НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ
Науково-навчальний центр прикладної інформатики

ІНСТИТУТ ІННОВАЦІЙНОЇ ОСВІТИ

ІННОВАТИКА В СУЧАСНІЙ ОСВІТІ ТА НАУЦІ: ТЕОРІЯ, МЕТОДОЛОГІЯ, ПРАКТИКА

МАТЕРІАЛИ
III Міжнародного літнього наукового симпозіуму

24–25 липня 2020 р.
м. Одеса

Одеса
Інститут інноваційної освіти
2020

УДК 001(063):378.4 (Укр)
ББК 72я43
І66

До збірника увійшли матеріали наукових робіт (тези доповідей, статті), надані згідно з вимогами, що були заявлені на конференцію.

Роботи друкуються в авторській редакції, мовою оригіналу.
Автори беруть на себе всю відповідальність за зміст поданих матеріалів.
Претензії до організаторів не приймаються.
При передруку матеріалів посилання обов'язкове.

І66 **Інноватика в сучасній освіті та науці: теорія, методологія, практика :** Матеріали ІІІ Міжнародного літнього наукового симпозіуму (м. Одеса, 24–25 липня 2020 р.) / ГО «Інститут інноваційної освіти»; Науково-навчальний центр прикладної інформатики НАН України. – Одеса : ГО «Інститут інноваційної освіти», 2020. – 108 с.

Матеріали конференції рекомендуються освітянам, науковцям, викладачам, здобувачам вищої освіти, аспірантам, докторантам, студентам вищих навчальних закладів тощо[1].

Відповідальний редактор: *С.К. Бурма*
Коректор: *П.А. Немкова*

Матеріали видано в авторській редакції.

УДК 001(063):378.4 (Укр)

Підписано до друку 31.07.2020. Формат 60х84/16.
Віддруковано з готового оригінал-макету.
Папір офсетний. Друк цифровий. Гарнітура Charter. Ум. друк. арк. 6,28.
Зам. № 3107/20-10. Тираж 100 прим. Ціна договірна. Виходить змішаними мовами: укр., анг.

Виготівник. ФОП Москвін А.А. Цифрова друкарня «Copy Art».
69095, Запоріжжя, просп. Соборний, 109. Тел.: (061) 708-08-80
Інститут інноваційної освіти: e-mail: novaosvita@gmail.com; сайт: www.novaosvita.com

Видання здійснене за експертної підтримки
Науково-навчального центру прикладної інформатики НАН України
03680, Київ-187, просп. Академіка Глушкова, 40.

[1] *Відповідає п. 12 Порядку присудження наукових ступенів Затвердженого Постановою Кабінету Міністрів України від 24 липня 2013 р. № 567; п. 28 Постанови Кабінету Міністрів України від 30 грудня 2015 р. № 1187 «Про затвердження Ліцензійних умов провадження освітньої діяльності»; п. 13 Постанови Кабінету Міністрів України від 12 липня 2004 р. № 882 «Про питання стипендіального забезпечення»*

Розділ 8

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

УДК 004.832

В.А. Стороженко,
здобувач вищої освіти ступеня бакалавра,
факультет інформаційних технологій та комп'ютерної інженерії,
Вінницький національний технічний університет
А.В. Дудатьєв,
кандидат технічних наук, доцент, доцент кафедри захисту інформації,
Вінницький національний технічний університет

ІНФОРМАЦІЙНО-АНАЛІТИЧНИЙ ЦЕНТР УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ

Анотація. Проведено аналіз сучасного стану питання використання інформаційно-аналітичних центрів, розглянуто використання аналітичних центрів. Визначено основні задачі та розроблено багаторівневу структуру інформаційно-аналітичного центру, приведено аналітичний опис залежностей, що формалізує зв'язок вихідних параметрів з вхідними.

Ключові слова: кібербезпека, інформаційно-аналітичний центр.

Вступ. В сучасних умовах досить актуальним стає підвищення ефективності управління кібербезпекою держави регіонів корпораціями та підприємствами [1]. Це обумовлено ускладненням сучасних управлінських завдань, їх багатоаспектністю і багатокритеріальністю, збільшеним потоком керуючих впливів, що виходять з державних, регіональних і місцевих органів влади. У сфері управління підвищився обсяг інформаційного обміну та його динаміка. Загострилася необхідність оперативного і адекватного реагування на економічні, соціально-політичні ситуації в країні і за кордоном [2]. Однією з особливостей управлінської праці є постійна необхідність прийняття рішень в умовах дефіциту часу. Процес вироблення і прийняття рішень в системі управління за суттю є інформаційним процесом. Рішення – це "згусток" інформації, спеціально зібраної, проаналізованої і опрацьованої суб'єктом управління. Рішення інформаційне за своєю сутністю, при чому являє собою констатацію нинішнього стану системи, синтез інформації про сьогоднішній день з

інформацією про майбутнє, яке виражене у меті, яка поставлена перед системою [3].

Результати дослідження. Після проведення аналізу відомих інформаційно аналітичних центрів було розроблено структуру інформаційно аналітичного центру управління кібербезпекою [4–5]. Структура інформаційно аналітичного центру побудована на основі лінійно функціональної структури, Лінійно-функціональна структура реалізує принцип єдиноначальності, лінійної побудови структурних підрозділів і розподілу функцій управління між ними і раціонального поєднання централізації і децентралізації. Типовими рівнями управління в лінійно-функціональній структурі виступають:

* вищий – рівень (генеральний директор, директор, президент). Діяльність керівника Державного ІАЦ обумовлена цілями і стратегіями розвитку системи в цілому. На цьому рівні реалізується велика частина зовнішніх зв'язків. Тут велика роль особистості та її професійних якостей;

* середній – рівень, який об'єднує керівників Регіональних ІАЦ та їх апарат. Керівники середньої ланки вирішують завдання, що випливають з функціональної специфіки;

* нижчий – рівень, який об'єднує керівників низової ланки, що знаходяться безпосередньо над виконавцями. Керівників нижчої ланки називають операційними. Вони відповідальні за забезпечення Інформаційної безпеки на підприємствах. Комунікації тут переважно внутрішньо групові та між групові.

При такій структурі управління всю повноту влади бере на себе лінійний керівник, очолює певний колектив. Йому при розробці конкретних питань і підготовці відповідних рішень, програм, планів допомагає спеціальний апарат, що складається з функціональних підрозділів (управлінь, відділів, бюро тощо). У даному випадку функціональними підрозділами виступають Спеціалісти з ІАЦ. Всі співробітники є спеціалістами з інформаційної безпеки і поділяються за обов'язками, спеціалісти що працюють на підприємствах в відділах кібербезпеки забезпечують інформаційну безпеку на підприємстві та збір даних по загрозах .Спеціалісти що працюють в ІАЦ займаються аналізом, структуризацією даних , прийняттям рішень. Перевагами такої структури є глибока підготовка рішень і планів, пов'язаних зі спеціалізацією працівників. Звільнення головного лінійного керівника від глибокого аналізу проблем. Можливість залучення консультантів і експертів. Поєднання переваг лінійної та функціональної структур.

Аналіз видів управлінської діяльності дозволяє визначити завдання, які вирішуються в організації, і виконавців цих завдань. За ступенем інтелектуальності і складності завдання можна класифікувати [7]:

Перший клас – найбільш прості завдання, які складаються з повністю формалізованих процедур і виконання яких, крім витрат часу, не становить ніякої складності для виконавців. Ці завдання стандартизуються і програмуються. До них відносяться контроль і облік, оформлення документів, їх тиражування, розсилка та ін. Такі завдання вирішуються практично всіма автоматизованими інформаційними системами.

Завдання цього класу, якщо вони використовуються для прийняття рішень, називаються завданнями прийняття рішень в умовах повної визначеності. При цьому випадкові і невизначені чинники відсутні.

Другий клас – більш складні завдання: прийняття рішень в умовах ризику, тобто в тому випадку, коли наявні випадкові чинники, для яких відомі закони їх впливу. Постановка і вирішення таких завдань можливі на основі методів теорії ймовірностей, аналітичного та імітаційного моделювання.

Третій клас завдань складають слабко структуровані завдання, які містять невідомі або не вимірювані компоненти (кількісно не оцінювані). Для цих завдань характерна відсутність методів розв'язання на основі безпосереднього опрацювання даних. Постановка завдань базується на прийнятті рішень в умовах неповної інформації. У ряді випадків, на основі теорії нечітких множин і застосувань цієї теорії вдається побудувати формальні схеми рішення.

Четвертий клас завдань складають завдання прийняття рішень в умовах протидії або конфлікту (наприклад, необхідно враховувати наявність активно діючих конкурентів). У завданнях цього класу можуть бути наявні випадкові чинники, для яких невідомі закони їх впливу. Постановка і вирішення таких завдань можливі (але не завжди) методами теорії ймовірностей, нечітких множин і теорії ігор.

П'ятий клас – найбільш складні завдання прийняття рішень, які характеризуються відсутністю можливості формалізації через високий ступінь невизначеності. До таких завдань відноситься більшість проблем прогнозування та перспективного планування.

Процеси прийняття управлінських рішень посідають центральне місце в структурі управлінської діяльності виробничо-економічних систем, оскільки саме вони найбільшою мірою визначають зміст цієї діяльності та її результату, то на їх ефективності суттєво відбивається недостатність науково-методичного забезпечення управлінського персоналу підприємств з питань підготовки та прийняття управлінських рішень в системі функціонування та розвитку підприємств [6].

Ситуаційний центр управління інформаційною безпекою (Security Operation Center, SOC) – комплекс, призначений для централізованого збору та аналізу інформації про події, що надходять з різних джерел автоматизованої системи підприємства. Впровадження ситуаційного

центру управління інформаційною безпекою дозволить не тільки контролювати всі події, що відбуваються в інформаційній системі, а й забезпечити своєчасне реагування на інциденти ІБ, а також запобігання їх у майбутньому.

Процес створення ІАЦ управління інформаційною безпекою складається з декількох етапів:

– обстеження;
– проектування;
– впровадження програмно-технічної частини центру;
– технічний супровід центру.

ІАЦ складається з трьох частин: програмно-технічної, документаційної та кадрової. Програмно-технічні компоненти реалізуються на основі спеціалізованих систем моніторингу подій інформаційної безпеки. У західній термінології дані системи позначаються абревіатурою SIM (Security Information Management) або SIEM (Security Information and Event Management). Одним із прикладів подібних систем є продукт ArcSight ESM, який займає одну з лідируючих позицій в даній області [7].

Висновки. У ході розробки структури інформаційно-аналітичного центру управління інформаційною безпекою визначено необхідність створення ІАЦ, проаналізовано та визначено основні задачі інформаційно-аналітичного центру й можливостей його використання, розроблено структуру ситуаційного центру, запропоновано такі ієрархічні рівні, як: моніторинговий, аналітичний та управлінський, а також визначено конкретні завдання, що вирішуються на відповідних рівнях. Побудовано структуру інформаційно-аналітичного центру управління інформаційною безпекою, представлено аналітичний опис структури, що формалізує зв'язок вихідних параметрів з вхідними. Визначено ієрархічні рівні центру. Визначено особливості процесу створення та принципів побудови ІАЦ.

Список використаних джерел

1. Методичні вказівки до проведення практичних занять та до виконання самостійної й індивідуальної роботи з дисципліни „Основи науково-дослідної роботи / Укладачі: А. О. Азарова, В. В. Карпінець. – Вінниця: ВНТУ, 2013. – 44 с.
2. Шартов В.Ф. Ситуационные центры. Информационное обеспечение решений на высшем уровне управления. // Системные проблемы качества, математического моделирования, информационных и электронных технологий. Часть 2. Имитационное моделирование и конфликтология. / Материалы Международной конференции и Российской научной школы. – М.: Радиосвязь, 2003. – 8-17 с.
3. Холин А.И. Ситуационные центры: перспективы цифровых технологий/А.И. Холин // Научная периодика: проблемы и решения. – 2011. – №6. – С. 6-9.

4. Ильин Н.И. Развитие систем специального информационного обеспечения государственного управления / Н.И. Ильин, Н.Н. Демидов, П.Н. Попович: Федеральная служба охраны Российской Федерации – М.: Медиапрес, 2009. – 288 с.
5. Петрик В.М. Соціально-правові основи інформаційної безпеки. Навч. посіб. / В.М. Петрик, А.М. Кузьменко, В.В. Остроухов, О.А. Штоквич, В.І. Полевий — К.: Росава, 2007. — 496 с.
6. Уманець Т. Інформаційно-аналітична база регіонального управління: сучасний стан та перспективи розвитку/ Т. Уманець //Економіка України – 2007. – №8 – С. 39–45.
7. ArcSight ESM [Електронний ресурс]. – Режим доступу до ресурсу: http://www8.hp.com/ru/ru/software-solutions/software.html?compURI=1340477#.U1BFyPl_vhk.

Storozhenko Vitaliy A.*, *Dudatyev Andriy V.,

Information and analytical center of cybersecurity management.

Summary. In the project the current state of the use of information-analytical centers was analyzed, the use of think tanks was examined. The main problems were defined and was developed multi-level structure of information-analytical center, brought analytic description of dependencies that formalizes the relationship of input output parameters.

Keywords: cybersecurity, information-analytical center.