діяльність правоохоронних підрозділів у боротьбі з злочинністю та надано обґрунтовані рекомендації щодо вдосконалення підготовки персоналу для боротьби з кіберзлочинністю в Україні.

Матеріали всеукраїнської науково-практичної конференції адресовано вченим, працівникам правоохоронних органів, аспірантам (ад'юнктам), слухачам магістратури, студентам та курсантам вищих навчальних закладів.

ОЦІНКА ДАНИХ ТА ІНФОРМАЦІЇ АНАЛІТИЧНИМИ ПІДРОЗДІЛАМИ ДЕРЖАВНОЇ ПРИКОРДОННОЇ СЛУЖБИ УКРАЇНИ ДЛЯ ЗДІЙСНЕННЯ ПРОГНОЗУВАННЯ РИЗИКІВ НА СУХОПУТНІЙ ДІЛЯНЦІ ДЕРЖАВНОГО КОРДОНУ

Балтовский О.А.
д.т.н., доцент, професор кафедри кібербезпеки та інформаційного забезпечення ОДУВС
Мільчев А.І.,
студент 2-го курсу ОПП «Кримінальний аналіз» освітній ступінь магістр ОДУВС

В умовах ведення Росією гібридної війни проти України дуже важливо вміти оцінювати данні та інформацію, що надходить з різних джерел. Гібридна війна розгорнута на усіх можливих напрямках. Найважливішим полем боротьби за свідомість громадян став інформаційний простір. Це не лише інформаційна війна, а одночасно й економічна, репутаційна, смислова, людська. Визначено, що «розквіту» інформаційної війни сприяло існування недержавних проросійських ЗМІ, обмеження сепаратистами доступу до українських ЗМІ, подання ворогом інформації як єдиної об’єктивної.

Однією з форм інформаційної боротьби є інформаційна розвідка – пошук, збір, обробка та аналіз інформації про інформаційні ризики і загрози.

Інформаційне та аналітичне забезпечення – це сукупність технологій, методів збору та обробки інформації, що характеризує об'єкт управлінського впливу (соціальні, політичні, економічні й інші процеси), специфічних прийомів їхньої діагностики, аналізу й синтезу, а також оцінки наслідків прийняття різних варіантів управлінських рішень та прогнозів розвитку обстановки.

Кінцевим продуктом інформаційно-аналітичної роботи є аналітичний документ.

Засоби інформаційно-аналітичної роботи становлять собою сукупність інтелектуальних та технологічних засобів, які забезпечують виконання поставленого завдання. Під технологічними засобами інформаційно-аналітичної роботи маються на увазі різноманітні каталоги, інформаційні картки, за допомогою яких формують каталоги (тематичні або алфавітні), інформаційні системи (у тому числі автоматизовані), щоденники (головне завдання – регулярна реєстрація інформації про ті чи інші події), системи інформаційного обслуговування, експертні системи, системи штучного інтелекту тощо.

У свою чергу інтелектуальні засоби інформаційно-аналітичної роботи становлять собою різноманітні відомості (характеристики властивостей об'єкта), дані (факти або відомості, представлені в формалізованому вигляді) та повідомлення. По суті, ми маємо справу з інформацією, тобто фактами, які є основою для прийняття рішень щодо проведення адміністративно-організаційних, політичних та

інших заходів, а також для підготовки різноманітних пропозицій і рекомендацій стратегічного та тактичного характеру.

В державній прикордонній службі України головними видами аналізу ризиків є: періодичний,тематичний, ситуативний, аналіз нетипових випадків.

Періодичний, тематичний і ситуативний аналізи ризиків, а також аналіз нетипових випадків можуть здійснюватися за такими етапами*:*

– визначення мети, опис проблем і визначення переліку необхідної для аналізу інформації;
– збір, оцінка, накопичення та обробка інформації з використанням доступних баз даних;
– складання та синтез інформації, її перевірка;
– аналіз, зіставлення та порівняння інформації, формулювання попередніх висновків;
– розроблення загальних висновків для підготовки гіпотез;
– аналіз системної правильності гіпотез;
– розроблення варіантів рекомендацій;
– презентація та передача результатів аналізу ризиків;
– перевірка правильності та об'єктивності зроблених висновків і проведеного аналізу;
– коригування висновків на підставі нової отриманої інформації.

Передумовою ефективності аналізу ризиків є організація аналітичного процесу, який повинен включати упорядкований оперативний цикл восьми взаємопов'язаних і послідовних елементів, серед яких:

– визначення завдань;
– збирання даних та інформації;
– оцінка (даних та інформації);
– впорядкування (даних та інформації);
– аналіз (даних та інформації);
– презентація результатів аналізу;
– поширення аналітичних документів;
– оцінка результатів.

Детально проаналізувавши елементи оперативного циклу ми дійшли таких висновків.

1. Під час визначення завдань необхідно передбачити:
– вид необхідних даних;
– джерела інформації;
– відповідальних посадових осіб;
– порядок збору та накопичення даних;
– аналітичні методи;
– терміни виконання визначених завдань;
– порядок презентації результатів аналізу;
– поширення результатів аналізу.

2. Збирання даних та інформації має здійснюватися планово й цілеспрямовано, з урахуванням мети і теми аналітичного дослідження.

Порядок збирання даних та інформації для періодичного аналізу ризиків визначається відповідним нормативним актом, наприклад інструкцією з аналізу ризиків, для тематичного аналізу – планом аналітичного дослідження, ситуативного аналізу та аналізу нетипових випадків – запитом на інформацію керівника аналітичного підрозділу або розпорядженням уповноваженої посадової особи.

Для забезпечення ефективного збирання даних та інформації аналітичному підрозділу необхідно надати: доступ до відомчих баз даних (інформаційних масивів), інших правоохоронних органів, міністерств і відомств, міжнародних структур та установ; повноваження щодо запиту на інформацію до структурних підрозділів поліції, інших правоохоронних органів, міністерств і відомств.

До того ж, підрозділ необхідно забезпечити спеціальними програмними продуктами для пошуку й отримання інформації з відкритих джерел, поширення результатів аналізу в структурі правоохоронних органів.

3. Оцінка інформації має забезпечити подальшу її ґрунтовну інтерпретацію. З цією метою доцільно застосовувати методику оцінки інформації 4х4, яку вже тривалий час використовують у межах кримінального аналізу.

Запровадження системи оцінки інформації за методом 4х4 передбачає:

– досягнення єдиного розуміння та тлумачення інформації компетентними посадовими особами

всіх структурних підрозділів;

– застосування компетентними посадовими особами уніфікованої методології та ідентичних критеріїв для оцінки інформації;

– визначення цінності отриманої інформації для прийняття адекватних рішень, проведення оперативних, процесуальних або адміністративних дій;

– приведення форми надання інформації у відповідність до норм, що застосовуються правоохоронними органами країн – членів Європолу.

Упровадження зазначеної методології дає змогу:

застосовувати єдину методологію та ідентичні критерії оцінки інформації, однаково розуміти й інтерпретувати її, унеможливити довільність у цій сфері;

визначати відповідну цінність здобутої інформації та приймати адекватні рішення щодо проведення оперативних, процесуальних чи адміністративних дій;

більш ефективно розвивати обмін оперативною інформацією з іншими правоохоронними органами, які застосовують цей метод;

підвищити рівень достовірності інформації, що передається в межах міжнародної співпраці.

Оцінка інформації за методом 4х4 передбачає окреме оцінювання джерела та змісту інформації.

Це здійснюється згідно з певними критеріями, відповідно до яких кожній інформації, що надходить до компетентних посадових осіб оперативних підрозділів, присвоюють код, що складається з двох частин: результату оцінки джерела (значення A, B, C, D) та результату оцінки інформації (значення 1, 2, 3, 4).

4. Наступний елемент оперативного циклу – упорядкування, під час якого необхідно забезпечити «відсіювання» неправдивих і несуттєвих даних.

На цьому етапі роботи з інформацією аналітик повинен чітко розрізняти поняття «інформація» та «інформаційний шум».

Наприклад, згідно з повідомленням прикордонного наряду «Прикордонний патруль», в районі прикордонного знаку 0000 виявлено та затримано двох громадян Молдови, порушників Державного кордону України. Для відділу прикордонної служби це повідомлення є інформацією, оскільки пов'язане з порушенням законодавства про Державний кордон України, і подальше провадження належить до її повноважень. Для оперативного підрозділу з протидії злочинам у сфері транскордонної злочинності – це інформаційний шум. Водночас, коли під час вивчення обстановки прикордонний наряд повідомить про виявлення в лісопосадці ящиків з цигарками, повідомлення прикордонного наряду набуде для нас статусу інформації.

5. Етап аналізу передбачає:

ґрунтовну інтерпретацію (роз'яснення, тлумачення) інформації;

виявлення індикаторів ризиків, тенденцій, формування висновків, прогнозів;

оцінку загроз, вразливості правоохоронної системи, негативного впливу (як можливого, так і прогнозованого);

співставлення результатів оцінки, виявлення взаємозв'язків між фактами й оцінками, висновками та прогнозами;

здійснення прогнозу розвитку обстановки.

Підбиваючи підсумки, можна констатувати доцільність виокремлення таких видів аналізу ризиків: а) періодичний; б) тематичний; в) ситуативний; г) аналіз нетипових випадків.

Передумовою ефективності аналізу ризиків є організація аналітичного процесу, що повинен передбачати впорядкований оперативний цикл взаємопов'язаних і послідовних елементів: визначення завдань; збирання даних та інформації; оцінку (даних та інформації); впорядкування (даних та інформації); аналіз (даних та інформації); презентацію результатів аналізу; поширення аналітичних документів; оцінку результатів.

Дослідження елементів оперативного циклу дало змогу дійти таких висновків щодо кожного з них:

1. Під час визначення завдань слід передбачити вид необхідних даних; джерела інформації; відповідальних посадових осіб; порядок збору та накопичення даних; аналітичні методи; терміни виконання визначених завдань; порядок презентації результатів аналізу та їх поширення.

2. Збирання даних та інформації має здійснюватися планово і цілеспрямовано, з урахуванням мети й теми аналітичного дослідження.

3. Оцінка інформації має забезпечити подальшу обґрунтовану інтерпретацію інформації (доцільно застосовувати методику оцінки інформації 4х4, яка вже тривалий час використовується в межах кримінального аналізу).

4. Упорядкування, під час якого необхідно забезпечити «відсіювання» неправдивих і несуттєвих даних.

5. Аналіз.

Література:

1. Бокоч, В. М. Релігія в гібридній війні на Сході України // Вісн. Нац. техн. ун-ту України «Київський політехнічний інститут». Політологія. Соціологія. Право. 2017. № 1/2. С. 27–31.
2. «Гібридна» війна Росії – виклик і загроза для Європи / Укр. центр екон. і політ. дослідж. ім. Олександра Разумкова. Київ, 2016. 91 с.
3. Дрогомирецька, В. К. Співробітництво України з міжнародними організаціями у формуванні Європейської безпеки в умовах «гібридної війни» на Сході України / В. К. Дрогомирецька // Прикарпат. вісн. НТШ. Думка. 2018. № 5. С. 195–200.
4. Основи публічної політики та управління: навч. посіб/ авт.кол.: С.О. Телешун, С.В. Ситник, І.В Рейтерович, О.Р. Титаренко, С.І Вировий. К.: НАДУ, 2011. 312 с.
5. Розвиток системи кримінального аналізу та аналізу ризиків, сумісної зі стандартами ЄС в структурах правоохоронних органів України які протидіють злочинам, що пов'язані з торгівлею людьми. Київ : МВС України, 2015. 92 с.