джерел, застосування коефіцієнтів (ваги) до кожної інформації та грамотний аналіз отриманої інформації. Детально про методи OSINT можна ознайомитись в літературі Е. Ющука [4], Дороніна [5], а також в матеріалах, представлених в блогах, роликах і презентаціях таких експертів, як Д. Золотухін [6], А. Масалович [7], А. Лукацький [8] та інших.

Варто відзначити, що при роботі з великими обсягами даних можуть використовуватися системи підтримки прийняття рішень (СППР). СППР виконують 2 основні завдання, до яких відносяться вибір найкращого рішення з безлічі можливих (оптимізація) та впорядкування можливих рішень за перевагами (ранжування). Правильний вибір ССПР залежить від цілей, задач та обраних критеріїв (універсальність або сегментованість рішення). До найбільш розповсюджених ССПР відносяться такі ПЗ, як ICEBERG, PMS, FOCUS, CIS, PIMS, ISDS, MAUD, Экспресс, Симплан, Прожектор тощо [2].

Список використаних джерел:

1. Стайкуца С. В. Стратегия выживания / Сергей Владимирович Стайкуца. // Бизнес и безопасность. – 2016. – С. 32–33.

2. Стайкуца С. В. Методи і технології підтримки прийняття рішень / С. В. Стайкуца, М. С. Івахненко. // Радіоелектроніка та молодь у XXI столітті. – 2017. – С. 99–100.

3. Саука К. Инструменты и методы получения данных в конкурентной разведке [Електронний ресурс] / Кеннет Саука // Элитариум. – 2016. – Режим доступу до ресурсу: http://www.elitarium.ru

4. Ющук Е. Интернет-разведка. Руководство к действию / Евгений Ющук. – Москва: Издательство деловой литературы «Вершина», 2006.

5. Доронин А. И. Бизнес-разведка, 5-е издание / А. И. Доронин. – Москва: Ось-89, 2009. – 245 с.

6. Конкурентная разведка [Електронний ресурс] // Сайт Дмитрий Золотухина – Режим доступу до ресурсу: http://razvedka.in.ua/

7. Масалович А. И. Конкурентная разведка на основе Интернет [Електронний ресурс] / Андрей Игоревич Масалович // SlideShare. – 2015. – Режим доступу до ресурсу: http://www.slideshare.net/ArtemAgeev/ss-45875484.

8. Бизнес без опасности [Електронний ресурс] // Блог Алексей Лукацкого – Режим доступу до ресурсу: http://lukatsky.blogspot.com/.

Ярмола В.Г.

студент,
Навчально-науковий інститут інформаційної безпеки,
Національна академія Служби безпеки України

ПРОБЛЕМНІ АСПЕКТИ ВИЗНАЧЕННЯ ПОНЯТТЯ «КІБЕРБЕЗПЕКА»

Кібербезпека виникає у сферах інформаційної та традиційної безпеки для боротьби з різким зростанням кіберзлочинності та в деяких випадках за наявності ознак кібервійни. Кібербезпека охоплює захист інформаційних активів шляхом боротьби зі загрозами безпеці інформації, яка обробляється,

зберігається та передається в інформаційних системах, об'єднаних за допомогою мереж [1].

Повсюдна широкосмугова мережа, бізнес і суспільство, орієнтовані на ІТ, та соціальна стратифікація навичок використання ІТ змінюють традиційне середовище ІТ з централізованим контролем та управлінням на відкритий світ, де всі користуються багатьма пристроями, із розмитими межами між діловим та особистим. Водночас багато ділових операцій уже позбавлені нецифрових (паперових або очних) альтернатив. Такі зміни супроводжуються появою на світовому ринку нового покоління користувачів пристроїв. Це нове покоління має кардинально інше бачення безпеки та більш схильне до переважаючої довіри та розповсюдження ідей, поданих в чисельних соціальних мережах, на платформах для обміну та в інноваційних пропозиціях послуг [1].

Для боротьби з кіберзлочинністю та у відповідь на соціальні зміни багато урядів та установ запустили ініціативи в галузі кібербезпеки, починаючи з настанов і стандартизації та закінчуючи комплексним законодавством і регуляторними актами [1].

Європейські закони та регуляторні акти з кібербезпеки, як правило, суворіші в тих галузях, які регулюються або класифікуються як критична інфраструктура, на відміну від нерегульованих галузей. Однак, наявність правових норм чи регуляторних актів є не єдиною рушійною силою кібербезпеки. У деяких галузях кіберзлочинність, кібервійни та промисловий шпіонаж спостерігаються частіше, ніж в інших [2].

Протягом останніх років традиційна інформаційна безпека постала перед викликом зародження та швидкого росту рівня кіберзлочинності та кібервоєн. Порушення безпеки почалися з непередбачуваних атак окремих осіб і переросли в цільові атаки, які часто відносять до організованої злочинності або актів агресії між національними державами. ЄС і його держави-члени запускають широкомасштабні програми та ініціативи для посилення кібербезпеки у відповідь на виклики, пов'язані зі захистом ініціатив із кібербезпеки, у тому числі:

• агентство ENISA , засноване у 2004 році, що спершу надавало настанови та рекомендації з інформаційної безпеки, а згодом розширило сферу своєї діяльності на вирішення питань кібербезпеки;

• Стратегію кібербезпеки, видану Європейською комісією, на якій ґрунтується низка національних стратегій;

• цілу низку заходів, пов'язаних із кібербезпекою, в галузі науково-дослідних робіт, регулювання та управління в ЄС і його державах-членах, наприклад:

- директиву щодо мережевої та інформаційної безпеки;
- програму з досліджень і розвитку Горизонт 2020;
- міжорганізаційну та міжнародну співпрацю в галузі політики та правоохоронних систем;
- 14 дій з кібербезпеки у Цифровому порядку денному для Європи [2].

Для аналізу, координування та застосування цінної інформації, наведеної в усіх цих джерелах, підприємства потребують настанов із практичного

впровадження кібербезпеки в європейському контексті. Для забезпечення цінної цільової інформації про впровадження кібербезпеки Серія документів про впровадження європейської кібербезпеки використовує загальновизнані підходи та стандарти [3].

Термін «кібербезпека» стосується процесу корпоративного управління, менеджменту та надання впевненості щодо безпеки, які виходять за межі стандартної інформаційної безпеки. Кібербезпека зосереджується на особливих формах складних атак та охоплює їх технічний і соціальний аспекти. Оскільки існує багато визначень кібербезпеки, цей термін часто розуміють неправильно. Офіційне визначення ЄС наступне:

Кібербезпека зазвичай стосується заходів і дій, спрямованих на захист кіберпростору в цивільній і військовій сферах від загроз, які можуть завдати шкоди взаємозалежним мережам та інформаційній інфраструктурі або є пов'язаними з ними. Кібербезпека спрямована на збереження доступності та цілісності мереж та інфраструктури, а також конфіденційності інформації, яка міститься в них. ISACA дає наступне визначення кібербезпеки:

Захист інформаційних активів шляхом боротьби зі загрозами безпеці інформації, яка обробляється, зберігається та передається за допомогою інформаційних систем, що взаємодіють за допомогою мереж [3].

У своїй публікації Трансформація кібербезпеки ISACA описує кібербезпеку детальніше:

Кібербезпека охоплює все, що захищає організації та фізичних осіб від умисних атак, порушень, інцидентів і їх наслідків. На практиці кібербезпека насамперед стосується тих типів атак, порушень та інцидентів, які є цільовими, високотехнологічними та складними у виявленні чи управлінні. Кібербезпека зосереджується на так званих складних спрямованих постійних загрозах APT (advanced persistent threats) – спрямовані постійні загрози, кібервійнах і їх впливі на організації та людей.

Організації повинні вміти розрізняти стандартну інформаційну безпеку (нижчого рівня) та кібербезпеку. Різниця полягає в масштабах, мотивах, можливостях і методах атак. Кібербезпека повинна зосереджуватися на APT, щоб бути в змозі вжити низку чітких цільових заходів і дій із кібербезпеки.

Крім сфери кібербезпеки, яка описана у визначеннях і зосереджена на певних видах загроз, ризиків та атак, кібербезпеку слід розглядати також з урахуванням міжнародновизнаних рівнів загроз, визначених державами або наднаціональними установами.

Незважаючи на будь-яке узгоджене визначення кібербезпеки, завдання залишається незмінним: організації повинні встановити чіткі межі між стандартною інформаційною безпекою та кібербезпекою. Щодо першої часто встановлюються бюджетні та ресурсні обмеження; остання стосується високоінтелектуальних атакуючих сторін, які мають мотив, можливості та часто вражаючі навики. Затверджуючи корпоративне визначення кібербезпеки, необхідно враховувати ці факти.

Основне завдання організацій – зачинити «вікно можливостей» перед атакуючими; Cisco продемонструвала черговий рекорд за часом виявлення загрози – 13 годин.

За даними підготовленого компанією Cisco звіту з інформаційної безпеки за перше півріччя 2016 року (Midyear Cybersecurity Report, MCR), організації не готові до появи нових різновидів витончених програм-вимагачів. Нестабільна інфраструктура, погана мережева гігієна, низька швидкість виявлення – все це забезпечує зловмисникам можливість довгий час діяти приховано. Отримані результати говорять про те, що основні труднощі компанії відчувають при спробах обмежити оперативний простір атакуючих, і це ставить під загрозу всю базову структуру, необхідну для цифрової трансформації. Також в звіті наголошується розширення сфери активності зловмисників за рахунок атак на сервери, зростаюча витонченість атак і застосування шифрування для маскування зловмисної діяльності [4].

Список використаних джерел:

1. http://www.ey.com/gl/en/services/advisory/ey-global-information-security-survey-2015-1.
2. (EUROPOL) http://www.europol.europa.eu
3. http://biz.censor.net.ua/m9622
4. ENISA (TheEuropeanNetworkandInformationSecurityAgency) – Європейське агентство з питань мережевої та інформаційної безпеки http://www.enisa.europeu