УДК 004.738.5:351.862.4
DOI: 10.31733/15-03-2024/2/371-374

Ілля ОРЕХОВ
слухач магістратури факультету
підготовки фахівців для підрозділів
превентивної діяльності

Наталія КОМИХ
доцент кафедри гуманітарних
дисциплін та психології
поліцейської діяльності
Дніпропетровського державного
університету внутрішніх справ,
кандидат соціологічних наук, доцент

ПРІОРІТЕТИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

У сучасному світі, де технологічний прогрес стає двигуном соціального, економічного та політичного розвитку, кібербезпека стає невід'ємною складовою національної безпеки для багатьох країн, включаючи Україну. Високий рівень залежності від інформаційних технологій і кіберпростору породжує нові виклики та загрози, що вимагають відповідальної та комплексної стратегії для забезпечення захисту від кібернебезпеки.

Забезпечення кібербезпеки є важливим завданням для будь-якої країни, включаючи Україну. Національні пріоритети в цьому напрямку можуть включати ряд заходів і стратегій для захисту інформаційних ресурсів, мереж і систем від кіберзагроз.

Створення ефективної стратегії кібербезпеки для України вимагає комплексного підходу та урахування різноманітних аспектів, що включають технічні, правові, освітні та міжнародні аспекти.

Перший крок полягає в ретельному аналізі потенційних кіберзагроз і ризиків для країни. Визначення потенційних сценаріїв атак, виявлення критичних інфраструктур та оцінка наслідків можливих інцидентів є важливим етапом.

Створення адекватного законодавчого середовища є ключовим елементом стратегії. Це включає прийняття та актуалізацію законів, що визначають відповідальність за кіберзлочини, механізми співпраці з приватним сектором та міжнародними партнерами [5, с. 90-93].

Запровадження програм підвищення обізнаності щодо кібербезпеки серед населення, бізнес-спільноти та публічних служб є необхідним для створення високої культури кібербезпеки в країні.

Визначення та захист критичних інфраструктур, таких як енергетика, транспорт, телекомунікації, є пріоритетом. Розробка та впровадження стандартів безпеки для цих секторів грає ключову роль у стратегії.

Україна має активно взаємодіяти з міжнародними організаціями та іншими країнами для обміну досвідом та інформацією, а також для створення міжнародних механізмів взаємодії в разі кіберзагроз.

Забезпечення країни сучасними технічними засобами для виявлення, аналізу та відповіді на кіберзагрози. Це включає розробку та впровадження систем інтелігентного моніторингу та виявлення вторгнень.

Створення ефективної системи кризового управління для швидкого та координованого реагування на кіберінциденти та відновлення роботи систем після атак.

Стратегія кібербезпеки має бути динамічною та адаптивною, враховуючи постійні зміни в кіберзагрозах та технологічному середовищі. Ключовим елементом є також постійний моніторинг та оновлення стратегії для відповіді на нові виклики у сфері кібербезпеки.

Законодавство та регулювання в галузі кібербезпеки в Україні визначається рядом нормативно-правових актів, спрямованих на забезпечення ефективного захисту інформаційної безпеки країни.

Однією з ключових правових основ є «Про Кібербезпеку» – закон, що визначає основні положення та принципи захисту інформаційних систем, визначає відповідальність

за порушення кібербезпеки, а також визначає ролі та обов'язки органів влади та підприємств.

У рамках боротьби з кіберзлочинами прийнято ряд законів, що визначають кримінальну відповідальність за кібератаки, крадіжку конфіденційної інформації, а також інші правопорушення в цій сфері.

Законодавство визначає процедури та вимоги стосовно стандартів безпеки та сертифікації інформаційних систем, зокрема, для критичних об'єктів інфраструктури.

Закони визначають механізми партнерства та обміну інформацією між державними органами та приватним сектором для спільного захисту від кіберзагроз.

Україна враховує міжнародний аспект кібербезпеки, забезпечуючи відповідність національного законодавства міжнародним стандартам і участь у міжнародних ініціативах [1, с. 100-108].

Цей законодавчий фреймворк сприяє створенню ефективної системи кібербезпеки в Україні, обумовлює відповідальність у всіх сферах суспільства та сприяє розвитку та модернізації існуючих заходів та стратегій в цій області.

Забезпечення безпеки в кіберпросторі починається з ефективного підвищення обізнаності та навчання серед різних шарів суспільства. Перш за все, важливо розробити та впровадити комплексні навчальні програми для громадян, охоплюючи різні вікові групи та соціальні верстви. Ці програми повинні включати основи кібербезпеки, методи виявлення соціально-інженерних атак, та відповідальність в інтернет-просторі.

Другий аспект полягає в підвищенні кібербезпекової культури серед бізнес-середовища. Підприємства повинні бути свідомі ризиків та приймати заходи для захисту своїх інформаційних ресурсів. Розробка та надання навчальних курсів для працівників є важливим елементом в цьому процесі, адже вони повинні мати не лише технічні знання, але й навички виявлення та врегулювання інцидентів.

Уряд повинен ініціювати та підтримувати ініціативи з підвищення обізнаності в галузі кібербезпеки серед державних службовців. Це включає надання періодичних тренінгів, семінарів та вебінарів, щоб управлінці та робітники могли ефективно взаємодіяти та реагувати на кіберзагрози.

Завершальним етапом є розширення співпраці з освітніми установами та дослідницькими організаціями для створення передових програм з образотворчою кібербезпеки. Це сприятиме підготовці фахівців з високим рівнем експертизи, які зможуть вирішувати сучасні виклики в галузі кібербезпеки. Усі ці заходи спільно сприятимуть підняттю рівня обізнаності та компетентності населення в кібербезпеці, зменшуючи загрози інформаційної безпеки для країни в цілому [4, с. 140-145].

Захист критичних інфраструктур є однією з ключових складових національної кібербезпеки України. Критичні інфраструктури охоплюють енергетичні, транспортні, телекомунікаційні та інші системи, які є життєво важливими для функціонування країни. Забезпечення їхньої стійкості та захищеності від кіберзагроз вимагає комплексного підходу.

Важливо визначити та класифікувати критичні інфраструктури, ідентифікувати їхні слабкі місця та потенційні ризики. Для цього потрібна система моніторингу та аналізу, яка дозволить вчасно виявляти непередбачувані кіберзагрози.

Важливо розробити та впровадити заходи щодо кіберзахисту. Це може включати удосконалення кіберструктури, впровадження ефективних механізмів ідентифікації та аутентифікації, а також встановлення систем захисту від вторгнень.

Забезпечення реагування на кіберінциденти також є важливою частиною захисту критичних інфраструктур. Розробка та впровадження планів контингенції, тренування персоналу для ефективної реакції на інциденти та впровадження систем моніторингу для виявлення аномалій – це ключові аспекти у підвищенні стійкості систем.

Співпраця з приватним сектором та міжнародними організаціями є необхідною для обміну інформацією та вдосконалення кіберзахисту. Важливо встановити партнерства та об'єднати зусилля для виявлення та протидії кіберзагрозам, які можуть мають глобальний характер.

Міжнародне співробітництво в галузі кібербезпеки є надзвичайно важливим аспектом для забезпечення ефективного захисту від кіберзагроз. Перш за все, це означає активну участь України у міжнародних форумах та організаціях, де обговорюються та формуються стандарти та стратегії кібербезпеки. Така участь дозволяє країні отримувати доступ до найновіших інформаційних технологій та методів захисту [5, с. 90-93].

Другий аспект полягає у встановленні та удосконаленні багатосторонніх співпраць

із партнерами з інших країн. Обмін досвідом, інформацією про кіберзагрози та спільні навчальні ініціативи сприяють підвищенню загальної рівня кібербезпеки.

Національна кібербезпекова стратегія має враховувати спільні міжнародні стандарти та бути відкритою до адаптації до найкращих практик. Координація з іншими країнами допомагає вирішувати транскордонні кіберзагрози, такі як кібершпигунство та кібертероризм.

Важливо встановлювати більше двосторонніх угод та меморандумів з іншими країнами для обміну інформацією та спільного реагування на кіберінциденти. Розвиток міжнародного партнерства у сфері кібербезпеки є ключовим елементом у створенні колективної оборони від сучасних кіберзагроз.

Розвиток кіберзахисту в армії є критично важливим в умовах сучасних технологічних загроз та кібератак. Забезпечення безпеки інформаційних систем та комунікаційних мереж стає необхідністю для успішного функціонування військових структур.

Армія повинна активно інвестувати в розробку та вдосконалення технічних рішень для кіберзахисту. Це включає в себе розробку та впровадження спеціалізованих програмних продуктів, які виявляють та блокують кіберзагрози.

Не менш важливою є підготовка персоналу. Військові повинні мати високий рівень обізнаності щодо кібербезпеки, а також отримувати регулярне оновлення знань та тренування з виявлення та протидії кіберзагрозам. Створення спеціальних військових підрозділів для кіберзахисту та кібероперацій може бути ефективним рішенням.

Співпраця з приватним сектором та науковими установами є ключовою для впровадження передових технологій та стратегій в області кіберзахисту. Армія повинна активно взаємодіяти з компаніями, які спеціалізуються на кібербезпеці, для обміну досвідом та отримання доступу до передових технологічних розробок [2, с. 119-121].

Важливо вдосконалювати стратегії виявлення та реагування на інциденти кібербезпеки. Швидке виявлення та ізоляція кіберзагроз дозволяє мінімізувати можливість значних втрат та перерв у військових операціях.

Загалом, розвиток кіберзахисту в армії передбачає комплексний підхід, який включає технічні інновації, підготовку персоналу, співпрацю зі зовнішніми партнерами та постійне вдосконалення стратегій безпеки. Тільки таким чином можна забезпечити високий рівень кіберзахисту в армії та ефективну відповідь на сучасні кіберзагрози.

Створення Центру кіберзахисту є важливим етапом для країни в забезпеченні високого рівня кібербезпеки. Цей Центр має бути спеціалізованою установою, яка координує та управляє всіма аспектами захисту інформаційних систем в країні.

Центр кіберзахисту повинен мати чіткий мандат, визначений національним законодавством, що визначає його функції та повноваження. Його основним завданням є розробка та реалізація стратегій кібербезпеки, а також виявлення, аналіз та реагування на кіберзагрози.

Центр сприятиме ефективній координації зусиль між державними органами, приватним сектором та іншими зацікавленими сторонами. Йому слід створити механізми для обміну інформацією та співпраці між різними суб’єктами для швидкого та ефективного реагування на кіберзагрози.

Центр повинен мати кваліфікований персонал із глибокими знаннями у сфері кібербезпеки. Важливо забезпечити постійне навчання та підвищення кваліфікації для персоналу з урахуванням швидко змінюючихся технологічних та кіберзагроз [4, с. 140-145].

У Центрі має бути доступ до сучасних технічних рішень і інфраструктури для ефективного виявлення та захисту від кіберзагроз. У його складі потрібні аналітичні інструменти, системи моніторингу, тестування безпеки та інші засоби для виявлення та аналізу інцидентів.

Центр маєактивно співпрацювати з міжнародними кібербезпековими організаціями та іншими країнами для обміну інформацією, прийняття кращих практик та координації заходів з кіберзахисту на міжнародному рівні.

Розвиток технічної інфраструктури в Україні передбачає значний акцент на мережеву інфраструктуру. Це включає в себе широкосмуговий інтернет, розгортання високошвидкісних мереж для ефективного обміну даними та забезпечення стійкості до кіберзагроз. Створення інфраструктури для 5G-зв’язку стає однією з ключових стратегічних ініціатив для забезпечення високошвидкісного та надійного з’єднання.

Розбудова центрів обробки даних є важливим компонентом розвитку технічної

інфраструктури. Використання хмарових технологій дозволяє збільшити ефективність обробки та зберігання великих обсягів інформації, забезпечуючи при цьому високий рівень безпеки та доступності.

Розвиток кіберфізичних систем, що поєднують в собі обчислювальні та фізичні компоненти, визначає новий етап технічної інфраструктури. Упровадження розумних міст, промислових об'єктів та транспортних систем збільшує автоматизацію та взаємодію між різними секторами, в той час забезпечуючи відповідні заходи кіберзахисту.

Під час розвитку технічної інфраструктури слід враховувати кібербезпеку як невід'ємну складову. Запровадження передових засобів шифрування, систем виявлення та протидії кіберзагрозам, а також регулярне оновлення кіберзахисних заходів, стає критичним для запобігання інцидентів та збереження стійкості систем [3, с. 23-28].

Отже, у змінливому світі кіберзагроз, Україна має активно реагувати на виклики, пов'язані із кібербезпекою, здійснюючи важливі кроки для захисту своїх інформаційних ресурсів та критичних інфраструктур. Здійснення комплексних заходів, від розробки стратегії до підвищення обізнаності та технічного розвитку, є важливими кроками для забезпечення ефективного кіберзахисту. Тільки через співпрацю всіх зацікавлених сторін, Україна зможе відповісти на виклики кіберпростору та зберегти свою кібербезпеку в умовах постійної зміни технологічного ландшафту.

1. Бакалінська О., Бакалинський О. Правове забезпечення кібербезпеки в Україні. *Підприємництво, господарство і право.* 2019. № 9. С. 100-108.

2. Богуш В. М. Кібербезпека та захист критичної інформаційної інфраструктури. *Правова інформатика.* 2015. № 2. С. 119-121.

3. Веселова Л. Особливості державної політики України у сфері забезпечення кібербезпеки в умовах гібридної війни. *Науковий вісник Херсонського державного університету.* Серія: «Юридичні науки». 2019. № 2. С. 23-28.

4. Геращенко Ю. Державна політика у сфері кібербезпеки в Україні. *Вчені записки ТНУ імені В.І. Вернадського.* Серія: «Державне управління». 2019. № 1. С. 140-145.

5. Даник Ю. Г. Основи кібербезпеки та кібероборони: підручник. Видання друге, перероб. та доп. Одеса.: ОНАЗ ім. О.С. Попова, 2019. 320 с.

УДК 004.738.5:351.862.4:341.31
DOI: 10.31733/15-03-2024/2/374-375

Артур ПАНТЮШЕНКО
курсант ННІ права та підготовки
фахівців для підрозділів
Національної поліції

Олена БОЙКО
старший викладач кафедри
тактико-спеціальної підготовки
Дніпропетровського державного
університету внутрішніх справ

АКТУАЛЬНІ ПИТАННЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ УКРАЇНИ ПІД ЧАС ВОЄННОГО СТАНУ В СУЧАСНОМУ ІНФОРМАЦІЙНОМУ ПРОСТОРІ

Звертаючи увагу на виклики сьогодення перед Україною, захист прав, свобод, суверенітету і територіальної цілісності посідає значне місце. Підсилюючим фактором для захисту є військові дії на території України, які дуже сильно шкодять соціальному середовищу України. Крім того, зовнішні фактори це лише одна частина небезпеки для держави, оскільки існують і внутрішні фактори, такі як кібератаки, кіберзлочини, шахрайства на гуманітарній основі, розкрадання державного майна шляхом проведення відкритих торгів з основою фіктивних публічних закупівель через сайт «Прозоро». Також, у зв'язку із військовою агресією, постає питання захисту персональних даних громадян у цифрову епоху, оскільки сьогодні дістати інформацію про особу через соціальні мережі чи інші сайти дуже проста задача для шахраїв та агентів. І тому нижче ми висвітлимо напрямки для підвищення ефективності інформаційного захисту.