На правах рукопису

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Одеська національна академія харчових технологій
Навчально-науковий інститут комп`ютерних систем і технологій
"Індустрія 4.0" ім. П.М. Платонова
Факультет Комп`ютерної інженерії, програмування та кіберзахисту

XIX Всеукраїнська науково-технічна конференція молодих вчених, аспірантів та студентів

“СТАН, ДОСЯГНЕННЯ І ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ”

Матеріали конференції. Частина 1

Одеса
22 квітня 2019 р.

Стан, досягнення і перспективи інформаційних систем і технологій / Матеріали XIX Всеукраїнської науково-технічної конференції молодих вчених, аспірантів та студентів. Одеса, 22 квітня 2019 р. - Одеса, Видавництво ОНАХТ, 2019 р. - 84 с.

Збірник включає матеріали доповідей її учасників, які об'єднані по секціях кафедр: комп'ютерної інженерії (КІ), інформаційних технологій та кібербезпеки (ІТтаКБ).

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Організаційний комітет

Голова – д.т.н., проф., **Єгоров Б.В.**, ректор ОНАХТ.

Співголови:

Поварова Н.М. – к.т.н., доц., проректор з наукової роботи ОНАХТ,

Котлик С.В. – к.т.н., доц., директор ННІКСіТ "Індустрія 4.0" ОНАХТ,

Даріуш Долива, д.математичн.наук, уповноважений декана факультету Інформатики УІтаПЗ, м. Лодзь, Польща,

Ковалюк Т.В. - к.т.н., доц. кафедри АСОІтаУ НТУУ «Київський політехнічний інститут».

Члени оргкомітету:

Плотніков В. М. – д.т.н., проф., завідувач кафедри ІТтаКБ ОНАХТ,

Артеменко С.В. – д.т.н., проф., завідувач кафедри КІ ОНАХТ,

Князєва Н.О. – д.т.н., проф. кафедри КІ ОНАХТ,

Хобін В.А. – д.т.н., проф., завідувач кафедри АТПтаРС ОНАХТ,

Тарасенко В.П. – д.т.н., проф., завідувач кафедри СКС НТУУ «Київський політехнічний інститут»,

Невлюдов І.Ш. – д.т.н., проф., завідувач кафедри КІТАМ ХНУРЕ,

Мельник А.О. – д.т.н., проф., завідувач кафедри ЕОМ НУ "Львівська політехніка",

Жуков І. А. – д.т.н., проф., завідувач кафедри КСтаМ НАУ.

Матеріали подано українською, російською та англійською мовами.

Редактор збірника Котлик С.В.

ВИКОРИСТАННЯ МОДЕЛІ ЕНДСЛІ ДЛЯ РОЗРОБКИ СИСТЕМ КІБЕР-СИТУАЦІЙНОЇ ОБІЗНАНОСТІ

Тимошенко Л.М., Єрьоменко А.І.
Одеський національний політехнічний університет

Термін «ситуаційна обізнаність» з'явився у військовій галузі ще під час Першої світової війни, але з розвитком технологій він набуває подальшого розвитку. Це означає можливість отримання досить повного і точного набору необхідної для прийняття рішення інформації про ситуації в реальному часі, у тому числі характер і особливості місцевості, дані про противника та свої війська тощо [1,2]. Такий комплексний підхід у володінні ситуацією актуальний в різних областях, де є великий обсяг інформаційних потоків і високий ступінь ризику, зокрема, в кібер-просторі. Побудова автоматизованого механізму виявлення створить картину ситаційної обізнаності в кібер-просторі для керівників різних рівнів.

Згідно моделі Ендслі (Endsley) стан ситуаційної обізнаності є результатом процесу аналізу та оцінки ситуації (рис. 1) [3].

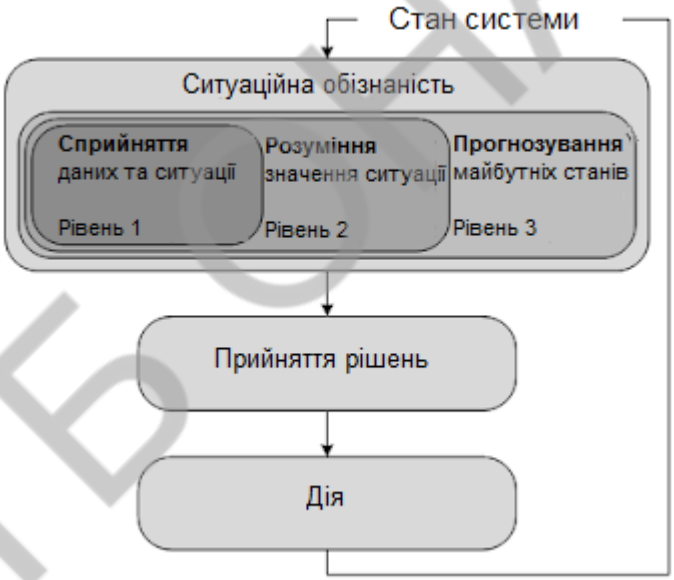

Рис.1 - Модель Ендслі

Сьогодні перед керівником відділу безпеки будь-якої організації стоять наступні ключові завдання: визначення цілей і пріоритетних напрямків роботи по забезпеченню безпеки організації; розробка і впровадження стратегії безпеки, що відповідає бізнес-задачам організації; забезпечення дотримання політик безпеки.

Необхідною умовою ефективного вирішення цих завдань є глибоке володіння інформацією в реальному часі, тобто ситуаційна обізнаність. Інструментом фахівця для ефективного управління безпекою організації, є системи ситуативного інформування про стан системи підтримки прийняття

рішень. Базовий алгоритм реалізації системи включає три етапи: підготовка даних, аналіз даних, візуалізація [4].

Результатом роботи такої системи є комплексне представлення різнорідної інформації в єдиній системі з метою забезпечення ефективного управління. Керівникам служб безпеки немає необхідності знати технічні деталі, наприклад, кількість виявлених вірусів, але важливо розуміння, чи існують загрози щодо бізнесу в рамках допустимих меж. У будь-якій організації комплекс засобів забезпечення інформаційної безпеки дуже широкий. Тому складною і важливою задачею системи ситуативного інформування є злиття різнорідних даних з метою підвищення якості оцінок стану і прогнозів. Особливість процесу злиття - отримання нової якості даних при скороченні їх об'єму. Для цього пропонується використати модель злиття даних, запропоновану робочою групою міністерства оборони США Joint Directors of Laboratories (JDL) [5]. Модель JDL включає п'ять рівнів обробки інформації. Результати злиття даних представляють у вигляді спеціальних діаграм, звітів, повідомлень про небезпечні ситуації згідно основних вимог моделі.

Очевидно, що забезпечення ситуаційної обізнаності має стати важливим напрямком інтересів фахівців, які керують безпекою великих організацій. Для цього доцільно використати модель Ендслі для розробки системи кібер-ситуаційної обізнаності, зокрема моделювання критичних ситуацій, у тому числі виявлення можливих майбутніх нападів.

1. Х. І. Микіч, Є. В. Буров. Дослідження причин виникнення невизначеностей у системах із ситуаційною обізнаністю та аналіз методів їх опрацювання // Восточно-европейский журнал передовых технологий. - 2016. - N 1 / 4 (79). - С. 19-27.
2. Ian Murphy. Cyber Security Situational Awareness // Digital Forensic. - №6. - 2011. [Електронний ресурс]. – Режим доступу: https://www.digitalforensicsmagazine.com/index.php?option=com_content&view=article&id=574&Itemid=99
3. Endsley M. R. Toward a theory of situation awareness in dynamic systems // Human Factors: The J. of the Human Factors and Ergonomics Society. – 1995. - № 1. - С. 32-64.
4. Jared Holsopple, Shanchieh Jay Yang. FuSIA: Future Situation and Impact Awareness // IEEE International Conference on Information Fusion – 2008. (July 1-3). - Cologne, Germany, 2008. [Електронний ресурс]. – Режим доступу: https://mafiadoc.com/fusia-future-situation-and-impact-awareness-citeseerx_59c5c2011723dd3dade29097.html
5. Erik P. Blasch, Susan Plano. JDL Level 5 fusion model: user refinement issues and applications in group tracking // Aerosense. - 2002. – С. 270-272. [Електронний доступ]. – Режим доступу: https://www.researchgate.net/publication/269071694_JDL_level_5_fusion_model_User_refinement_issues_and_applications_in_group_tracking