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

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

Таким чином, бібліотека numpy дозволяє ефективно здійснювати розрахунки з великими масивами чисел, при цьому зберігаючи зручність використання python мови, що дозволяє швидко і ефективно виконувати аналіз великих обсягів даних.

Список використаних джерел

1. Бойко В. Д. Інструменти моделювання та аналізу даних у навчальному та дослідному процесі. *Європейські орієнтири розвитку україни в умовах війни та глобальних викликів XXI століття. Синергія наукових, освітніх та технологічних рішень :* матеріали Міжнар. наук.-практ. конф. 19 трав. 2023 р. / ред. С. В. Ківалов. Одеса, 2023. Р. 618–621.

2. Бойко В. Д. Використання interactive python для моделювання, аналізу та обробки даних у навчальному та дослідницькому процесах. *Інформаційне суспільство: Проблеми та перспективи* : матеріали VIII всеукр. наук.-практ. конф. (м. Одеса, 2 черв. 2023 р.). Одеса, 2023. Р. 51–56.

3. Harris C. R. et al. Array programming with NumPy. *Nature. Springer Science; Business Media LLC*. 2020. Vol. 585, N 7825. P. 357–362.

4. Beazley D. M. Python distilled. Pearson, 2021. 352 p.

Ключові слова: аналіз даних, відкрите програмне забезпечення, відкриті формати даних, відкриті протоколи зв'язку, аналіз логів, аналіз логів веб-серверів.

Keywords: python, numpy,ipython, bigdata, data explore, data mining, data analysis, open software, open data formats, open communication protocols, log analysis, web server logs, analysis of web server logs, threats and risks.

Кухаренко Сергій Вікторович
Національний університет «Одеська юридична академія»,
доцент кафедри кібербезпеки, кандидат технічних наук, доцент

ПОЛІТИКИ ТА ПРОЦЕДУРИ РЕАГУВАННЯ НА ПОРУШЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНОЇ СИСТЕМИ

Політика безпеки інформаційної системи визначає сукупність правил, вимог і керівних принципів в області інформаційної безпеки, якими керується організація в своїй діяльності та безпосередньо встановлює основні положення і завдання щодо системи управління інформаційною безпекою. Політика безпеки є нормативною основою для захисту інформаційних активів організації з метою забезпечення їх цілісності, конфіденційності та доступності [1].

Подія щодо кібербезпеки це – зміна стану кібербезпеки, яка може вплинути на діяльність організації.

Інцидент у кібербезпеки це – окрема або серія небажаних або неочікуваних подій з кібербезпекою або таких, що є можливими ознаками кібератаки які можуть поставити під загрозу роботу організації.

Існує багато типів інцидентів інформаційної безпеки, які можна класифікувати як інциденти кібербезпеки, починаючи від серйозних атак кібербезпеки на критично важливу національну інфраструктуру та великих організованих кіберзлочинів, через хакерство та базові атаки зловмисного програмного забезпечення (шкідливий програмний код), до внутрішнього неправомірного використання систем і збою програмного забезпечення.

Відповідний перелік типів кіберінцидентів розроблений з використанням та відповідає рекомендації Європейської агенції з кібербезпеки (ENISA Reference Incident Classification Taxonomy), а також спільному документу ENISA та Європейського центру боротьби з кіберзлочинністю Європолу (Common Taxonomy for Law Enforcement and The National Network

of CSIRTs), який «призначений для впровадження єдиної класифікації як інструменту для обміну інформацією щодо кіберінцидентів» [2].

Проведені дослідження показують, що не існує єдиного загального визначення інциденту кібербезпеки. Інцидент визначається як: цифровий (слабкі паролі тощо); фізичний; внутрішній; зовнішній; екологічний; недбалість; навмисний.

Управління інцидентами безпеки – процеси підготовки, виявлення, звітування, оцінки, реагування на інциденти кібербезпеки, роботи з ними та навчання на них.

Інциденти кібербезпеки – це ризик, який слід включити до загальної політики управління ризиками організації. Крім того, управління інцидентами кібербезпеки означає не лише застосування технологій. Це також вимагає розробки плану, який буде інтегрований в існуючі процеси та організаційні структури, щоб уможливити, а не перешкоджати критичним бізнес-функціям. Таким чином, вище керівництво повинно брати активну участь у визначенні плану запобігання кібербезпеці організації та реагування на інциденти, тому що це є ключем до успіху плану.

Реагування на інциденти – це комплекс заходів з виявлення та дослідження результатів кібератак і витоку системних даних в організації, а також стратегія відновлення даних, глибокий аналіз того, що сталося, і розробка детального плану дій для усунення наслідки [3].

Реагування на інцидент керуватиметься залежно від рівня ваговитості інциденту, тобто його впливу або загрози роботі або цілісності інформації організації, що в свою чергу визначає пріоритет для обробки інциденту, а також час і ступінь реагування на нього.

Для класифікації інцидентів та відповідно дій на його реагування використовується шість рівнів: некритичний (білий), низький (зелений), середній (жовтий), високий (помаранчевий), критичний (червоний), надзвичайний (чорний) [4] але в загальному вигляді їх можливо поділити натри рівні: високий, середній і низький.

Рівень інциденту безпеки буде вважатися «високим», якщо існує будь-яка з умов що: загрожує значним несприятливим впливом на велику кількість систем, завдаючи їм значної шкоди або збою; створює потенційний великий фінансовий ризик; загрожує конфіденційним даним.

Рівень інциденту безпеки вважатиметься «середнім», якщо існує будь-яка з умов що: негативно впливає на пересічну кількість систем, некритичну корпоративну систему або службу організації; має помірну ймовірність розповсюдження на інші системи, спричиняючи помірну шкоду або збій.

Інциденти «низького» рівня тяжкості мають такі характеристики: негативно впливають на невелику кількість систем; порушує роботу незначної кількості мережевих пристроїв або сегментів; має невеликий ризик розповсюдження, або не має такого ризику, або спричиняє лише мінімальні пошкодження.

План реагування на інцидент створюється для усунення ймовірного порушення даних у кілька етапів:

- планування (створення політики безпеки що передбачає реагування на інциденти);
- реалізація (визначення переліку інформаційних активів, що підлягають захисту та впровадження механізмів, процедур захисту політики безпеки);
- аналіз або аудит (моніторинг) виконання політики безпеки (пошук відхилень від нормальних операцій і діяльності, виявлення витоку даних та визначення, звідки він походить та на що він вплинув);
- локалізації та документування наслідків інцидентів; удосконалення (видалення недоліків та процесів, які призвели до порушення та зміна політики безпеки);
- відновлення (відновлення даних та систем захисту у робочий стан).

Реагування на інциденти в загальному вигляді викладені в Порядку реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі, Методичних рекомендаціях щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросто-

рі [4, 5] та інших нормативних документах аналізуючи які можливо запропонувати наступні елементи, які повинні забезпечити реагування на інциденти:

1. Швидке та ефективне реагування та відновлення після інцидентів.

2. Забезпечення захисту від кібератак, витоків даних та інших загроз, що можуть призвести до фінансових втрат та втрат інформаційних активів.

3. Добре розроблений план реагування на інциденти з використанням безпечних методів, які спроможні мінімізувати наслідки інцидентів для подальшої безпечної роботи.

4. Управління наслідками порушення безпеки, збір доказів та вжиття заходів для запобігання подальшим атакам.

5. Мінімізація наслідків інцидентів безпеки та запобігання його повторенню з часом.

Список використаних джерел

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII у ред. від 01.01.2024 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

2. Перелік категорій кіберінцидентів. Державна служба спеціального зв'язку та захисту інформації України. URL: https://www.cip.gov.ua/ua/news/perelik-kategorii-kiberincidentiv

3. Реагування на інциденти. URL: https://cqr.company/ua/service/reaguvannya-na-incidenty/

4. Порядок реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі : постанова КМУ від 04.04.2023 р. № 299. URL: https://zakon.rada.gov.ua/laws/show/299-2023-%D0%BF#Text

5. Методичні рекомендацій щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі : наказ Адмін. Держ. служби спец. зв'язку та захисту інформації України від 03.07.2023 р. № 570. URL: https://ips.ligazakon.net/document/FN077992

Ключові слова: кібербезпека, кіберінцидент, політика безпеки, захист інформації, захист даних, кібератака.
Keywords: cyber security, cyber incident, security policy, information protection, data protection, cyberattack.

Чепурна Олена Євгенівна
Національний університет «Одеська юридична академія»,
доцент кафедри кібербезпеки, кандидат фізико-математичних наук, доцент

КІБЕРЗАГРОЗИ ДЛЯ БІЗНЕС-СЕРЕДОВИЩА ТА СУЧАСНІ ЗАХОДИ ПРОТИДІЇ

В умовах сучасної гібридної війни, що охопила Україну, кіберпростір став ареною жорстоких зіткнень, які не менш значимі, ніж традиційні воєнні дії. Військові конфлікти тепер не обмежуються лише фізичним простором; вони проникають у віртуальний світ, де битви за інформаційний простір і безпеку даних стають вирішальними. Для бізнес-середовища в Україні, як і для всього суспільства, кіберзагрози в цей період набули особливої актуальності.

Кібератаки, фішинг, злом баз даних – це лише деякі з викликів, з якими зіткнулися українські компанії. У таких умовах, коли віртуальний фронт стає таким же важливим, як і фізичний, питання кібербезпеки виходить на перший план. Воно вимагає негайної уваги та координації зусиль на всіх рівнях – від окремих користувачів до великих корпорацій та державних структур.

Стратегічне планування, освіта та постійне оновлення заходів безпеки стануть ключовими в забезпеченні стійкості українського бізнесу та суспільства в цілому перед обличчям кіберзагроз воєнного часу [1].