ВИКОРИСТАННЯ НАВЧАЛЬНИХ СИТУАЦІЙНИХ ЦЕНТРІВ ДЛЯ УПРАВЛІННЯ РЕСУРСАМИ

*Київський національний торговельно-економічний університет, м. Київ, Україна

Анотація. У статті розглядається питання про доцільність використання навчальних ситуаційних центрів (НСЦ) для управління ресурсами. Розглядається застосування інформаційних технологій у процесі навчання в ситуаційних центрах та принципів, які вони реалізують: принцип; принцип системності і послідовності; принцип індивідуалізації навчання; принцип; принцип активності. Розглядається застосування навчальних ситуаційних центрів для формування та розвитку практичних навичок управлінського проектування у студентів. Розглядаються і аналізуються аспекти захисту важливої інформації від витоків із використанням інформаційних технологій у навчальних ситуаційних центрах. Наводяться основні принципи класифікації даних, які необхідно використовувати при класифікації інформації, яка потребує захисту. Наводяться основні види засобів мережевого захисту, які необхідно використовувати при побудові системи захисту важливої інформації. Розглядається процес розробки та впровадження в навчальний процес НСЦ для підготовки майбутніх користувачів СЦ, а також у подальшому і розробників таких центрів у різних галузях народного господарства України. Наводяться способи використання рішень щодо захисту інформації в ситуаційних центрах від витоків, які базуються на інформаційних технологіях. Розглядається питання, «що потрібно захищати», яке містить три аспекти: конфіденційну інформацію, чутливі дані, комерційну таємницю. Конкретизується, що в кожному конкретному випадку відповідь на дане питання залежить від того, яку інформацію організація розглядає для себе як найціннішу.

Ключові слова: ситуаційний центр, нові технології, інформаційні та комунікаційні технології, інформація, захист, засоби захисту, конфіденційність, принципи, засоби мережевого захисту, керування, контроль, інфраструктура, вразливості, шифрувальники, навчальний ситуаційний центр, конфіденційна інформація, чутливі дані, комерційна таємниця.

Аннотация. В статье рассматривается вопрос о целесообразности использования учебных ситуационных центров (УСЦ) для управления ресурсами. Рассматривается применение информационных технологий в процессе обучения в ситуационных центрах и принципов, которые они реализуют: принцип; принцип системности и последовательности; принцип индивидуализации обучения; принцип; принцип активности. Рассматривается применение учебных ситуационных центров для формирования и развития практических навыков управленческого проектирования студентов. Рассматриваются и анализируются аспекты защиты важной информации от утечек с использованием информационных технологий в учебных ситуационных центрах. Приводятся основные принципы классификации данных, которые необходимо использовать при классификации информации, нуждающейся в защите. Рассматриваются основные виды средств сетевой защиты, которые необходимо использовать при построении системы защиты важной информации. Рассматривается процесс разработки и внедрения в учебный процесс УСЦ для подготовки будущих пользователей СЦ, а также в дальнейшем и разработчиков таких центров в различных отраслях народного хозяйства Украины. Приводятся способы использования решений по защите информации в ситуационных центрах от истоков, основанных на информационных технологиях. Рассматривается вопрос, «что нужно защищать», который содержит три аспекта: конфиденциальную информацию, чувствительные данные, коммерческую тайну. Конкретизируется, что в каждом конкретном случае ответ на данный вопрос зависит от того, какую информацию организация рассматривает для себя как ценную.

Ключевые слова: ситуационный центр, новые технологии, информационные и коммуникационные технологии, информация, защита, средства защиты, конфиденциальность, принципы, средства сетевой защиты, управление, контроль, уязвимости, инфраструктура, шифровальщики, учебный

ситуаційний центр, конфіденціальна інформація, чутливі дані, комерційна тайна.

Abstract. The article considers the expediency of using educational situation centers (ESC) for resource management. The application of information technologies in the process of learning in situation centers and the principles they implement are considered: the principle; the systemicity and consistency principle; the principle of education individualization; the activity principle. The application of training situational centers for the formation and development of practical management design skills in students is considered. The aspects of protecting important information from leakages using information technology in educational situation centers are considered and analyzed. The basic principles of the classification of data, which should be used in the classification of information that needs protection are given. The main types of network security tools that are used in constructing a system for the protection of critical information are presented. The process, development and introduction into the educational process of ESC for the training of future users of SC, as well as further developers of such centers in different sectors of the national economy of Ukraine are considered. The using of solutions to protect information in situation centers from sources based on information technologies is given. The question “what needs to be protected” is considered, which contains three aspects: confidential information, sensitive data, commercial secrets. Specifies that in each particular case, the answer to this question depends on what kind of information the organization considers for itself as the most valuable.

Keywords: situation center, new technologies, information and communication technologies, information, protection, means of protection, confidentiality, principles, means of network protection, management, control, vulnerabilities, infrastructure, encryption, educational situation center, confidential information, sensitive data, commercial secret.

DOI: 10.34121/1028-9763-2019-4-110-116

1. Вступ

У сучасному світі у зв'язку з високими темпами трансформації суспільно-політичних і економічних процесів суттєво збільшується складність постановки і реалізації задач керування. Бурхливий розвиток інформаційних технологій в останні роки викликав появу великих масивів інформаційних, комунікаційних, аудіо-відеоданих, які необхідно усвідомити, структурувати і аналізувати для прийняття грамотних управлінських рішень.

Використання нових ІТ-рішень для захисту даних в організаціях призвело до того, що, здавалися б до цього безпечними технологіями, опинилися під загрозою цілеспрямованих атак.

Конкурентоспроможність організації в різних галузях безпосередньо залежить від збереження їх комерційних даних – клієнтської бази, бізнес-стратегій, закупівельних цін і технологічного процесу. Однак обсяг конфіденційної інформації останнім часом зростає не по днях, а по годинах, і вибрати засоби захисту від витoku інформації стає непросто.

Засобами подолання суперечності між зростанням кількості багатоаспектної інформації, що аналізується у процесі вирішення управлінських проблем, і здатністю управлінців до виконання даного виду може бути створення ситуаційних центрів (СЦ).

На сьогоднішній день як найбільш прийнятна і сучасна форма реалізації системи підтримки прийняття оптимальних рішень при проведенні інжинірингу, в повній мірі використовуючи можливості концепції управління знаннями, розглядається Ситуаційний центр [1].

Так, у загальному вигляді Ситуаційний центр (СЦ) представляє собою комплекс спеціально організованих робочих місць для персональної та колективної аналітичної роботи з оперативного управління, контролю і моніторингу різних об'єктів і ситуацій. Основним призначенням Ситуаційного центру є підтримка прийняття стратегічних рішень на основі візуалізації та поглибленої аналітичної обробки оперативної інформації [1].

Ситуаційний центр дає можливість промодельовувати варіанти розвитку подій, продумати наслідки тих чи інших дій заздалегідь, не чекаючи настання кризової ситуації. У

ситуаційному центрі максимально зростає роль групового вирішення управлінських проблем із застосуванням сучасних засобів підтримки і прийняття рішень. У зв'язку з цим виникає потреба в розвитку не тільки інформаційних технологій, а також у навчанні управлінців володінню цими технологіями. Рішенням даної проблеми є навчальні ситуаційні центри (НСЦ).

Ситуаційний центр – це простір, призначений для динамічного колективного формування образу ситуації, забезпечений ключовими (критичними щодо розв'язуваної задачі) ресурсами. Основні особливості СЦ:

- унікальність аналізованої ситуації і розв'язуваної задачі;
- формування колективного образу ситуації;
- наявність центру як точки збірки (місця у просторі), яке є визначальним для дій організації;
- розподіл ресурсів на критичні та інші (залежні від розв'язуваної задачі) [2].

2. Актуальність використання навчальних ситуаційних центрів та методи захисту інформації в них

У рамках сучасних освітніх інновацій велика увага приділяється методологічному забезпеченню навчального процесу, зокрема, використання активних методів навчання, розробки та впровадження нових методологій навчання для розвитку у студентів аналітичного мислення.

Актуальність створення СЦ обумовлена багатьма факторами, в числі яких необхідність комплексного підходу до питань управління, збалансованого поєднанням центральних та регіональних інтересів при вирішенні економічних і соціальних проблем, необхідність прийняття рішень в умовах дефіциту часу. При виробленні рішень необхідно оцінювати ризики досягнення поставлених цілей (політичних, економічних, соціальних та ін.), швидко конструювати варіанти рішень і наочно представляти результати оцінки і прогнозування їх наслідків [1].

Основна функція СЦ – комплексна оцінка проблемної ситуації на основі застосування спеціальних методів обробки великих обсягів інформації, а також оперативної побудови і «програвання» сценаріїв їх розвитку. Цю функцію виконують системи підготовки та підтримки прийняття рішень (СППР), які базуються на всьому арсеналі засобів обробки інформаційних ресурсів, технологіях доступу до інформаційно-аналітичних систем (ІАС), інструментально-моделюючих засобах і методах візуалізації. З іншого боку, що є принциповою відмінністю від традиційних систем, вони орієнтовані на конкретного користувача, його знання, досвід, інтуїцію, його систему цінностей при прийнятті рішень, що забезпечує вирішення навіть слабкоструктурованих задач [1].

Так, одним із нововведень вважається створення в навчальних закладах навчальних ситуаційних центрів (НСЦ).

Навчальний ситуаційний центр призначений для формування та розвитку практичних навичок управлінського проектування у студентів. Одна з головних проблем сучасної освіти – розрив між навчальною діяльністю і практикою, а технології ситуаційного центру здатні допомогти студентам відчувати себе «в робочих умовах».

Навчальний ситуаційний центр дозволяє:

- зв'язати різні знання користувачів в єдину, що постійно розвивається, систему знань, яка сприяє інтенсифікації процесу отримання ефективного управлінського рішення;
- сформувати і вдосконалювати навички управління і, перш за все, управлінського мислення, при розробці та реалізації конкретних проектів, враховуючи індивідуальні когнітивні особливості та освітні потреби користувачів;

– значно полегшити практичну роботу користувачів, перевести їх у дослідницький режим. Зробити цю роботу цікавою і захоплюючою, підвищити продуктивність інтелектуальної діяльності.

При навчанні в середовищі НСЦ знання формуються «еволюційно» на підставі експериментів з відповідними моделями. Правила роботи, критерії та методи оцінки учнів можуть значно змінюватися, що не дозволяє використовувати традиційний підхід до навчання. Таким чином, саме функціонування НСЦ зумовлює перехід у навчальному процесі до інноваційних, суб'єктно і діяльнісно-орієнтованих методів навчання (еволюційне навчання, рефлексивно-гуманістична психологія, педагогіка, співтворчість, проєктивна педагогіка та ін.). В.А. Філімонов у статті «Технології ситуаційного центру для соціальної інженерії» визначив основну відмінність навчального та дослідницького СЦ:

– переважна увага приділяється вивченню методів, а не розгляду інформації, що відноситься до певної задачі;

– для розглянутих задач існують рішення, свідомо кваліфіковані як «правильні»;

– одним із основних завдань, що вирішуються в навчально-дослідному центрі, є аналіз і оцінка компетентності, а також збільшення компетентності у процесі навчання індивідуально для кожного учасника навчально-проєктної групи;

– якість проєктів, що розробляються навчально-проєктними групами, є вторинним показником щодо зростання індивідуального рівня кваліфікації.

При організації навчального ситуаційного центру необхідно вирішити задачу:

– технічного оснащення ситуаційного центру. Ситуаційний центр являє собою складний технічний комплекс. Цей комплекс може включати в себе безліч таких підсистем, як підсистема збору інформації (комп'ютери, бази даних, сервери); підсистема структурування та аналізу інформації (інформаційні системи, спеціалізований софт, моделі); підсистема зберігання інформації (сервери, спеціалізоване обладнання для запису і зберігання); підсистема передачі інформації (локальна і глобальна мережа, канали зв'язку); підсистема візуалізації інформації (спеціалізований софт для візуалізації, дисплейні системи, управління виводом інформації, озвучування, інтерактивні засоби); підсистема забезпечення безпеки інформації;

– навчання професорсько-викладацького складу, який бере участь у реалізації навчального процесу з використанням технологій СЦ;

– створення і розробки нових методик викладання. Основними завданнями викладача є контроль знань, оцінка прийнятих рішень і управління потоками вхідних даних для формування типових і екстрених ситуацій. Для цього викладач повинен знати пристрій СЦ, принципи і механізми його роботи, а також допустимі і найбільш імовірні значення вхідних параметрів.

Застосування інформаційних технологій у процесі навчання в ситуаційних центрах сприяє реалізації деяких принципів і наповнює їх новими можливостями:

– принцип науковості – використання сучасної обчислювальної техніки дозволяє відображати в освітньому процесі сьогодишні рубежі науки і виводити студентів на рівень випереджальних знань;

– принцип системності і послідовності забезпечується за рахунок програмного подання навчальної інформації, що обумовлює успішне засвоєння не тільки предметних знань відповідної науки, а й її структури, логіки та методики вивчення;

– принцип індивідуалізації навчання реалізується за допомогою адаптивних програмних засобів, що забезпечують кожному студенту свій рівень складності наданої інформації;

– принцип наочності реалізується в достатній мірі на основі технологій мультимедіа;

– принцип активності – робота з ІКТ забезпечує підвищення у студентів творчої діяльності і психічних процесів (сприйняття, асоціації, інтуїції та ін.), що в підсумку впливає на формування рівня знань.

Розглядаючи навчання студентів у ситуаційному центрі як застосування інноваційних технологій у навчальному процесі, спрямоване на набуття ними системних знань, умінь і практичних навиків, пов'язаних з підготовкою до дій у різних обставинах, особлива увага при проведенні занять має приділятися аналітичному інструментарію, методичним аспектам оцінки обстановки і алгоритмам прийняття рішення.

Нові технології в навчанні студентів діям у різних обставинах базуються на створенні структурно-логічних схем і алгоритмів дій.

Відповідно до методологічних призначень ситуаційного центру, його основною метою є освоєння студентами техніки проведення конкретних видів аналітичної роботи, навчити їх правильно структурувати і викладати свої думки при з'ясуванні отриманого завдання, оцінки обстановки при підготовці проекту рішення на проведення спеціальної операції.

Таким чином, мова йде про методологію прикладного аналізу оцінки обстановки, підготовки і проведення спеціальної операції. Використовуючи інформаційні технології, студенти вчаться прогнозувати розвиток оперативної обстановки, виводити кількісний аналіз можливих варіантів розвитку подій, вирішувати завдання вибору оптимальних рішень.

У даному випадку під методологією проведення аналітичної роботи розуміється комплексна система методів, інструментів і технологій, спрямована на розвиток і вдосконалення у студентів практичних навичок вибору оптимальних рішень.

Крім того, стоїть питання щодо захисту інформації в самих ситуаційних центрах, так як ця інформація може нести конфіденційний характер.

Стандартна відповідь фахівця з інформаційної безпеки на питання, що потрібно захищати, буде містити три аспекти – конфіденційну інформацію, чутливі дані, комерційну таємницю. Однак необхідно конкретизувати, що в кожному конкретному випадку відповідь на дане питання залежить від того, яку інформацію організація розглядає для себе як найціннішу. Для якоїсь компанії це може бути клієнтська база, для іншого – геопозиційна інформація, і, напевно, для всіх організацій – це інформація, пов'язана з їх фінансовою діяльністю та технологічним процесом [3].

При цьому будь-яка організація – це сукупність бізнес-підрозділів і сервісних служб, керівники яких можуть допомогти фахівцю з інформаційної безпеки зрозуміти, що саме важливе для організації, яка конкретна інформація.

Після вибору інформації, яку буде віднесено до цінних (критичних) даних, необхідно перейти до класифікації існуючого в організації масиву даних. Знизити трудомісткість і підвищити якість виконання цього етапу робіт дозволяють широко представлені на ринку засоби автоматизації класу Data Classification Application) – Digital Guardian, Forcepoint, Varonis IDU Classification Framework, Titus, Classifier360 та ін. Зазначені рішення забезпечують пошук і класифікацію масиву даних організації за заданими критеріями і часто використовуються як один із елементів комплексу засобів захисту від витоків інформації. На рис. 1 зображені основні принципи класифікацій даних в організації.

Цю структуру даних необхідно зафіксувати у внутрішніх документах організації – описати рівні конфіденційності чутливої інформації (перелік відомостей конфіденційного характеру) і визначити методологію роботи з цією інформацією – розробити політику забезпечення інформаційної безпеки, регламенти роботи з конфіденційною інформацією.

Ключовим елементом, що забезпечує ефективність захисту організації від витоків інформації, є інформування співробітників про склад конфіденційної інформації і правила роботи з нею.

Сучасним підходом до задачі навчання і контролю знань співробітників є використання спеціалізованих програм підвищення обізнаності користувачів (наприклад, такі рішення є у компаній UBS, Kaspersky Lab та ін.). Навчання і контроль знань співробітників організації здійснюються інтерактивно, в форматі відеоуроків і тестів, а також вікторин та квестів –для користувачів з високим рівнем доступу до інформації.

Рисунок 1 – Основні принципи класифікації даних

Як основні складові інформаційно захищеного периметра організації можна виділити наявність засобів мережевого захисту і управління вразливими місцями в організації.

Зазвичай більшість організацій використовують такі основні види засобів мережевого захисту з використанням інформаційних технологій (рис. 2).

Рисунок 2 – Основні види засобів мережевого захисту

Міжмережеві екрани, а точніше, NGFW або UTM-рішення (Check Point NGTP, Palo Alto NGFW, Fortinet FortiGate і ін.). Сучасні міжмережеві екрани вже мають мінімальні DLP-движки, що дозволяють виявляти витоки за налаштованими шаблонами [2].

Функція Web-контролю трафіка як окремий шлюз або у складі NGFW (Blue Coat SG, McAfee WGW, Cisco WSA, Check Point NGTP, Palo Alto NGFW, Fortinet FortiGate і ін.). Зокрема, корисно буде заборонити використання сервісів Google (Disk, Gmail), принаймні, на операцію вивантаження файлів (upload) [2]. У тому числі, необхідно виконувати моніторинг дій користувачів в інтернеті, лімітувати обсяги завантаженої інформації [2].

Якщо організація використовує корпоративний портал для зберігання конфіденційних документів, має сенс звернути увагу на рішення класу Web Application Firewall (WAF).

Керування вразливостями – процес вкрай важливий для побудови захищеної інфраструктури. Останні події з вірусом WannaCry і Petya недвозначно нагадали про це. Так,

захист від вірусів-шифрувальників ближче до області рішень по захисту даних від втрат, ніж до крадіжки інформації. Наприклад, процес управління оновленнями програмного забезпечення (Patch Management), у цілому, ускладнить принципове проникнення в інформаційний периметр організації незалежно від його мети.

3. Висновки

Таким чином, розробка та впровадження в навчальний процес НСЦ є актуальним завданням, вирішення якого дозволяє підготувати майбутніх користувачів СЦ, а також у подальшому і розробників таких центрів у різних галузях народного господарства України.

Навчання в ситуаційному центрі дозволить підняти навчальний процес на новий рівень сучасних навчальних інновацій і вивести випускників вузів на новий щабель професійної підготовки.

НСЦ – дійсно ефективна форма передачі знань. Сьогодні знання, кадри, фахівці – важлива умова, вона найближчим часом буде визначати розвиток усіх сфер діяльності в нашій країні.

Використання рішень щодо захисту інформації в ситуаційних центрах від витоків, які базуються на інформаційних технологіях, вимагає комплексного підходу і ретельного технічного опрацювання.

Отже, використання інформаційних технологій для забезпечення захисту даних є одним із пріоритетних завдань будь-якої організації.

СПИСОК ДЖЕРЕЛ

1. Краскевич В.Є., Литвинов В.В., Луцик С.Л., Кривогуз А.М. Концепція створення учбового ситуаційного центру для фінансового, правового і зовнішньоторгового інжинірингу. *Математичні машини і системи*. 2015. № 1. С. 124–129.
2. Анісімов О.С., Берс А.А., О.А. Жирков О.А. Компоненти інформаційних технологій ситуаційних центрів / ред. В.А. Філімонова. Омськ: ТОВ «Інформаційно-технологічний центр», 2010. 152 с.
3. Ромака В.А., Лагун А.Е., Гарасим Ю.Р. Аудит інформаційної безпеки: підручник / Держ. служба України з надзвич. ситуацій, Львів. держ. ун-т безпеки життєдіяльності, НАН України, Ін-т приклад. проблем механіки і математики ім. Я.С. Підстригача. Львів: Сполом, 2015. 363 с.

Стаття надійшла до редакції 21.06.2019