Наталія ФІЛІПЕНКО
докторка юридичних наук, професорка,
професорка кафедри права гуманітарно-правового факультету
Національного аерокосмічного університету
ім. М.Є. Жуковського «Харківський авіаційний інститут», м. Харків, Україна
ORCID: 0000-0001-9469-3650
e-mail: n.filipenko@khai.edu

Володимир ТРОФИМЕНКО
доктор юридичних наук, професор, заслужений юрист України,
заступник голови Державної служби спеціального зв'язку та захисту інформації України
ORCID: 0000-0001-6032-5550
e-mail: tvm.stolica@gmail.com

Ганна СПІЦИНА
докторка юридичних наук, професорка,
перший заступник директора Національного наукового центру
«Інститут судових експертиз ім. засл. проф. М.С. Бокаріуса», м. Харків, Україна
ORCID: 0000-0001-9131-0642
e-mail: Spitsyna.Hanna@nncise.org.ua

Сергій ЛУКАШЕВИЧ
кандидат юридичних наук, доцент,
професор кафедри права гуманітарно-правового факультету
Національного аерокосмічного університету ім. М. Є. Жуковського
«Харківський авіаційний інститут», м. Харків, Україна
ORCID: 0000-0001-8386-6237
e-mail: s.lukashevych@khai.edu

Aleksandar IVANOVIĆ
доктор філософії в галузі права, професор кримінології,
професор юридичного факультету Університету Чорногорії,
радник з питань освіти і науки в Управлінні поліції Чорногорії
e-mail: ialeksandar@t-com-me

КІБЕРПОЛІГОНИ ЯК ІНСТРУМЕНТ ПРОТИДІЇ ТЕРОРИЗМУ

Abstract. The article deals with the issues of developing and implementing a set of measures to ensure information and cyber-terrorist security at critical infrastructure facilities and aerospace enterprises with the development of measures to counteract hybrid criminal influences. The authors propose the creation of cyber training grounds that provide an opportunity to study complex cyber terrorist attacks and train cybersecurity specialists.
Keywords: critical infrastructure facilities, aerospace industry enterprises, cyber training ground, cyber terrorist threat, cybersecurity.

1. Вступ

Загрози для критичної інфраструктури, такі як кібератаки, терористичні акти, диверсії та військова агресія стають все більш актуальними в умовах сучасного глобалізованого світу. Одна з основних причин цього полягає в тому, що критична інфраструктура включає

системи, які підтримують життєдіяльність держави та її громадян - це енергетика, авіакосмічна галузь, водопостачання, транспорт, фінансові системи та охорона здоров'я. Пошкодження будь-якої з цих систем може призвести до катастрофічних наслідків не тільки для конкретного регіону, а й на міжнародному рівні.

Терористичні атаки на об’єкти критичної інфраструктури спрямовані на підрив не тільки матеріальних ресурсів, але й морального духу населення, створення відчуття небезпеки. У такому контексті терористичні акти можуть спричиняти вибухи або фізичні атаки на об'єкти підвищеної небезпеки - атомні станції, підприємства авіакосмічної галузі, гідротехнічні споруди чи транспортні системи [1, с.92-100].

Дуже небезпечними для об’єктів критичної інфраструктури мають військові дії. Військова агресія російської федерації проти України постійно супроводжується навмисними ударами по інфраструктурі для підриву економічної спроможності нашої країни та дестабілізації її роботи. Як свідчать данні [2], проведення військових дій на території України збройними силами країни-агресорки не обходить стороною об’єкти ядерної енергетики (Запорізька та Південноукраїнська АЕС), що становить серйозну потенційну загрозу для всього світу. Негативний вплив на безпеку об’єктів критичної інфраструктури носять ракетно-артилерійські обстріли об’єктів енергетичної галузі України. Зокрема, було нанесено значну шкоду шляхом обстрілів системи енергетики: ГЕС – Дніпровської, Кременчуцької, Київської, Каховської, ТЕС – Київської, Трипільської, Харківської, Старобешівської, Слов’янської, Миронівської, Луганської, Курахівської, Зуївської, Зміївської, Запорізької, Вуглегірської. Об’єкти інфраструктури із забезпечення життєдіяльності населення, електромережі, об’єкти із генерування та передачі електроенергії, водоканал, тепло- та газомережі, телефонні лінії та ін. постійно піддаються обстрілам по всій території України. Особливо гостро це стосується Запорізької, Херсонської, Миколаївської областей, окупованих, деокупованих та територій, де проводяться військові дії.

Значна шкода (часткова руйнація чи ліквідація) через ведення військових дій нанесена об’єктам портового господарства, транспортним магістралям, мостам, переправам, об’єктам промисловості, нафтопроводам та сховищам; газопроводам та ін. об’єктам критичної інфраструктури по всій території нашої держави [2].

Війна становить також значний вплив на авіакосмічну галузь, створюючи низку небезпек. Воєнні дії можуть призвести до збільшення авіаційних катастроф через можливі атаки на аеропорти, літаки та іншу інфраструктуру, що кратно впливає на небезпеку значних людських жертв та економічних збитків. Також перебої в роботі авіаційної та космічної інфраструктури через руйнування або пошкодження об'єктів може призвести до перебоїв у

постачанні товарів та послуг, а також до проблем з комунікаціями та навігацією. До того ж існують дуже великі ризики зменшення інвестицій в авіакосмічну галузь через невизначеність та небезпеки, пов'язані з війною. Це може призвести до уповільнення розвитку галузі та втрати робочих місць.

Серед найбільших загроз об’єктам критичної інфраструктури варто виділити кібертерористичні атаки, які можуть порушити роботу інформаційних систем, відповідальних за управління об'єктами інфраструктури, що може загрожувати безпеці мільйонів людей. Це робить їх особливо вразливими до зовнішніх втручань.

2. Аналіз публікацій, у яких ініційовано вирішення цієї проблеми. У загальному вигляді питання захисту об’єктів критичної інфраструктури від кібертерористичних атак присвячено праці багатьох учених, зокрема: О. М. Бандурки, В. В. Бондара, В. С. Батиргареєвої, Ю. В. Кузьменко, О. М. Литвинова, Ю. В. Орлова, Г. О. Спіциної, Н. Є. Філіпенко, В. Ю. Шепітька та ін. [3; 4; 5; 6 та ін.]. Однак більшість науковців розробляла один або декілька аспектів порушеної проблематики, не вирішуючи проблему в комплексному, інтегрованому вигляді. Особливо нерозробленими є питання захисту об’єктів критичної інфраструктури та підприємств авіакосмічної галузі під час війни, а також використання в Україні передового досвіду іноземних держав щодо подолання цих загроз та мінімізації ризиків та пошкоджень.

3. Результати та їх обговорення

Кібертерористичні атаки є однією з найбільших загроз сучасності, оскільки вони здатні паралізувати не лише окремі бізнеси або організації, але й цілі державні інституції. Такі атаки можуть спричинити серйозні порушення в роботі об’єктів критичної інфраструктури, підприємств авіакосмічної галузі, телекомунікаційних систем, що є критично важливими для координації діяльності служб надзвичайних ситуацій, медичних установ, поліції та інших організацій, відповідальних за захист життя та безпеки громадян. Порушення у функціонуванні таких систем може призвести до значних затримок у реагуванні на аварії, катастрофи чи інші надзвичайні ситуації, що, в свою чергу, становить реальну загрозу для життя та здоров'я багатьох людей.

За час повномасштабної війни кількість кібератак в Україні зросла у декілька разів порівняно з попередніми роками. Від 24 лютого 2022 зафіксували понад 4500 кібератак. У 2020 їх було всього 800, а в 2021 – близько 2000 [7].

Це підкреслює необхідність постійного вдосконалення систем кіберзахисту та належної підготовки фахівців у сфері інформаційної безпеки для забезпечення стійкості національних систем.

У низці державних та приватних організації, в умовах ізоляції та збільшення співробітників, які працюють віддалено, з'явився досвід активного перенесення частини своєї діяльності до мережі Інтернет [8]. У зв'язку з цим виникли нові реальні та потенційні загрози, розширився спектр кібератак на критично важливу та суспільно значущу інфраструктуру, що вимагає забезпечення стійкості функціонування державних і приватних корпоративних систем і мереж. Забезпеченню їхньої стійкості сприяє здійснення моделювання сценаріїв кіберзлочинів - комплексу взаємопов'язаних і взаємозалежних дій та операцій їх учасників у кіберпросторі – створенню надсучасних кіберполігонів.

Як зазначають науковці, кіберполігон – це сукупність програмно-апаратних засобів, об'єднаних єдиною розподіленою локальною мережею з виходом в Інтернет, що призначена для відпрацювання прикладних питань розробки, проектування та проведення випробувань програмно-технічних систем (комплексів) забезпечення інформаційної (інформаційно-психологічної) та кібербезпеки в ході реалізації функцій моніторингу, захисту та активних впливів, проведення багатосторонніх навчань, забезпечення узагальнення досвіду, розвитку форм, способів та методів прогнозування, запобігання, виявлення і протидії кризовим ситуаціям в кіберпросторі, здійснення заходів практичної підготовки, перепідготовки та підвищення кваліфікації військових (цивільних) фахівців (за національними стандартами та стандартами НАТО), а також для проведення фундаментальних та прикладних наукових досліджень у галузі інформаційної і кібербезпеки та кібероборони держави [9].

Кіберполігони стануть платформою для дослідження комплексних кібертерористичних операцій та підготовки кваліфікованих фахівців з кібербезпеки. Основною метою таких кіберполігонів є розробка та впровадження методологій, які забезпечать автоматизований моніторинг кіберпростору, аналітичну обробку даних, прогнозування можливих загроз та планування заходів протидії. Важливу роль відіграють як пасивні, так і активні заходи захисту, які дозволять ефективніше реагувати на інформаційні загрози та захищати критичну інфраструктуру. Кіберполігони також стануть інструментом для імітації реальних атак у віртуальному середовищі, що дозволить відпрацьовувати сценарії реагування на загрози у безпечних умовах, одночасно підвищуючи рівень компетенцій фахівців у цій галузі.

В Україні такі технології з кінця 2020 року стали системно розроблятися і з 2021-2022 рр. впроваджуватися у життя та діяльність правоохоронних структур. У навчальних закладах шляхом застосування нових технологій вживаються заходи щодо скорочення розриву між поширенням дистанційних методів навчання з використанням територіально-розподілених інформаційних систем та недостатнім рівнем їх захисту.

Наприклад, військовий інститут телекомунікації та інформатизації ЗСУ отримав навчально-тренувальний комплекс з кібербезпеки, який призначений для виявлення, реагування, протидії та попередження кіберзагроз. Також, комплекс можна використовувати для аналізу та розслідування кіберінцидентів, він призначений для підвищення якості освітнього процесу. До складу комплексу входять програмно-технічні засоби, ситуаційний центр, комплекс технічних засобів та включає в себе 80 автоматизованих робочих місць для курсантів та слухачів інституту, що навчаються за спеціальністю «Кібербезпека» [10].

Глобалізація призводить до посилення взаємопов'язаності державних і приватних структур. В Україні стрімко розвивається й приватний безпековий сервіс. Так, було запущено кіберполігон Unit Range [11], який створений для практичного тренування спеціалістів з кібербезпеки в умовах максимально наближених до реальних. В системі вже є понад 150 сценаріїв, а навчання проходять спеціалісти з українських державних та приватних органів. Відпрацювання кібердій здійснюється в замкненому віртуальному середовищі, яке імітує реальну інфраструктуру, яку фахівцям з кібербезпеки доведеться атакувати або захищати, в залежності від профілю діяльності. Це як правило хмарне рішення на віртуальних машинах (в нас повністю все в Amazon Web Services), де розгортаються сценарії які розробляються експертами з кібербезпеки. Такі сценарії максимально імітують хакерські атаки, або системи які треба атакувати (якщо тренуєш offense). Unit Range створювався безпосередньо під час війни, а його розробники враховували особливості ведення сучасної війни, де бойові дії часто комбінуються з кібератаками та спробами знищити цифрову інфраструктуру противника. Крім того, Unit Range надає інформаційну панель даних у реальному часі, де вимірюється результативність та профіль ризику для всіх членів команди, від керівників до звичайного IT-персоналу.

Підвищена пов’язаність інформаційних і кіберфізичних систем створює додаткові ризики у сфері забезпечення інформаційної безпеки, тому управління системним ризиком вимагає співпраці та обміну інформацією, спонукає до пошуку нових методів і засобів моніторингу, виявлення та нейтралізації кіберзагроз, мінімізації їхніх наслідків. Системні ризики вирізняються взаємопов'язаністю, поширюються в корелюючих системах, долаючи межі ситуаційної обізнаності або оперативного контролю. Ризики особливо небезпечні в електроенергетиці, атомній промисловості, на підприємствах авіакосмічної галузі, фінансах, держуправлінні тощо. Системний ризик починається з розподіленого вразливого стану, який змінюється в міру ускладнення соціальних і технологічних систем. Джерелом ризику може бути залежність взаємопов'язаних систем від інформаційних і комунікаційних технологій, що підтримують спектр додатків, що розширюється. Системний ризик може використовуватися зловмисником для дестабілізації або руйнування критичних функцій. Окремі інциденти, що

ініціюють, накопичуються і призводять до небажаних ефектів, які посилюються з наростаючим збитком. У результаті виникають каскадні ефекти, здатні зачепити як окремі корпоративні інформаційні системи, так і цифрову інфраструктуру одного або декількох секторів економіки.

Напади відбуваються з різних джерел і включають атаки типу «відмова в обслуговуванні», поширення шкідливих вірусів, які заражають мережу об'єкта критичної інфраструктури і використовують проломи в безпеці для доступу до конфіденційної інформації, а також підроблені електронні листи із запитом конфіденційних даних від співробітника, який нічого не підозрює, фішинг.

Особливо часто зловмисники зараз використовують можливості Штучного інтелекту. Так, мовний застосунок ChatGPT здатний за запитом користувача надавати готову до використання інформацію з інтернету. Таким чином він значно прискорює процес пізнання кримінальної сфери, впорядковуючи великі обсяги змістовної інформації. Вочевидь це дає зловмисникам можливість значно краще підготовити та згодом вчиняти посягання різних видів. Окрім наведеного ChatGPT здатний створювати код на різних мовах програмування, що відкриває безмежні можливості для кіберзлочинів [11]. З поточною версією застосунку вже можна створювати базові інструменти для різноманітних шкідливих цілей - фішингових сторінок, зламу баз даних тощо [12, с.1084-1096].

Моделювання фішингової атаки включає виявлення і блокування системою виявлення вторгнень і протидії комп'ютерним атакам, антивірусним програмним забезпеченням - електронних повідомлень, що містять шкідливий код, прочитання їх користувачами комп'ютерів, а також блокування передачі повідомлень на сервери зловмисників. Вектори атаки вибудовуються із застосуванням засобів комп'ютерної автоматизації. Для цього можуть розроблятися повні графові моделі деструктивних кібервпливів на мережеву інфраструктуру складних об'єктів критичного призначення.

Незважаючи на безліч методів моделювання загроз безпеки інформації і визнаних реєстрів або баз даних вразливостей програмного забезпечення, різних систем класифікації та оцінки критичності вразливостей, нерідко науковцями під час розроблення методики виявлення взаємозв'язків між виявленими вразливостями інформаційних систем та загроз безпеки інформації, як основне джерело відомостей про загрози та вразливості використовують тільки банки даних державних структур. За такого підходу до оцінки неактуальності загрози несанкціонованого відновлення віддаленої захищеної інформації для інформаційної системи з боку допущених до інформації користувачів обґрунтовується припущення про недоцільність дій з відновлення і так відомої порушнику інформації та

залишається поза увагою можливість активізації в такий спосіб заздалегідь впровадженого шкідливого програмного коду.

Також, подолати ці труднощі допомагають експериментальні методи, засновані переважно на моделюванні (CyberVAN) та емуляції (Testbed, INSALATA, SoftGrid та LARIAT), а також на методах накладання та демонстрації сценаріїв. В ході навчань нерідко імітується багатозв'язкова мережа (центри управління, центри обробки даних) та атаки на системи інформаційних та операційних технологій через Інтернет (SQL-ін'єкції, відключення Apache, знищення системи NMS, перехоплення дампу бази даних через протокол передачі файлів, програми-вимагачі, DDoS, SCADA тощо).

Щоб убезпечити об'єкти критичної інфраструктури від кібератак, ми пропонуємо:

1. Моделювання навчальної обстановки методом імітації кібератак.

З кожним роком багатокрокові скоординовані розподілені кібератаки зі складною організацією, реалізацією і безліччю цілей змінюються, проводяться дедалі частіше і витонченіше. На етапі вторгнення кібератаки зазвичай виявляють із використанням сигнатурних, поведінкових, комбінованих та інших методів. У сучасному ландшафті кібертерористичних загроз на перший план висувається створення інтелектуальних засобів захисту, що дають змогу виявляти цільові атаки на початкових етапах їх реалізації.

Відмінною рисою критичної інфраструктури є її функціонування за допомогою взаємодії зі світовим кіберпростором, що формує додаткові уразливості для можливої їхньої експлуатації при здійсненні деструктивних впливів на державні і муніципальні системи, об'єкти економіки без безпосереднього проникнення на територію держави та оголошення санкцій. У кіберпросторі можливе дистанційне керування і переведення у режим функціонування в інтересах порушника аж до збоїв у роботі автоматизованих інформаційних систем і відключення об'єктів критичної інфраструктури. Особливо небезпечним є переведення об'єкта у режим надзвичайної ситуації, що призводить до його руйнування. Під час проведення навчань у кіберпросторі моделювання кібертерористичних атак є важливим етапом їхньої підготовки. Моделювання засноване на формалізації логічного ланцюжка: взаємодії множин виявлених уразливостей програмного забезпечення, релевантних загроз, імовірних сценаріїв реалізації загроз, можливих кіберфізичних наслідків, кількісної оцінки ризиків порушення кібербезпеки.

Аналіз зарубіжного досвіду проведення кібертерористичних навчань

Останніми роками кіберазловмисники продемонстрували готовність до кіберактивності проти об'єктів критичної інфраструктури та підприємства авіакосмічної галузі шляхом використання доступних в Інтернеті ресурсів та програмного забезпечення.

Кібербезпека як проблема, що постійно розширюється і загострюється, охоплює поєднання фізичних, програмних і людських систем. Для вироблення навчальної платформи у світі організовується низку заходів. Тренінги відіграють ключову роль у формуванні та перевірці організаційної та технічної готовності для відбиття реальних кібератак.

Як зазначають спеціалісти [14; 15 та ін.], комплексному навчанню кібербезпеки технічних фахівців у США сприяє програма Cybersecurity Defense Initiative (CDI), безоплатно проводяться курси для її освоєння. Курси «Комплексний захист кібербезпеки» і «Спеціаліст оперативного реагування з кібербезпеки» сертифіковані Міністерством внутрішньої безпеки США. Секретна служба США (USSS) за участю правоохоронних органів і партнерів із приватного сектору проводить навчання з реагування на інциденти кібербезпеки та відпрацювання стратегій пом'якшення їхніх наслідків методом віртуального моделювання атак із використанням програм-здирників і криптовалюти. На семінарах FEMA Region III з кібербезпеки здійснюється презентація плану реагування на інциденти, проводяться штабні тренування. Для співробітників федерального уряду та інших органів влади, державних підрядників доступне сформоване на безкоштовній онлайн-платформі віртуальне навчальне середовище кібербезпеки FedVTE, кероване DHS. Середовище, доступ до якого здійснюється за запитом, містить модулі моніторингу інцидентів, управління ризиками та аналізу шкідливих програм. Федеральні департаменти використовують системи виявлення вторгнень Einstein і US-Cert. Для захисту від атак шкідливого ПЗ під час підключення до федеральних систем DHS вживає заходів щодо скорочення кількості точок доступу в Інтернет [15].

Модель актуальних кібертерористичних може розроблятися для окремих систем, мереж та інформаційно-телекомунікаційної інфраструктури, на якій вони функціонують. Загрози, пов'язані інтерфейсами взаємодії із системами та мережами, ініціюються під час відпрацювання навчальних епізодів доведенням ввідних.

Процес моделювання кібертерористичних атак включає визначення можливих негативних наслідків від їх реалізації, умов реалізації та джерел загроз, оцінку можливостей зловмисників, сценаріїв реалізації загроз і небезпеки кібератак. Цілі та сценарії здійснення загроз, прогнозовані наслідки від їхньої реалізації уточнюються експертним методом. Критично важливі системи зв'язку та енергопостачання вважаються настільки значущими для США, що їхнє виведення з ладу або руйнування може мати згубний вплив на різні види безпеки: національну, економічну, громадську. Офіційні особи визнають усунення наслідків навмисних кібератак на критично важливі інфраструктури дорогим для країни [16]. Тому для розв'язання системних проблем необхідні визначення пріоритетів, розроблення загальної термінології, організація реагування на інциденти.

4. Висновки.

Стан захищеності об'єктів критичної інфраструктури та підприємства авіакосмічної галузі є невід'ємною складовою національної безпеки України. На сьогоднішній день гостро постає проблема фінансування та матеріально-технічного забезпечення тих об'єктів, які постраждали внаслідок військових дій. В умовах терміновості були оперативно доопрацьовані нормативно-правові акти, що стосуються створення ефективних умов для функціонування та відновлення критичної інфраструктури під час військового стану. Це питання є основоположним у процесі формування продуктивних механізмів для забезпечення інтересів національної безпеки нашої країни. У зв'язку з цим, подальшого наукового вивчення вимагають питання адаптації міжнародного досвіду щодо системи захисту та підвищення стійкості критичної інфраструктури, зокрема в контексті військових загроз. Необхідно врахувати, що ефективна реалізація заходів щодо захисту критичної інфраструктури вимагатиме інтеграції нових технологій, впровадження інноваційних рішень та розвитку співпраці між державними структурами і приватними компаніями. Це дозволить не тільки відновити пошкоджені об'єкти, а й значно зміцнити їхню стійкість до потенційних загроз у майбутньому.

З цією метою пропонується:

По-перше, створювати розгалужену систему державних та приватних кіберполігонів, що дозволить:

1. Досліджувати реальні сценарії кібертерористичних атак: навчальні полігони дозволять імітувати різні типи атак, від DDoS-атак до фішингу та викрадення даних. Це дасть можливість дослідникам та фахівцям з кібербезпеки вивчати поведінку зловмисників, розробляти нові методи захисту та вдосконалювати існуючі системи безпеки.

2. Підготувати висококваліфікованих спеціалістів: навчання на кіберполігонах дозволить майбутнім фахівцям з кібербезпеки набути практичних навичок, необхідних для роботи в реальному світі. Вони зможуть відпрацьовувати різні сценарії, розвивати аналітичні здібності та вдосконалювати свої навички реагування на кіберзагрози.

3. Розробити методи автоматизованого моніторингу: за допомогою штучного інтелекту та машинного навчання можна створити системи, які автоматично виявлятимуть підозрілу активність в мережі.

4. Вдосконалити інструменти аналітичної обробки інформації: аналіз великих обсягів даних дозволить виявити тенденції та патерни кібертерористичних атак на об’єкти критичної інфраструктури та підприємства авіакосмічної галузі, що допоможе в прогнозуванні та запобіганні майбутнім інцидентам.

5. Створити системи прогнозування та планування: завдяки аналізу даних та моделюванню можна буде прогнозувати майбутні кіберзагрози та розробляти плани їх нейтралізації.

6. Забезпечити ефективну протидію інформаційним загрозам: навчання на кіберполігонах дозволить розробити стратегії пасивної та активної протидії кібертерористичним нападам, включаючи розробку нових технологій захисту та удосконалення існуючих систем безпеки.

Створення кіберполігонів є ключовим кроком для забезпечення кібербезпеки в сучасному світі. Це дозволить підготувати нове покоління фахівців з кібербезпеки, розробити ефективні методи захисту та забезпечити безпеку інформаційних систем від кібернападів.

По-друге, з метою попередження кібертерористичних атак на об'єкти критичної інфраструктури та підприємства авіакосмічної галузі пропонуємо:

1. Посилити кібербезпеку державних та приватних підприємств: Впровадити багатофакторну автентифікацію (MFA) для всіх користувачів та адміністраторів. Регулярно оновлювати програмне забезпечення та операційні системи, щоб усунути відомі вразливості. Застосовувати системи виявлення та запобігання вторгнень (IDS/IPS) для моніторингу мережевого трафіку та блокування підозрілих дій. Встановити систему резервного копіювання даних та відновлення після катастрофи, щоб мінімізувати збитки від кібератак. Проводити регулярні навчання персоналу з питань кібербезпеки та безпечного користування Інтернетом.

2. Покращити співпрацю між державними органами: Повідомляти про підозрілі кіберзагрози та інциденти до відповідних органів. Брати участь у спільних навчаннях та тренінгах з кібербезпеки. Сприяти розробці та впровадженню національних стандартів кібербезпеки.

3. Залучати приватний сектор: Створити платформу для обміну інформацією про кіберзагрози та кращі практики. Заохочувати інвестиції в розробку та впровадження інноваційних рішень кібербезпеки. Співпрацювати з дослідницькими установами для розвитку нових технологій захисту від кібератак.

4. Збільшити обізнаність населення: Проводити інформаційні кампанії про загрози кібербезпеки та способи захисту. Навчати дітей та молодь основам кібербезпеки. Створити онлайн-ресурси з інформацією про кібербезпеку та рекомендації щодо захисту.

Застосування цих заходів допоможе значно підвищити рівень кібербезпеки об'єктів критичної інфраструктури і підприємств авіакосмічної галузі та мінімізувати ризики кібертерористичних атак.

Використана література:

1. Leblanc S.P., Partington A., Chapman I.M., Bernier M. An overview of cyber attack and computer network operations simulation. SpringSim (MMS), 2011, pp. 92–100.

2. Кузьменко Ю. В., Коропатов О. М., Думанський Р. В. Адміністративно-правове забезпечення захисту об'єктів критичної інфраструктури України під час воєнного стану. Юридичний Бюлетень. Випуск 27. 2022. DOI https://doi.org/10.32850/LB2414-4207.2022.27.08 с. 63

3. Батиргареєва В. С., Бабенко А. М. Аналіз сучасної криміногенної ситуації в Україні як інформаційна модель для розробки стратегії зменшення можливостей вчинення злочинів. Архів кримінології та судових наук : наук. журнал / Ред. кол.: О. М. Клюєв, В. С. Батиргареєва, Г. О. Спіцина та ін. Харків : ХНДІСЕ, 2020. No. 1. С 39–53.

4. Mykola Nechyporuk, Volodymyr Pavlikov, Nataliia Filipenko, Hanna Spitsyna, Ihor Shynkarenko Cyberterrorism Attacks on Critical Infrastructure and Aviation: Criminal and Legal Policy of Countering. Integrated Computer Technologies in Mechanical Engineering – 2020. Synergetic Engineering P. 206–220. ISBN 978-3-030-66716-0 ISBN 978-3-030-66717-7 (eBook). URL: https://doi.org/10.1007/978-3-030-66717-7.

5. Філіпенко Н. (2022) Протидія кібератакам на об'єкти критичної інфраструктури та життєзабезпечення під час військової агресії проти України. Український дослідницький простір в умовах війни: адаптація й перезавантаження технічних і юридичних наук: збірник матеріалів доповідей учасників міжнародної науково-практичної конференції. (Харків-Рига, 31 травня 2022 р.). Харків, 2022. С. 213-217.

6. Кузьменко Ю.В., Бондар В.В. Захист об'єктів критичної інфраструктури: адміністративно-правове забезпечення. Юридичний бюлетень. 2021. Вип. 21. С. 67-72.

7. Національний центр резервування державних інформаційних ресурсів (НЦ). https://uss.gov.ua/service/natsionalnyj-tsentr-rezervuvannya-derzhavnyh-informatsijnyh-resursiv-nts/#:~:text=За%20час%20повномасштабної%20війни%20кількість,а%20в%202021%20–%20близько%202000.

8. Lallie H.S., Shepherd L.A., Nurse J.R.C., Erola A., Epiphaniou G., Maple C., Bellekens X. (2021). Cyber security in the age of COVID-19: a timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers and Security, 105, [102248]. URL: http://doi.org/10.1016/j.cose.2021.102248

9. Даник Ю.Г. (2019) Особливості створення кіберполігонів для дослідження комплексних кібердій та підготовки фахівців з кібербезпеки. Confrontation in the cybernetic. Modern Information Technologies in the Sphere of Security and Defence № 1(34)/2019. DOI:10.33099/2311-7249/2019-34-1-95-102

10. ВІТІ отримав кіберполігон. https://mil.in.ua/uk/news/viti-otrymav-kiberpoligon/

11. Єгор Аушев запустив кіберполігон для тренування спеціалістів — там вже є понад 150 сценаріїв атаки і захисту. https://dou.ua/lenta/news/about-unit-range/

12. Europol Tech Watch Flash. www.europol.europa.eu Retrieved from https://www.europol. europa.eu/cms/sites/default/files/documents/Tech%20Watch%20Flash%20-%20The%20Impact%20of%20Large%20Language%20Models%20on%20Law%20Enforcement.pdf [in English].

13. Філіпенко Н.Є., Лукашевич С.Ю. (2023) Інформаційні методики дослідження кримінальних правопорушень, вчинених з використанням технологій штучного інтелекту. Наукові перспективи (Серія «Державне управління», Серія «Право», Серія «Економіка», Серія «Медицина», Серія «Педагогіка», Серія «Психологія») Випуск № 11(41)2023. Київ. 2023. № 1(7) С.1084-1096.

14. Thakur K, Ali ML, Jiang N et al. Impact of cyber-attacks on critical infrastructure. In: 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE

International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), 2016. New York, NY, USA.

15. Kavak H., Padilla J.J., Vernon-Bido D., Diallo S.Y., Gore R.J., Shetty S. Simulation for Cybersecurity: State of the Art and Future Directions. Journal of Cybersecurity, Volume 7, Issue 1, 2021. DOI: 10.1093/cybsec/tyab005

16. CISA, Cyber Storm VI: National Cyber Exercise, D.o.H. Security, Editor, 2020. URL: http://www.cisa.gov/cyber-storm-vi