УДК 004.9: 004.056
DOI: 10.31673/2409-7292.2020.022731

Мужанова Т.М.

ГЕОПРОСТОРОВИЙ ПІДХІД ДО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

У статті розглянуто роль та функції геоінформаційних технологій у забезпеченні кібербезпеки організації. Встановлено, що основною метою застосування геоінформаційних систем (ГІС) у галузі кібербезпеки є досягнення всебічного спільного бачення ситуації в кіберпросторі усіма суб'єктами управління організації, що дозволить забезпечити ефективне і своєчасне прийняття рішень щодо формування обізнаності, запобігання, захисту, реагування та відновлення після інцидентів кібербезпеки. Проаналізовано концепцію застосування ГІС у галузі кібербезпеки компанії-виробника ГІС-платформ ESRI, яка пропонує впроваджувати геопросторову модель захисту периметру з метою виявлення й оцінювання спроб компрометації ІТКС та формувати лінії кіберпідтримки для виконання критичних місій організації.

Ключові слова: кібербезпека, кіберзахист, геоінформаційні технології, геоінформаційні системи.

Вступ

В умовах активної розбудови кіберпростору з кожним днем зростає кількість, різноманіття, а також масштаби негативних впливів на об'єкти інформаційно-телекомунікаційних систем/ Так, відповідно до статистики, кількість порушень кібербезпеки у 2019 році зросла на 11% у порівнянні з попереднім роком і на 67% - у порівнянні з 2014. Втрати бізнесу та організацій від кіберінцидентів постійно зростають і, за розрахунками експертів, до 2021 року сягнуть позначки у 6 трильйонів доларів за рік [1]. Водночас, фахівці переконані, що 80% кіберпорушень можуть не статися за умови проведення належних превентивних заходів з кібербезпеки, зокрема оцінки вразливостей і загроз [2]. Кіберзагрози впливають не лише на інфраструктуру ІТКС організації або її керівництва. Вони можуть негативно позначитися на виконанні її основних функцій. Тому зусилля із забезпечення кібербезпеки мають оцінюватися з точки зору їх безпосереднього внеску в успішну реалізацію проектів організації та виконання її основної місії.

Сьогодні кіберзахист не може обмежуватися технічними заходами, а має бути інтегрований у традиційні види діяльності з безпеки, такі як забезпечення фізичної безпеки та безпеки персоналу, бути частиною загально-організаційних зусиль з метою захисту усіх бізнес-операцій як від зовнішніх, так і від внутрішніх загроз. Активності з кібербезпеки мають бути у числі пріоритетних та узгоджуватися із стратегічною діяльністю бізнесу. Зростанню ефективності забезпечення кібербезпеки сприяють технології геоінформаційних систем (ГІС), які формують основу для створення спільної ситуаційної обізнаності фахівців з міждисциплінарних видів діяльності в межах організації.

ГІС - це автоматизована система, яка забезпечує збирання, зберігання, інтеграцію та графічне представлення просторової інформації у вигляді схем або карт. Більшість сучасних ГІС здійснюють комплексну обробку інформації, використовуючи такі функції: введення і редагування даних, підтримка моделей просторових даних, зберігання інформації, перетворення систем координат і трансформація картографічних проекцій, растрово-векторні операції, вимірювальні операції, полігональні операції, операції просторового аналізу, різні види просторового моделювання, цифрове моделювання рельєфу та аналіз поверхонь, подання результатів у різних формах, а також багато різних специфічних, залежно від призначення системи, функцій моделювання [3].

Постановка завдання. Розглянути засади використання ГІС як засобу підвищення ефективності забезпечення кібербезпеки і, як наслідок – виконання місій (завдань) організації.

Основна частина.

Сучасні організації дуже зацікавлені у забезпеченні безпеки кіберпростору, оскільки це дозволяє їм ефективно й економічно вигідно координувати діяльність роз'єднаних у просторі підрозділів або частин бізнесу практично в реальному часі. Особливо важливим є вчасно і вірно визначати, коли і де необхідно впроваджувати заходи з кібербезпеки. З огляду на

недостатність ресурсів для виконання усіх завдань з кіберзахисту на усіх об’єктах ІТКС упродовж усього часу їх роботи, організації потребують засобів, які допоможуть заздалегідь обрати пріоритетні дії з кібербезпеки, ліквідовуючи таким чином прогалини в системі безпеки і реагування на інциденти.

ГІС відіграють важливу роль у вирішенні зазначених проблем, оскільки здатні моделювати як фізичне, так і віртуальне середовище організації, збирати й аналізувати необхідні дані, швидко ідентифікувати загрози і обґрунтовувати планування оптимальної діяльності з кібербезпеки. Поєднуючи традиційні кіберіндикатори з геопросторовими даними, організація може швидко виявляти й обирати пріоритетні з усіх видів кіберзагроз, в тому числі природних і антропогенних, навмисних і випадкових, створюючи комплексну модель, яка інтегрує всі наявні дані. Результатом є здатність організації швидко і гнучко впроваджувати заходи фізичного і кіберзахисту у відповідь на несанкціоновані втручання в роботу сервісів і комплексні вторгнення, а також встановлювати першочергові превентивні дії з метою запобігання перебоям або пом’якшення їхнього впливу. Відповідно до бачення Командування ЗС США з питань навчання та доктрини (TRADOC) [4] кіберпростір складається з чотирьох рівнів, кожен з яких має вузли, які можна локалізувати у просторі та часі. Сюди входять дані, пристрої, мережі та географічне розташування.

Рівні даних часто розподіляють залежно від типу використовуваного вузла, яким може бути людина чи пристрій. Однак, на думку фахівців, правильно розмежовувати вузлові рівні відповідно до типу потоку даних. Так, для обміну інформацією на соціальному рівні (між людьми) документи надходять на рівні пристроїв; для обміну документами пакети рухаються на мережевому рівні; а для обміну пакетами електромагнітна енергія протікає між двома конкретними точками у просторі та часі, представленими географічним рівнем.

Пристрої ІТКС виконують свої функції на різних рівнях. Так, наприклад, якщо маршрутизатор виходить з ладу на рівні мережі, деякій підмножині хостів на рівні пристроїв буде відмовлено в необхідних пакетах. Втрата пакетів призводить до того, що пристрої не можуть обмінюватися документами, а деяким користувачам відмовляють у необхідній інформації. Саме втрата або пошкодження інформації, а не пристроїв, безпосередньо впливає на виконання місій організації. Географічний рівень є загальним інтегруючим каркасом для всіх розглянутих вище рівнів. Інтеграція досягається шляхом геолокації всіх вузлів, включаючи людей, пристрої користувачів та інфраструктури, а також контури в межах рівнів та між ними. Ці функції виконують ГІС.

Накладання всіх рівнів на географічну основу забезпечує реалізацію підходу, за яким можна досягти всебічного спільного бачення ситуації в кіберпросторі. Комплексна ГІС-платформа створює можливість підтримувати робочі процеси користувачів, співпрацю та динамічне ситуаційне інформування для задоволення різноманітних вимог кіберзахисту.

Ця технологія, будучи доступною на багатьох пристроях і мережах, забезпечує персоналу швидкий доступ до інформації та даних, потрібних для прийняття рішень щодо формування обізнаності, запобігання, захисту, реагування та відновлення після інцидентів кібербезпеки. Платформа ГІС може бути використана для об'єднання даних про місцезнаходження та кіберактивність, а також іншої інформації з метою кращого прогнозування, виявлення, реагування та відновлення після кіберінцидентів. Також ГІС-технології дають можливість надавати актуальну інформацію іншим суб’єктам управління організації для ефективного прийняття рішень та координації спільних дій, сприяючи таким чином безперервності бізнесу та його стійкості.

ГІС дозволяє організаціям захищати свої електронні ресурси, швидко виявляти та встановлювати пріоритетність кіберзагроз, створюючи геопросторове рішення, яке інтегрує всі наявні дані для зменшення невизначеності. Мета полягає в тому, щоб забезпечити раннє виявлення та оперативне реагування на кіберпроникнення у всій організації. Налаштування платформи ГІС для забезпечення кібербезпеки дозволяє організаціям краще узгоджувати свої ділові операції з операційними системами, ІТ та безпекою, щоб бути частиною більш широких зусиль, спрямованих на пом'якшення кіберзагроз.

Платформа ГІС надає інструменти, що дозволяють персоналу побічно координувати діяльність з технічного обслуговування, реагування та відновлення, працюючи з загальною картиною ситуації відповідно до їхніх конкретних потреб. Фахівці, відповідальні за підтримку потоку даних можуть виявити та оцінити вплив потенційних порушень та мати можливість контактувати з особами, що забезпечують заходи із пом'якшення наслідків, за потреби.

ГІС легко інтегрується в існуючу в організації структуру управління та контролю, щоб забезпечити доступ керівництва до повних і точних даних для прийняття рішень. ГІС-платформи вже широко використовуються в рамках забезпечення національної безпеки, включаючи оборону, розвідку, захист критичної інфраструктури та управління надзвичайними ситуаціями. Розширення цієї можливості для включення кіберпрограм поряд із більш традиційними напрямами є дуже перспективним і дозволяє покращити синхронізацію заходів безпеки.

Концепція геопросторового аналізу компанії ESRI. Компанія ESRI, яка є однією з найбільш знаних у сфері розробки програмного забезпечення для ГІС, запропонувала концепцію їх застосування у галузі кібербезпеки [5]. Відповідно до їхнього бачення завдяки ГІС користувачі зможуть побачити загальну оперативну картину ситуації і, таким чином, врахувати вплив нецифрових, кінетичних подій на електронні системи.

Традиційні масиви геопросторових даних, таких як погода, використання земель та щільність населення, можуть мати цінність для операторів кіберпростору при прогнозуванні й оцінці ризиків несправності чи виведення з ладу об’єктів ІТКС критичного значення, а також визначенні впливу таких інцидентів на досягнення місій організації.

Зазначений підхід просуває впровадження ГІС-технологій в кібербезпеці за двома напрямами: побудова геопросторової моделі захисту периметру (Perimeter Defence) з метою виявлення й оцінювання спроб компрометації ІТКС та формування лінії кіберпідтримки (Cyber Supply Line - CSL) для виконання критичних місій організації.

Рисунок 1 показує процес кіберзахисту, який відповідно до концепції ESRI полягає у послідовному здійсненні п’яти оцінок щодо кожної підозрілої події [5].

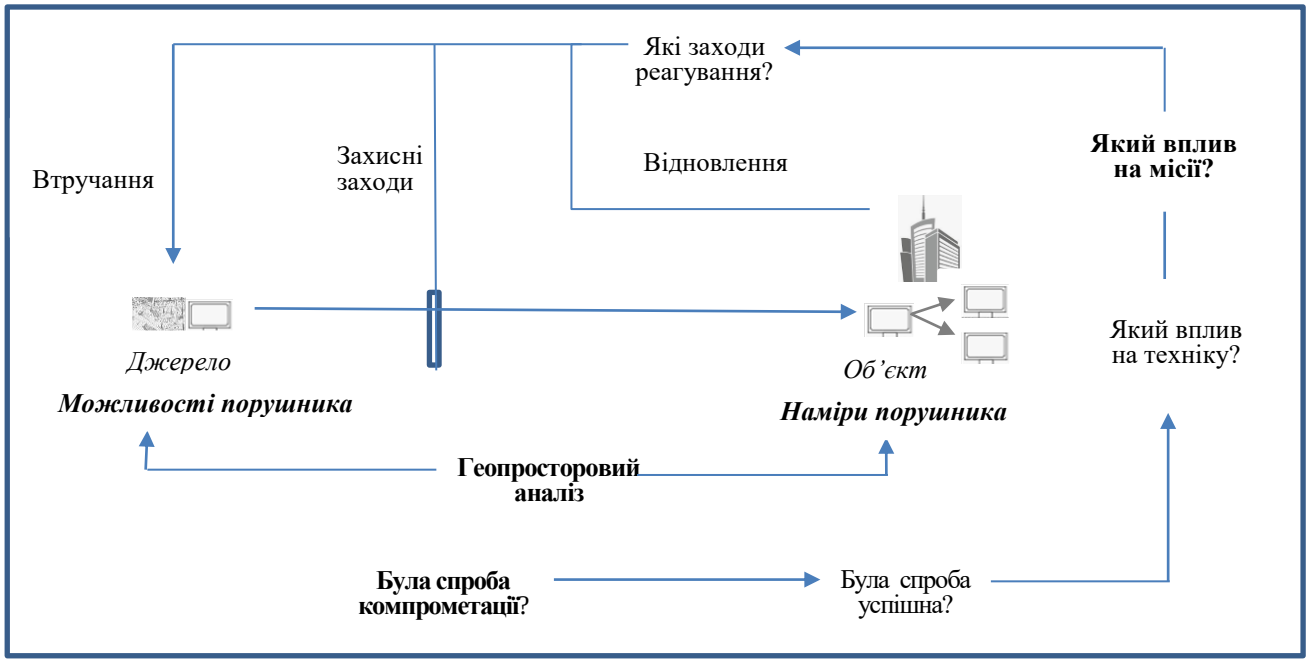

Рис.1. Процес кіберзахисту відповідно до концепції компанії ESRI.

Геопросторова модель для захисту периметру. Захисна кібердіяльність включає виявлення конкретних зловмисників, які становлять загрозу для ІКТС організації, та визначення профілактичних заходів, спрямованих на зменшення ризиків та вразливостей.

Фахівці ESRI пропонують розглядати діяльність із кіберзахисту як послідовність заходів у відповідь на п’ять питань:

Чи була спроба компрометації ІКТС організації?

Якщо так, чи була вона результативною?

Які технічні наслідки інциденту?

Як компрометація вплинула на місії організації?

Як організація має реагувати на інцидент?

Відповіді на зазначені питання може надавати ГІС-платформа як інструмент збору й аналізу даних.

Для визначення, чи мережа організації є під загрозою зловмисних дій використовують міжмережеві екрани й системи виявлення вторгнень. Однак, вони часто стикаються з такими обмеженнями як висока частота помилкових тривог або неможливість ідентифікувати нові вектори атак, наприклад, віруси та вразливі точки доступу.

Визначення того, чи була атака успішною, включає порівняння даних як із периметрів захисту, так і із захисних пристроїв, що розміщені на хості. Завдяки можливостям ГІС фахівці з кіберзахисту визначають технічні наслідки усіх підтверджених порушень кібербезпеки відповідно до такої класифікації: критично важливі дані або функціональні можливості були піддані ризику; внаслідок вторгнення надано несанкціонований доступ до інших машин, в результаті чого критично важливі дані або системи були піддані ризику; компрометація стосувалася тільки потерпілого пристрою-жертви. У перших двох випадках проводять оцінку впливу кіберінциденту на місії організації, щоб визначити, виконання яких організаційних функцій знаходиться під загрозою. В останньому - визначають найбільш прийнятне поєднання варіантів реагування: відновлення, зміцнення захисту мережі або вплив на джерело загрози.

Формування лінії кіберпідтримки (CSL) для виконання критичних місій організації. У контексті виконання місій організації основною метою кібербезпеки є доставка даних туди, де це потрібно, і уникнення ситуацій, коли дані не доставлені або є помилковими. Тому кіберфахівці не повинні забезпечувати підтримку безпеки всієї мережі, а захищати тільки критичні частини, необхідні для доставки інформації з одного конкретного джерела до конкретного пункту призначення на виконання встановлених місій.

При визначенні першочергових критичних пунктів призначення певні пристрої вважаються критичними за будь-яких умов, наприклад, сервери автентифікації та бази даних, що містять конфіденційні дані. Інші - є критичними лише за певних умов. Тому надмірне розширення статичного підходу обмежить швидкість та здатність організації реагувати на інциденти відповідно до їх пріоритетності. Для вирішення цього динамічного аспекту кіберзахисту фахівцями компанії Esri була розроблена модель CSL.

Esri визначає CSL як усі пристрої, що дозволяють переміщувати певний тип даних з одного джерела в одне місце призначення. Якщо для даного потоку даних призначено декілька пунктів призначення, виникають CSL від загального джерела до кожного місця розташування користувача, оскільки кожен передаватиме іншу підмножину інфраструктури кіберпростору. У мережі з комутацією пакетів кожна CSL матиме довжину від 16 до 18 кроків, де крок - це два пристрої, що складаються з комбінації маршрутизаторів, комутаторів, клієнтів та серверів, а також ідентифікованого носія передачі (кабель, супутникова низхідна лінія зв'язку або з'єднання в бездротовій мережі). Кожен пристрій має визначене місце в просторі і часі, належить організації і має сувору залежність від систем підтримки, таких як електропостачання та екологічний контроль. Якщо пристрій перебуває у CSL, виконання місії безпосередньо залежить від його коректної роботи.

CSL надає спільне рішення для менеджменту й кіберфахівців для обміну вимогами, пріоритетами та звітами. Для виконання конкретної місії керівництво організації визначає пріоритетні потоки даних, які є найбільш критичними в актуальних бізнес-умовах, а фахівці кіберзахисту обирають для кожного із пріоритетних потоків даних мережу, якою, ймовірно, будуть надходити дані. Мережа для місії створюється шляхом визначення найкоротшого

шляху, а потім навмисного виведення з ладу кожного пристрою, щоб встановити всі ймовірні маршрути, якими можуть пройти пакети. Кожен маршрут - це можлива CSL. Метою команди кіберзахисту є зосередження своїх ресурсів на кіберсупроводі пристроїв, через які проходять пріоритетні потоки даних, в тому числі в умовах кібератаки. На додаток до зміцнення кожного пристрою в мережі місії, кіберфахівці ретельно відстежують ці пристрої, щоб швидко виявити будь-яку подію, яка може негативно вплинути на CSL.

З огляду на тенденцію до конвергенції мереж, коли різні типи даних, такі як аудіо- і відео повідомлення, використовують одну і ту ж інфраструктуру, окремі потоки даних будуть відчутно перекриватися на рівні мережі місії. У таких випадках зусилля, що витрачаються технічними фахівцями для кіберпідтримки одного пристрою, допоможуть забезпечити безпеку безлічі потоків даних. Однак конвергенція не зменшує необхідність оцінювання кожного пріоритетного потоку даних, що створює основу для гнучкої реакції на появу будь-яких загроз.

Дана концепція дозволяє здійснювати не тільки низхідну комунікацію від керівництва до команди кіберзахисту, але й висхідну, забезпечуючи інформування керівництва про рівень кіберпідтримки і стан виконання місії. Крім того, CSL може бути використана для встановлення безперешкодної горизонтальної інтеграції, забезпечуючи зв'язок між організацією та її постачальниками послуг Інтернету й телекомунікацій. Оскільки кожен пристрій на CSL має вирішальне значення для загальної продуктивності, відомості про будь-яку подію, яка може негативно вплинути на пристрій, мають бути негайно повідомлені. Будь-яка схема співпраці, яка вимагає від усіх учасників постійного спілкування один з одним, не може бути досить швидкою, щоб захищати пріоритетні ресурси в кіберсередовищі. Забезпечення ефективної загальної оперативної картини - це суттєве покращення порівняно з особистими комунікаціями як за якістю, так і за гнучкістю.

Висновки. Отже, основною метою застосування ГІС у галузі кібербезпеки є володіння усіма суб'єктами управління організації загальною оперативною картиною ситуації в кіберпросторі, що дозволить забезпечити ефективне і своєчасне прийняття рішень щодо інформування, запобігання загрозам, реагування та відновлення об'єктів ІТКС після кіберінцидентів. Відповідно до концепції виробника ГІС-платформ ESRI за допомогою геопросторових технологій у галузі кібербезпеки можна реалізувати моделі захисту периметру та формування ліній кіберпідтримки (CSL). Перевага моделі CSL полягає в тому, що вона може організовувати та керувати процесом виконання завдань шляхом визначення всіх пристроїв, що підтримують шляхи передачі критичних даних організації. Оскільки значна частина поточної роботи в галузі кібербезпеки є розпорошена за місцем розташування та призначенням, модель CSL забезпечує інтеграцію цієї роботи, узгодження її з іншими безпековими напрямами діяльності та зосереджує увагу усіх на безпеці пріоритетних потоків даних, встановлених організацією.

Перелік посилань

1. Eye-Opening Cyber Security Statistics for 2019 [Електронний ресурс] // - Режим доступу: https://www.thesslstore.com/blog/80-eye-opening-cyber-security-statistics-for-2019/ (08.09.2020).
2. Must-know Cybersecurity Statistics for 2020 [Електронний ресурс] // - Режим доступу: https://www.cyber-observer.com/cyber-news-29-statistics-for-2020-cyber-observer/ (08.09.2020).
3. Жежнич П.І., Осика В.О. Функціональні та структурні вимоги до побудови сучасних географічних інформаційних систем [Електронний ресурс] // - Режим доступу: http://science.lpnu.ua/sites/default/files/journal-paper/2017/jun/3365/1096.pdf (08.09.2020).
4. The U.S. Army Concept for Cyberspace and Electronic Warfare. TRADOC Pamphlet 525-8-6 [Електронний ресурс] // - Режим доступу: https://fas.org/irp/doddir/army/tp525-8-6.pdf (08.09.2020).
5. The Geospatial Approach to Cybersecurity: Implementing a Platform to Secure Cyber Infrastructure and Operations. An Esri® White Paper [Електронний ресурс] // Режим доступу: https://www.esri.com/~/media/Files/Pdfs/library/whitepapers/pdfs/geospatial-approach-cybersecurity.pdf (08.09.2020).

Надійшла: 25.03.2020 Рецензент: д.т.н., проф. Савченко В.А.