МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Одеська юридична академія»

ЄВРОПЕЙСЬКІ ОРІЄНТИРИ РОЗВИТКУ УКРАЇНИ: НАУКОВО-ПРАКТИЧНИЙ ВИМІР В УМОВАХ ВОЄННИХ ВИКЛИКІВ

МАТЕРІАЛИ
Міжнародної науково-практичної конференції

Одеса, 26 квітня 2024 року

Одеса
«Фенікс»
2024

УДК 005.332.2(4):316.42(477)“364”“20”(062.552)
Є 24

Рекомендовано до друку вченою радою
Національного університету «Одеська юридична академія»
(протокол № 8 від 15.05.2024 р.)

За загальною редакцією ***С. В. Ківалова***

Відповідальний за випуск ***М. Р. Аракелян***

Є 24 **Європейські орієнтири розвитку України: науково-практичний вимір в умовах воєнних викликів** : матеріали Міжнар.наук.-практ. конф. (Одеса, 26 квітня 2024 р.) / за заг. ред. С. В. Ківалова. – Одеса : Фенікс, 2024. – 1000 с.
ISBN 978-617-8430-05-4

У збірнику відображено наукові напрацювання вчених, практиків, військовослужбовців у теоретичній та емпіричній площині у сферах філософських основ, загальної теорії та історичних досліджень держави і права, актуальних проблем світових соціально-політичних процесів, соціології та психології в умовах повномасштабного військового вторгнення. Висвітлено питання загроз національній безпеці в їх конституційному вимірі у рамках міжнародного та європейського права, трудового права та права соціального забезпечення, земельного, аграрного та екологічного права, пов’язані з функціонуванням економіки та підприємництва в умовах європейського вибору України. Розглянуто проблеми інформатизації та цифровізації суспільства, захисту інформації та кібербезпеки в умовах військового вторгнення, питання методики викладання іноземних мов, теорії та практики перекладу, проблеми лінгвістики та журналістики. Відображено наукові напрацювання у сферах адміністративного права та процесу, фінансового, морського та митного права, організації та вдосконалення судоустрою, прокуратури, інших правоохоронних органів, адвокатури. Висвітлено питання кримінального права, кримінально-процесуальних аспектів кримінального провадження та кримінологічних особливостей протидії злочинності в умовах воєнного стану, криміналістики, судової експертизи, психології та медицини у забезпеченні судочинства, цивільного та сімейного права, інтелектуальної власності та патентної юстиції, цивільного судочинства, господарського права та процесу. Розглянуто актуальні питання діяльності сучасних бібліотек у закладах вищої освіти, фізичної підготовки здобувачів вищої освіти.

Збірник розраховано на наукових і науково-педагогічних працівників, здобувачів вищої освіти, практичних працівників у сферах юридичної, економічної, соціологічної, політологічної, психологічної, філологічної наук, журналістики та кібербезпеки тощо.

УДК 005.332.2(4):316.42(477)»364»»20»(062.552)

Матеріали видано в авторській редакції

ISBN 978-617-8430-05-4

© НУ «Одеська юридична академія, 2024
© Автори статей, 2024

СЕКЦІЯ 24. КІБЕРБЕЗПЕКА ОСОБИ, СУСПІЛЬСТВА ТА ДЕРЖАВИ ЯК ФУНДАМЕНТАЛЬНИЙ ЕЛЕМЕНТ ЗАБЕЗПЕЧЕННЯ ОБОРОНОЗДАТНОСТІ УКРАЇНИ

СЕКЦІЯ 25. ПИТАННЯ МЕТОДИКИ ВИКЛАДАННЯ ІНОЗЕМНИХ МОВ, ТЕОРІЇ ТА ПРАКТИКИ ПЕРЕКЛАДУ ЯК ЗАСОБУ НАЛАГОДЖЕННЯ КОМУНІКАЦІЇ

6. Finlayson R. A more loss-tolerant RTP payload format for MP3 audio. *Internet Engineering Task Force*. 2008. URL: https://www.rfc-editor.org/rfc/rfc3119

7. Kim H. J., Choi Y. H. A novel echo-hiding scheme with backward and forward kernels. *IEEE Transactions on Circuits and Systems for Video Technology*. 2003. № 13 (8). P. 885–889.

Ключові слова: стеганографія, аудіофайли, MP3, поля заголовків аудіо даних.
Keywords: steganography, audio files, MP3, audio data header fields.

Разінкін Нікіта Сергійович
Національний університет «Одеська юридична академія»,
асистент кафедри кібербезпеки

КІБЕРЗАХИСТ ЕНЕРГЕТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ ВІЙНИ

Кіберзагрози в умовах війни набувають особливої актуальності та серйозності, оскільки конфлікти переходять у цифровий простір, де може бути атакована критична інфраструктура, урядові установи та цивільне населення. Військові дії сьогодні не обмежуються лише традиційним полем бою, вони розповсюджуються у віртуальний простір, де кібератаки використовуються для досягнення стратегічних цілей без необхідності фізичного втручання.

Кібервійна може включати різноманітні дії, такі як розповсюдження дезінформації, шпигунство через викрадення конфіденційної інформації, атаки на інфраструктуру з метою її виведення з ладу, втручання у виборчі процеси та підрив довіри до урядових інституцій. Це веде до ескалації напруженості між країнами, зростання страху та нестабільності серед цивільного населення.

Один з ключових аспектів кіберзагроз в умовах війни – це їх анонімність та складність визначення джерела атаки. Це ускладнює процес притягнення до відповідальності та формування ефективних стратегій захисту. Кібератаки можуть бути виконані з будь-якої точки світу, що робить кіберпростір особливо вразливим перед лицем геополітичних конфліктів [1].

Для протидії кіберзагрозам у воєнний час країни та організації повинні інвестувати у розбудову своїх кібероборонних можливостей, розвивати міжнародне співробітництво для обміну інформацією про загрози та координувати зусилля з кібербезпеки. Також важливо зосередитись на підвищенні обізнаності та освіті громадян у сфері кібербезпеки, адже людський фактор часто є слабким ланцюгом у захисті від кібератак.

Статистика кібератак в Україні під час війни показує значне зростання таких інцидентів. За даними Держспецзв'язку, кількість кібератак на українські цілі зросла втричі порівняно з попереднім періодом. Основні цілі атак включають державні органи влади, медійні ресурси, енергетичну сферу та сферу логістики.

Окремо варто відзначити реакцію України на такі виклики. Зокрема, було створено кібервійська в структурі Міністерства оборони, хоча вони не були повністю утворені до початку повномасштабної війни. Кіберполіція України відповідає за розслідування кіберзлочинів, Міноборони та Генштаб забезпечують захист військових об'єктів і об'єктів критичної інфраструктури, а Служба безпеки України працює над запобіганням терористичних атак у кіберпросторі.

Українське Міністерство цифрової трансформації працює над «цифровою блокадою» росії, закликаючи технологічні компанії припинити свою діяльність на російському ринку та вводити проти неї санкції. Станом на середину травня, звернення були здійснені до приблизно 500 компаній, більшість з яких відгукнулися позитивно.

За період з січня 2022 року по вересень 2023 року в Україні було зафіксовано майже 4000 кіберінцидентів. Зазначено, що кіберактивність у контексті російсько-українській війні не

обмежується діями урядових структур. Наприклад, в червні 2023 року проросійська хакерська група NoName057 погрожувала атакувати фінансовий сектор України, що призвело до DDoS-атак на численні українські банки [2].

Збільшення кібератак під час війни підтверджується статистикою, яка вказує на тривожну тенденцію зростання таких загроз, але також і на активну роботу України щодо підвищення свого кіберзахисту та впровадження контрзаходів.

Кіберзахист енергетичної інфраструктури в умовах війни є надзвичайно важливою сферою для забезпечення безпеки та стійкості країни. У військових конфліктах кіберзагрози можуть бути використані для порушення роботи енергетичних систем, що може призвести до серйозних наслідків для національної безпеки, економіки та суспільства загалом.

З огляду на ці ризики, Україна здійснює значні зусилля щодо зміцнення свого кіберпростору, особливо в секторі енергетики. Враховуючи високий рівень загрози, країна активізувала свої ресурси для ідентифікації та нейтралізації потенційних кібератак.

Ключові аспекти кіберзахисту енергетичної інфраструктури в умовах війни можна побачити у таблиці 1.

Таблиця 1

Аспекти кіберзахисту енергетичної інфраструктури

№	Аспект	Опис
1.	Системи виявлення та реагування на кіберзагрози	Спеціалізовані системи моніторингу і виявлення інцидентів можуть вчасно реагувати на кіберзагрози, виявляти аномальну активність та забезпечувати швидке реагування
2.	Кіберзахист інфраструктури критичних об'єктів	Енергетичні підприємства мають здійснювати заходи щодо захисту критичних систем від кібератак, включаючи мережеві інфраструктури, системи керування та автоматизації
3.	Резервне джерело живлення і комунікацій	Важливо мати резервні джерела енергії та засоби зв'язку, які можуть бути використані у випадку кібератаки або знищення енергетичної інфраструктури
4.	Навчання та підготовка персоналу	Регулярні тренування та навчання персоналу з кібербезпеки є ключовими для виявлення, відповіді та запобігання кібератак
5.	Міжнародне співробітництво	Співпраця з іншими країнами у сфері кібербезпеки може допомогти у виявленні та протидії кіберзагрозам, які можуть виникати у військових конфліктах
6.	Створення кібер-стратегії та планів надзвичайних ситуацій	Наявність чітких стратегій та планів дій у разі кібератаки або військового конфлікту допомагає забезпечити ефективне керівництво та координацію дій
7.	Захист інформаційної інфраструктури	Захист інформаційних систем, включаючи бази даних, важливий для запобігання несанкціонованому доступу до критичних даних та інформації.

Джерело: розроблено автором

Враховуючи постійне розвиток технологій та загроз кібербезпеки, необхідно постійно вдосконалювати заходи кіберзахисту енергетичної інфраструктури та бути готовими до найбільш непередбачуваних сценаріїв.

Кіберзахист енергетичної інфраструктури в Україні в умовах війни включає комплекс заходів, спрямованих на забезпечення стійкості енергетичної системи до ворожих кібератак. З огляду на значні збитки та руйнування, спричинені військовими діями, важливість кіберзахисту стає особливо актуальною. Енергетична інфраструктура, зокрема теплоелектростанції,

системи електропостачання та газопроводи, стали мішенями для атак. Це призвело до масштабних відключень та зупинок роботи важливих об'єктів, посиливши кризові ситуації у зоні конфлікту.

Для посилення кіберзахисту використовуються такі заходи, як встановлення оновлень та виправлень критичних вразливостей, особливо тих, що використовуються зловмисниками. Агентство з кібербезпеки та безпеки інфраструктури США (CISA) веде базу даних таких вразливостей, що може слугувати орієнтиром для визначення пріоритетних напрямків роботи. Ключовим елементом захисту є також перегляд політики контролю доступу до систем із зосередженням уваги на багатофакторній аутентифікації та необхідності ізоляції високоризикових систем. Важливо забезпечити актуальність захисту від шкідливого програмного забезпечення, регулярно оновлювати програмне забезпечення та проводити зовнішнє сканування вразливостей систем, що мають доступ до інтернету [3].

Крім технічних аспектів, велике значення має залучення персоналу та забезпечення його обізнаності про кіберзагрози, методи фішингу та шахрайські дій. Компаніям важливо організувати психологічну підтримку для співробітників та їхніх сімей, провести тренінги щодо поведінки в кризових ситуаціях, а також забезпечити доступ до надійних джерел інформації.

Кіберзахист енергетичної інфраструктури в Україні в умовах війни охоплює ряд заходів, спрямованих на захист від атак, що можуть пошкодити або зупинити роботу енергетичних об'єктів. Це включає встановлення оновлень та виправлень для критичних вразливостей, зосередження уваги на багатофакторній аутентифікації, захист від шкідливого програмного забезпечення, зовнішнє сканування вразливостей та регулярне створення резервних копій важливих даних. Важливим є також моніторинг безпеки для своєчасного виявлення та реагування на вторгнення, а також планування дій у випадку зупинки діяльності в регіонах бойових дій.

Значні збитки та руйнування, спричинені військовими діями, посилюють важливість заходів кібербезпеки, оскільки енергетична інфраструктура стала мішенню для атак. Пошкодження та зупинки роботи важливих об'єктів, як-от теплоелектростанції, системи електропостачання, та газопроводи, створюють кризові ситуації, що підкреслюють необхідність захисту від подібних інцидентів.

Підходи до кіберзахисту повинні бути інтегрованими, залучаючи як технічні заходи, так і забезпечення обізнаності та підготовку персоналу, щоб ефективно протистояти кіберзагрозам та мінімізувати ризики для енергетичної інфраструктури.

Список використаних джерел

1. Симонов А. А. Кіберзахист інформаційних і керуючих систем атомних електростанцій. *Кібербезпека енергетики* : матеріали наук.-практ. конф. Інту проб. моделювання в енергетиці ім. Г. Є. Пухова Нац. акад. наук України (м. Київ, 31 трав. 2023 р.). Київ, 2023. С. 93–95.

2. Свиридюк Ю. В Україні зафіксували майже 4 000 кібератак з боку РФ. 2023. URL: https://suspilne.media/619941-v-ukraini-zafiksuvali-majze-4-000-kiberatak-z-boku-rf/#:~:text=Команда%20реагування%20на%20надзвичайні%20ситуації,міністра%20фінансів%20США%20Грем%20Стіл.

3. Щавінський Ю. В., Пальчинська В. Б. Правові механізми забезпечення кіберзахисту об'єктів критичної інформаційної інфраструктури України в умовах гібридної війни. *Виклики та загрози критичній інфраструктурі* : монографія / НУО Інт Cyberspace Research. Детройт, США, 2023. С. 198–202.

Ключові слова: кіберзахист, енергетична інфраструктура, війна, бойові дії, безпека.
Keywords: cyber defense, energy infrastructure, war, combat operations, security.