ЧТЕІ ДТЕУ

Чернівецький торговельно-економічний інститут Державного торговельно-економічного університету

ФІНАНСОВО-ЕКОНОМІЧНІ, СОЦІАЛЬНІ ТА ПРАВОВІ АСПЕКТИ РОЗВИТКУ РЕГІОНІВ: ЗАГРОЗИ ТА ВИКЛИКИ

Міжнародна науково-практична конференція

24.05.2024

м. Чернівці

Міністерство освіти і науки України
Чернівецька обласна військова адміністрація
Чернівецька обласна рада
Чернівецька міська рада
Державний торговельно-економічний університет
Чернівецький торговельно-економічний інститут ДТЕУ
Громадська організація «Інститут сучасних інформаційних досліджень»
Університет ім. Штефана чел Маре (м. Сучава, Румунія)
Вища школа економіки та менеджменту державного
управління (м. Братислава, Словаччина)
Університет ARTIFEX (м. Бухарест, Румунія)
Університет менеджменту безпеки (м. Кошице, Словаччина)
Університет Трансмонтани і Верхнього Дору (м. Віла-Реал, Португалія)
Лодзинський університет (м. Лодзь, Польща)

ФІНАНСОВО-ЕКОНОМІЧНІ, СОЦІАЛЬНІ ТА ПРАВОВІ АСПЕКТИ РОЗВИТКУ РЕГІОНІВ: ЗАГРОЗИ ТА ВИКЛИКИ

МАТЕРІАЛИ МІЖНАРОДНОЇ
НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

24 травня 2024 року
м. Чернівці (Україна)

Чернівці
Технодрук
2024

Оксана Верстяк, к.е.н., доцент,
Чернівецький торговельно-економічний інститут ДТЕУ,
м. Чернівці

КІБЕРЗЛОЧИННІСТЬ ЯК ЗАГРОЗА РЕГІОНАЛЬНІЙ БЕЗПЕЦІ

Кіберзлочинність та кібертероризм на сьогодні становлять серйозну загрозу для регіональної та світової безпеки. Вони можуть мати різноманітні форми і прояви, включаючи крадіжку конфіденційної інформації, шахрайство, віруси, атаки на критичну інфраструктуру та багато іншого.

Одна з ключових проблем полягає в тому, що кіберзлочинці та кібертерористи можуть діяти анонімно з будь-якого місця у світі, що робить їх важкими для виявлення та зупинення. Вони можуть використовувати широкий спектр інструментів і технік, щоб проникнути в системи, викрасти дані або завдати шкоди.

Загроза кібертероризму стає особливо небезпечною через можливість атак на критичну інфраструктуру, таку як енергетичні системи, фінансові установи, медичні системи тощо. Пошкодження або відключення цих систем може призвести до серйозних наслідків для громадської безпеки та економічної стабільності.

В Україні були зареєстровані кібератаки на державні установи, банки, енергетичні підприємства та інші критичні інфраструктурні об'єкти. Деякі з найвідоміших інцидентів включають кібератаку на енергетичну систему, яка призвела до відключення електропостачання у деяких регіонах, а також атаки на банки та фінансові установи з метою крадіжки грошей або конфіденційної інформації.

Кібератаки в регіонах України можуть включати широкий спектр інцидентів, від спростовуваних сайтів до серйозних порушень безпеки критичних інфраструктурних об'єктів. Найбільш поширеними об'єктами кібератак є державні установи, банки, енергетичні компанії, телекомунікаційні мережі та інші критичні інфраструктурні об'єкти. Розглянемо основні етапи кібератак (рис. 1).

Рис. 1. Етапи кібератак

Саме тому необхідні корпоративні процеси для запровадження кібербезпеки (рис. 2).

Рис. 2. Корпоративні процеси для запровадження кібербезпеки

Безпека даних – процес захисту конфіденційності, цілісності та доступності даних від несанкціонованого доступу, втрати, пошкодження або розкриття.

Засоби, які дають найкращі результати:

- цифрування даних;
- встановлення багаторівневої системи доступу до даних;
- резервне копіювання;

- встановлення антивірусного програмного забезпечення.

Для боротьби з загрозами, країни повинні співпрацювати на міжнародному рівні, обмінюючись інформацією та ресурсами, розробляючи та впроваджуючи ефективні кіберзаходи безпеки, інвестуючи в кіберзахист та розвиток технологій, що містять в собі безпекові функції. Також важливо підвищувати свідомість громадськості про кібербезпеку та забезпечити надійність та захищеність критичних інфраструктур.

Список використаних джерел:

1. Найбільші кібератаки проти України з 2014 року. Інфографіка. (б.д.). Новини України та світу. Головні і останні новини-NV. URL: https://nv.ua/ukr/ukraine/events/najbilshi-kiberataki-proti-ukrajini-z-2014-roku-infografika-1438924.html

2. Limba, T.,Plėta, T.,Agafonov, K.,& Damkus, M.(2017).Cyber security management model forcriticalinfrastructure. Entrepreneurship and Sustainability Issues, 4(4),559–573. DOI: https://doi.org/10.9770/jesi.2017.4.4(12)

Oksana Verstiak, PhD of Economic Sciences,
Associate Professor,
Chernivtsi Institute of Trade and Economics of SUTE, Chernivtsi

CYBERCRIME AS A THREAT TO REGIONAL SECURITY

Cybercrime and cyberterrorism today pose a serious threat to regional and global security. They can take various forms and manifestations, including theft of confidential information, fraud, viruses, attacks on critical infrastructure, and much more. One of the key challenges is that cybercriminals and cyberterrorists can operate anonymously from anywhere in the world, making them difficult to detect and stop. They can employ a wide range of tools and techniques to penetrate systems, steal data, or cause damage.