ЗМІСТ

ВСТУП

Метою наукової роботи є комплексний аналіз та порівняння ряду проблем, визначення уразливих місць з відомими підходами до розв’язання, що дозволяє обґрунтувати наукові рекомендації і необхідність, доцільність та подальше удосконалення стратегій захисту критичної інфраструктури України.

Актуальність теми дослідження. Критична інфраструктура є основним елементом сучасного суспільства, забезпечуючи його стабільність та функціонування у всіх сферах, включаючи в себе об'єкти і системи, які забезпечують життєво важливі функції для соціуму, в галузях хімічної промисловості, енергетики, оборонно-промислового комплексу, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій, у банківському та фінансовому секторах та інші об'єкти.

Вони є не лише найбільш значущими для економічного та соціального розвитку держави, для її національної безпеки, але й найбільш уразливими перед різноманітними загрозами, включаючи природні катастрофи, техногенні аварії, терористичні акти, кібератаки, та агресивні дії на міжнародній арені.

Специфіка цих об'єктів вимагає високого рівня захисту, у воєнний період, коли загроза для національної безпеки стає ще більш актуальною, захист об'єктів критичної інфраструктури набуває критичного значення.

Пошкодження або знищення таких об'єктів може призвести до серйозного пошкодження та впливу на економіку, безпеку та стабільність країни, а також до значного зниження життєвого рівня населення.

У роботі «Захист об’єктів критичної інфраструктури, як складова забезпечення національної безпеки» можуть виникати певні протиріччя, пов’язані з багатогранністю самої теми.

Протиріччя між централізованим та децентралізованим управлінням:

Ефективний захист об’єктів критичної інфраструктури потребує як загальнодержавного контролю, так і гнучкого підходу на місцевому рівні. Для

забезпечення ефективного захисту об'єктів критичної інфраструктури необхідно поєднувати державний контроль із адаптивними підходами на місцевому рівні. Однак централізована модель управління часто супроводжується надмірною бюрократією, що уповільнює прийняття рішень, тоді як децентралізована система може страждати від браку координації, що призводить до появи слабких місць у загальній системі безпеки.

Протиріччя між швидким впровадженням стандартів і реальними можливостями інфраструктури:

Запровадження сучасних стандартів безпеки часто стикається з обмеженнями, пов’язаними зі станом застарілої інфраструктури. Багато об’єктів технічно не готові відповідати новим вимогам, що створює напруженість між необхідністю оперативного оновлення безпекових систем та труднощами, пов’язаними з високими витратами на модернізацію.

Ця ситуація ускладнюється тим, що негайне впровадження нових стандартів може бути критично важливим для протидії сучасним загрозам, але технічні та фінансові можливості часто виявляються недостатніми, що затримує процес реформ.

Протиріччя між фізичним захистом і кібербезпекою:

Захист об'єктів інфраструктури традиційно орієнтувався на фізичні заходи, такі як охорона, системи відеоспостереження та контроль доступу. Однак сучасні загрози все частіше проявляються в кіберпросторі, наприклад, у вигляді хакерських атак чи саботажу інформаційних систем.

Недостатня інтеграція фізичних і цифрових систем безпеки може залишати критичні вразливості, оскільки відсутність єдиної стратегії дозволяє зловмисникам використовувати прогалини як у фізичному, так і в кіберзахисті. Це створює ризик того, що навіть найкраще захищений фізично об’єкт може стати легкою мішенню для кібератак.

Виходячи з наявності протирічь тему магістерскої роботи можна вважати актуальною.

Об'єктом дослідження роботи. Система захисту об'єктів критичної інфраструктури в контексті національної безпеки, охоплює ключові аспекти, пов’язані із забезпеченням функціонування критично важливих об'єктів в умовах зростаючих загроз, зокрема фізичних, техногенних та кібернетичних. Увага зосереджується на механізмах, структурах та політиках, які формують цілісну систему захисту, а також на взаємодії між державними інституціями, приватними компаніями та міжнародними партнерами у цьому контексті.

Предмет дослідження. Захист безпосередньо об'єктів критичної інфраструктури, включаючи оцінку потенційних загроз, вивчення існуючих заходів безпеки, визначення їхньої ефективності та пропозиції щодо покращення заходів захисту .

Завдання роботи.

1. Аналізувати концепції критичної інфраструктури та її роль у забезпеченні національної безпеки.
2. Вивчення типів об'єктів критичної інфраструктури та їх важливості для стабільного функціонування суспільства.
3. Дослідити потенційних загроз, що можуть вплинути на об'єкти критичної інфраструктури, включаючи кібератаки, терористичні акти, природні катастрофи тощо.
4. Вивчити існуючі стратегій та методи захисту критичної інфраструктури від потенційних загроз.
5. Розглянути технічних засобів захисту, таких як системи кібербезпеки, інтелектуальні системи захисту, системи фізичного захисту тощо.
6. Аналізувати організаційні аспекти захисту критичної інфраструктури, таких як розробка політик безпеки, навчання персоналу, планування кризових ситуацій тощо.
7. Розглянути стратегічних аспектів захисту критичної інфраструктури на національному та міжнародному рівнях, включаючи міжнародне співробітництво та обмін найкращими практиками.

8. Рекомендації щодо покращення системи захисту критичної інфраструктури з метою забезпечення національної безпеки.

Методи даного дослідження. У процесі написання роботи використовувалися такі методи дослідження:

1. *Теоретичний аналіз:*

Вивчення наукових праць, монографій, статей, нормативно-правових актів та міжнародних документів з питань захисту критичної інфраструктури. Аналіз концепцій і підходів до забезпечення національної безпеки у контексті захисту критично важливих об’єктів.

2. *Порівняльний аналіз:*

Зіставлення підходів до захисту критичної інфраструктури в Україні та інших країнах. Оцінка сильних і слабких сторін різних моделей управління безпекою на основі міжнародного досвіду.

3. *Практичний метод:*

Збір і аналіз даних про інциденти на об’єктах критичної інфраструктури, а також ефективність заходів, вжитих для їх попередження чи усунення наслідків. Використання статистичних даних для оцінки загроз і ризиків.

4. *Метод сценарного підходу:*

Побудова сценаріїв потенційних загроз для критичної інфраструктури та оцінка можливих наслідків їх реалізації. Розробка рекомендацій на основі змодельованих ситуацій та можливих варіантів реагування.

Результат проведенного аналізу: Магістерська робота на тему «Захист об’єктів критичної інфраструктури, як складова забезпечення національної безпеки» присвячена аналізу ключових аспектів захисту критичних об'єктів та їхньому значенню для забезпечення національної безпеки. Відзначено важливість комплексного підходу до охорони об'єктів, які є критичними для стабільності та функціонування держави.

Критична інфраструктура складає основу для функціонування суспільства і економіки. Це енергетичні системи, транспортні вузли, водопостачання, комунікаційні мережі та інші стратегічно важливі об'єкти.

Їхнє функціонування є життєво важливим для підтримання соціальної стабільності та економічного розвитку. Тому забезпечення їхнього захисту є основною складовою частиною національної безпеки.

Аналіз показав, що захист критичних об'єктів стикається з численними проблемами. Це включає фізичні та кіберзагрози, можливі терористичні атаки, саботаж і природні катастрофи. Ефективний захист критичної інфраструктури вимагає постійного вдосконалення стратегій і технологій, а також інтеграції з іншими структурами.

Наукова новизна одержаних результатів. Полягає в тому, що у дослідженні обґрунтовується низка понять, концептуальних у теоретичному плані, і важливих для захисту обєктів критичної інфраструктури в контексті забезпечення національної безпеки положень, рекомендацій та висновків.

Теоретичною основою даного дослідження. Є аналітичні звіти також дослідження від національних або міжнародних організацій, що спеціалізуються на питаннях безпеки, законодавство та офіційні документи про захист критичної інфраструктури, постанови уряду, наукові статті та публікації в наукових журналах про безпеку і критичну інфраструктуру, звіти та дослідження від аналітичних агентств, які спеціалізуються на аналізі ризиків та безпеки, книги та монографії з тематики кібербезпеки, фізичної безпеки, захисту критичної інфраструктури, веб-сайти національних або міжнародних організацій, що спеціалізуються на питаннях безпеки, інтерв'ю з експертами з області безпеки, у тому числі представниками урядових органів, академічних дослідників, працівниками приватного сектору, документи та матеріали з міжнародних конференцій та симпозіумів з питань безпеки та критичної інфраструктури.

Структура роботи. Обумовлена метою дослідження. Робота складається зі вступу, основної частини, тобто 3 розділи, що включають в себе 11 підрозділів (загальна кількість сторінок 126), висновків , додатків (28) та списку використаних джерел (усього 57).

Апробація результатів роботи. Результати роботи були повідомлені,

обговорені та схвалені на наступних семінарах конференціях, круглих столах:
-Крутіков П.Д. тези доповідей «Актуальні проблеми теорії та практики службово-бойової діяльності складових сектору безпеки та оборони в сучасних умовах» 27 жовтня 2023 року, Київський інститут Національної гвардії України). – Київ: КІНГУ, 2024- С .91.
-Крутіков П.Д. тези доповідей «Проблеми ефективності професійної мовної комунікації в умовах інформаційної агресії » 26 квітня 2024 року, Київський інститун Національної гвардії України). – Київ: КІНГУ, 2024- С .62.
-Крутіков П.Д. тези доповідей «Сучасні наукові тенденції в роботах молодих вчених» 27 квітня 2024 року, Київський інститун Національної гвардії України). – Київ: КІНГУ, 2024- С .74, с. 77, с. 82.
-Крутіков П.Д. тези доповідей «Актуальні проблеми теорії та практики службово-бойової діяльності складових сектору безпеки та оборони в сучасних умовах» 24 травня 2024 року, Київський інститут Національної гвардії України). – Київ: КІНГУ, 2024- С .151.
-Крутіков П.Д. стаття науковий вісник Київського інституту Національної гвардії України №2,– Київ: КІНГУ, 2024- С .43.

Розділ 1. ПОНЯТТЯ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

1.1.Визначення терміну "критична інфраструктура"

В Україні, як і в інших країнах, наявні такі системи, об’єкти й ресурси, знищення або пошкодження яких матиме істотний негативний вплив на громадян, суспільство й державні інституції. При цьому було б неправильно стверджувати, що в нашій країні не приділяється увага їх захисту й безпеці. Навпаки, на сьогодні чинними є низка законодавчих і нормативних актів, що визначають повноваження та компетенцію державних органів у цій і суміжних сферах, встановлюють особливості забезпечення охорони та безпечного функціонування.

Таким чином, критична інфраструктура включає широкий спектр ресурсів та об'єктів, які є життєво важливими для сучасного суспільства та відображають різні аспекти його функціонування та розвитку.

Безпека цих об'єктів та їх функціонування як у нормальних умовах, так і в умовах надзвичайних ситуацій, таких як воєнний стан — один із пріоритетів держави.

Зрозуміло, що визначення в українському законодавстві цього основного для даної проблематики терміна має залишатися в межах загальновизнаних у світі підходів і повною мірою відображати специфіку безпекових умов, у яких перебуває країна. Це особливо важливо для забезпечення відповідності законодавства , міжнародним стандартам і нормам безпеки.

Чітке і узгоджене визначення терміна дозволить уникнути розбіжностей і конфліктів у міжнародних відносинах, а також забезпечить ефективне застосування законів у сфері безпеки в межах самої країни. Такий підхід сприятиме підвищенню рівня безпеки і захисту прав громадян, а також зміцненню міжнародного співробітництва в цій сфері.

В Україні термін «критична інфраструктура» неодноразово використовувався в нормативно-правових документах, проте його визначення й досі відсутнє в чинному законодавстві. Уперше в офіційних документах цей термін з'явився у 2006 р. в тексті Рекомендацій парламентських слухань з питання розвитку інформаційного суспільства, на жаль, без подальшого розвитку.

В Стратегії національної безпеки «Україна у світі, що змінюється» (2012 р.) цей термін згадувався при визначенні способів зміцнення енергетичної безпеки та напрямів забезпечення інформаційної безпеки. Проте, у новій Стратегії національної безпеки України (2015 р.) термін «критична інфраструктура» використовується більш деталізовано, його було уточнено й розширено, що дозволило краще розуміти суть та значення критичної інфраструктури в контексті національної безпеки. Це стало основою для визначення конкретних загроз та напрямів політики забезпечення безпеки критичної інфраструктури та боротьби з кіберзагрозами..

Уперше поміж «актуальних загроз національній безпеці» виокремлюються загрози критичній інфраструктурі, крім того, окремо в підрозділі «Загрози кібербезпеці і безпеці інформаційних ресурсів» згадується вразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак. Також уперше одними з «основних напрямів державної політики в сфері національної безпеки» названо забезпечення безпеки критичної інфраструктури та визначено пріоритети такого напряму.

Відсутність визначення терміна «критична інфраструктура» в українському законодавстві і, як наслідок, переліку об'єктів, які необхідно віднести до цієї інфраструктури, неодноразово перешкоджали ефективному виконанню першочергових безпекових завдань, таких як п. 6 Рішення Ради національної безпеки і оборони України «Про невідкладні заходи щодо забезпечення національної безпеки, суверенітету і територіальної цілісності України» від 01 березня 2014 р. (введено в дію Указом Президента України №189/2014 від 02 березня 2014 р.), на виконання. Наприклад, енергетичний

сектор у всіх країнах і в таких міжнародних об’єднаннях, як ЄС і НАТО, відносять до критичної інфраструктури.

Основна його функція полягає в забезпеченні потреб населення, суспільства й держави в енергії. Якщо акцент робитиметься на енергетичних об’єктах і системах, то без належного аналізу до критичної важливої інфраструктури можуть потрапити переважно об’єкти електрогенерації, тоді як об’єкти системи електропостачання є більш важливими для забезпечення послуг з електропостачання кінцевих споживачів.

Як свідчить світовий досвід, найтяжчі наслідки для забезпечення електроенергією суспільства виникають унаслідок аварій у системах передачі та розподілення електроенергії, а не у випадку виходу з ладу одного чи кількох об’єктів генерації. Збірник матеріалів міжнародних експертних нарад якого Міністерству внутрішніх справ України наказується забезпечити «посилену охорону об’єктів енергетики та критичної інфраструктури» (2, р2.1, ст13).

Сучасне життя людини, суспільства та держави нерозривно пов'язане з різноманітними системами, мережами та об'єктами, які забезпечують критично важливі послуги та виконують необхідні функції. Термін "критична інфраструктура" визначає коло таких систем, мереж і об'єктів, функціонування яких є життєво важливим для населення, суспільства та держави.

У різних країнах та міжнародних організаціях термін "критична інфраструктура" має подібне визначення, але існують відмінності, що відображають особливості національних та організаційних специфікацій. Наприклад, у США критична інфраструктура охоплює системи та ресурси, які є настільки важливими, що їхнє недієздатність може загрожувати національній безпеці, економіці, здоров'ю та безпеці населення.

У Німеччині під критичною інфраструктурою розуміють організаційні та фізичні структури, які є життєво важливими для суспільства та економіки країни. Англія та Нідерланди також мають власні визначення критичної інфраструктури, зосереджуючись на системах та мережах, які забезпечують нормальне функціонування країни та життя її громадян.

Зазначено, що в різних національних законодавствах акцент може бути розміщений не лише на фізичних об'єктах, але й на функціях та послугах, які вони забезпечують. Це дозволяє краще розуміти важливість кожного елементу для суспільства та держави.

Враховуючи вищезазначене, визначення терміна "критична інфраструктура" виступає як важлива складова безпекового та економічного розвитку країни, що має свої особливості в кожному конкретному національному контексті.

З огляду на викладене й досвід провідних країн світу з розроблення підходів до забезпечення національної безпеки на основі застосування концепції «критична інфраструктура», пропонуємо використовувати в Україні таке визначення цього терміна:

Критична інфраструктура - це сукупність об'єктів, систем та ресурсів, фізичних або в кіберпросторі, які є вирішальними для стабільного функціонування суспільства та економіки країни.

Вона включає в себе різноманітні види інфраструктури, що забезпечують життєво важливі послуги, безпеку та ефективність функціонування суспільства, соціально-економічного розвитку країни та забезпечення національної безпеки.

Складовими частинами є: енергетичні мережі, системи водопостачання та водовідведення, транспортні мережі (дороги, залізниця, морські та повітряні шляхи), телекомунікаційні мережі, банківські системи, медичні установи, системи захисту та безпеки, об'єкти оборони та інші.

Хоча в наведеному визначенні не наголошено на взаємозв’язку або взаємовпливі між окремими елементами критичної інфраструктури, саме ця особливість, важливо враховувати взаємозв'язок і взаємовплив між окремими елементами критичної інфраструктури, оскільки ця особливість впливає на масштаб наслідків в разі виникнення загроз або інцидентів.

Управління безпекою кожного окремого об'єкта має здійснюватися з урахуванням його взаємодії з іншими елементами системи критичної

інфраструктури. Це передбачає не лише захист окремих об'єктів, але й розуміння їхнього впливу на функціонування всієї системи. Такий підхід сприяє більш ефективному управлінню ризиками та забезпеченню стабільності та надійності з огляду на загальносистемні функції всієї критичної інфраструктури..

Потрібно надати також тлумачення поняття «захист критичної інфраструктури»:

Захист критичної інфраструктури України – це комплекс заходів, реалізований у нормативно-правових, організаційних, технологічних інструментах, спрямованих на забезпечення безпеки та стійкості критичної інфраструктури.

Захист критичної інфраструктури України є складним завданням, яке потребує комплексного підходу та використання різноманітних варіантів вирішення проблеми.

Нормативно-правові інструменти визначають правила, стандарти та вимоги до захисту критичної інфраструктури, встановлюють відповідальність за порушення цих вимог, і регулюють процеси планування та реагування на потенційні загрози.

Організаційні заходи включають у себе створення спеціалізованих організацій, комітетів або центрів управління кризовими ситуаціями, а також розробку планів та процедур реагування на різні види загроз.

Технологічні інструменти охоплюють впровадження сучасних технологій і систем захисту, включаючи системи контролю доступу, відеоспостереження, кіберзахисту та інші технічні засоби, що спрямовані на запобігання та виявлення можливих загроз.

Цей комплекс заходів має створити надійну систему захисту, яка забезпечить стійкість та надійність критичної інфраструктури України в умовах різноманітних внутрішніх та зовнішніх загроз.

Безпека критичної інфраструктури - це комплексний підхід до забезпечення захищеності об'єктів та систем, які є невід'ємною складовою

суспільства, і що має на меті забезпечення їхньої функціональності, безперервності роботи, відновлюваності, цілісності та стійкості у будь-яких умовах та обставинах..

Також варто зазначити, що поняття «безпека», використане у визначенні «захист критичної інфраструктури», містить і фізичну (фізичний захист), експлуатаційну та операційну безпеку.

Під стійкістю критичної інфраструктури розумітимемо її спроможність надійно функціонувати в нормальному режимі, адаптуватися до умов, що постійно змінюються, протистояти й швидко відновлюватися після аварій і технічних збоїв, зловмисних дій, природних лих та небезпечних природних явищ. Стійкість передбачає здатність продовжувати надавати свої послуги навіть після виникнення подібних подій.

Функціональність означає здатність об'єктів критичної інфраструктури виконувати свої функції згідно з призначенням у звичайних умовах та під час надзвичайних ситуацій. Це означає, що системи повинні бути розроблені та належним чином підтримуватися, щоб ефективно виконувати свої завдання.

Безперервність роботи передбачає, що навіть у разі виникнення перешкод, помилок або атак системи критичної інфраструктури мають забезпечити безперебійне функціонування або мінімізувати час простою.

Відновлюваність означає здатність систем відновлювати свою працездатність після виникнення негативних подій. Це включає відновлення даних, відновлення працездатності обладнання та забезпечення змоги відновити нормальний режим роботи.

Цілісність стосується здатності системи зберігати свою функціональну та даних в цілковитості, не допускаючи їх неправомірного доступу, змін або пошкоджень.

Для розкриття повної картини понятійних рамок і досягнення максимальної ефективності заходів з захисту критичної інфраструктури, необхідно також дати визначення терміну, «об’єкти критичної інфраструктури» та «сектор критичної інфраструктури».

Об’єкти критичної інфраструктури - об’єкти інфраструктури, їх частини та їх сукупність, важливі компоненти і системи, які є ключовими для економічного розвитку, національної безпеки та оборони країни, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам. Вони включають в себе об’єкти атомні, теплові, гідроелектростанції, залізничні мережі, станції, аеропорти, телекомунікаційні компанії, водозабірні станції та водосховища, лікарні та медичні центри та інші, які забезпечують нормальне функціонування суспільства.

Порушення функціонування цих об'єктів може призвести до серйозних наслідків, що загрожують життям і здоров'ю громадян, стабільності економіки та національній безпеці. Наприклад, атаки на енергетичні об'єкти можуть призвести до відключення електропостачання для широкого кола населення і підприємств, що вплине на виробництво, комунікації та інші критичні функції суспільства.

Тому важливо забезпечити надійний захист цих об'єктів, розвинути системи попередження та реагування на можливі загрози, а також вдосконалити механізми співпраці між різними секторами, урядовими та приватними структурами для ефективного управління ризиками та забезпечення стійкості критичної інфраструктури в умовах зростаючих загроз.

Сектор критичної інфраструктури – це сукупність об’єктів критичної інфраструктури, які належать до одного сектору (галузі) економіки та/або мають спільну функціональну спрямованість

Це означає, що об'єкти в межах одного сектору можуть мати подібний характер, призначення та значення для економіки та суспільства в цілому.

Наприклад, сектор транспорту може включати автомобільні дороги, залізничні мережі, аеропорти та порти, які забезпечують рух та перевезення товарів та людей.

Визначення секторів критичної інфраструктури допомагає управляти ризиками та виробляти стратегії захисту, спрямовані на забезпечення стійкості та надійності важливих галузей економіки. Це також сприяє координації дій

між різними урядовими та приватними структурами у сфері захисту критичної інфраструктури.

1.2. Види та класифікація критичної інфраструктури

Визначення видів критичної інфраструктури є переліку конкретних об’єктів, систем і ресурсів (елементів) критичної інфраструктури.

У нормативно-правовому полі України, близькі за змістом до об’єктів критичної інфраструктури. Українське законодавство щодо захисту об’єктів, які згідно зі світовою практикою належать до критичної інфраструктури, є досить розгалуженим і включає численні нормативно-правові акти, які, проте, мають переважно відомчий характер.

Чинне законодавство визначає такі категорії об’єктів, для яких встановлюються особливі умови забезпечення їх захисту й функціонування(1.ст.18.п2.3):

• підприємства, які мають стратегічне значення для економіки та безпеки держави;

• особливо важливі об’єкти електроенергетики;

• особливо важливі об’єкти нафтогазової галузі;

• важливі державні об’єкти, зокрема пункти управління органів державної влади та органів місцевого самоврядування;

• об’єкти можливих терористичних посягань;

• об’єкти, які підлягають охороні та обороні в умовах надзвичайних ситуацій і в особливий період;

• об’єкти, що підлягають обов’язковій охороні підрозділами Державної служби охорони за договорами;

• органи державної влади, що підлягають безоплатній охороні Національною гвардією України;

• об’єкти підвищеної небезпеки (в т.ч. Перелік особливо небезпечних підприємств, припинення діяльності яких потребує проведення спеціальних заходів щодо запобігання заподіянню шкоди життю та здоров’ю громадян, майну, спорудам, навколишньому природному середовищу;

• об’єкти, включені до Державного реєстру потенційно небезпечних об’єктів;

• радіаційно небезпечні об’єкти, для яких розробляється об’єктова проектна загроза;

• об’єкти, віднесені до категорій із цивільного захисту;

• об’єкти, що належать суб’єктам господарювання, проектування яких здійснюється з урахуванням вимог інженерно-технічних заходів цивільного захисту;

• чергово-диспетчерська система екстреної допомоги населенню за єдиним безкоштовним телефонним номером виклику екстрених служб 112;

• аварійно-рятувальні служби;

• Національна система конфіденційного зв’язку;

• Державна система урядового зв’язку України;

• платіжні системи;

• нерухомі об’єкти культурної спадщини.

Деякі із зазначених категорій об’єктів частково або повністю після виконання відповідного аналізу можуть бути віднесені до об’єктів критичної інфраструктури.

Виходячи з вищевказаних категорій пропоную наступні види :

1. **Енергетична інфраструктура:**

- Електростанції:

Атомні електростанції: Генерують електроенергію за допомогою ядерних реакцій. Ці електростанції відомі своєю високою потужністю та стабільністю постачання електроенергії, проте потребують високих заходів безпеки.

Теплові електростанції: Працюють на спалюванні вугілля, газу або нафти, щоб генерувати електроенергію. Ці станції є одними з найпоширеніших і забезпечують значну частину енергії в багатьох країнах.

Гідроелектростанції: Використовують потік води для приводу турбін, які генерують електроенергію. Ці електростанції є екологічно чистими і мають великий потенціал для виробництва стабільної електроенергії.

Вітроелектростанції: Вони використовують енергію вітру для приводу вітротурбін, які генерують електроенергію. Ці електростанції є одними з найшвидше розвиваючихся джерел виробництва енергії і мають низький вуглецевий відбиток.

- Електромережі та підстанції:

Електромережі: Це система проводів і трансформаторів, яка транспортує електроенергію від електростанцій до споживачів. Вони мають різну напругу та працюють на різних рівнях відповідно до потреб споживачів.

Підстанції: Це споруди, які забезпечують перетворення напруги та розподіл електроенергії в електромережі. Вони грають ключову роль у забезпеченні стабільності електропостачання та регулюванні напруги.

- Газопроводи, нафтопроводи та інші транспортні мережі для перевезення енергоносіїв:

Газопроводи: Транспортують природний газ з місця видобутку (нафтогазові родовища, підземні сховища тощо) до місць споживання (промислові підприємства, енергетичні станції, міські та сільські населені пункти тощо).

Газопроводи зазвичай складаються з трубопроводів, компресорних станцій для підвищення тиску газу, регуляторних станцій та інших споруд для контролю та підтримки потоку газу.

Забезпечення безпеки газопроводів включає контроль за тиском, виявлення та усунення витоків газу, запобігання корозії та інші заходи.

Нафтопроводи: Транспортують нафту та нафтопродукти (наприклад, бензин, дизельне паливо, авіаційне паливо) від місць видобутку (нафтові родовища, розливні термінали тощо) до різних пунктів споживання (нафтопереробні заводи, пункти роздрібної продажу тощо).

Складаються з великої кількості трубопроводів, насосних станцій для підтримки потоку рідини, регуляторних станцій для контролю та розподілу нафти, а також систем зберігання та перекачування.

Інші транспортні мережі: Такі мережі транспортують метан, отриманий з природного газу або інших джерел, до місць споживання або для подальшого використання (наприклад, у складі біопалива). Транспорт рідкого азоту, водню та інших речовин, які використовуються як енергетичні джерела або для промислових потреб.

2. **Транспортна інфраструктура:**

- Автомагістралі та шосе:

Складають мережу доріг для автотранспорту, яка забезпечує швидке та ефективне переміщення між містами та регіонами. Включає в себе широкі дороги, відповідно обладнані для безпечного руху автомобілів, пункти обслуговування (заправки, сервісні центри) та інші об'єкти.

- Залізничні мережі та станції: Забезпечують перевезення пасажирів та вантажів за допомогою залізничного транспорту. Включає в себе залізничні колії, станції для зупинок та пересадок, ремонтні центри та інші споруди.
- Аеропорти та повітряні шляхи:

Забезпечують пасажирські та вантажні перевезення за допомогою літаків. Включає в себе злітно-посадкові смуги, термінали пасажирів та вантажів, пункти контролю безпеки, ангари для літаків та інші об'єкти.

- Порти та морські термінали:

Забезпечують морські та річкові перевезення вантажів та пасажирів. Включає в себе пристані для суден, складські комплекси для зберігання вантажів, причали для вивантаження та завантаження суден, а також обладнання для погрузки та розвантаження.

3. **Інформаційна інфраструктура:**

- Інтернет-провайдери та телекомунікаційні компанії:

Забезпечують доступ до Інтернету та інших телекомунікаційних послуг для користувачів. Мережеве обладнання, які підтримують передачу даних, антени, кабельні лінії, супутникові системи та інші засоби зв'язку.

- Дата-центри та серверні установки:

Забезпечують зберігання, обробку та розподіл даних для користувачів та компаній. Включає в себе сервери, зберігання даних, комутаційне обладнання, системи охорони та безпеки, системи резервного копіювання та інші компоненти.

- Критичні інформаційні системи державного та комерційного значення:

Забезпечують роботу державних та комерційних організацій, включаючи системи управління, фінансові системи, медичні системи тощо. Програмне забезпечення, мережеве обладнання, системи забезпечення безпеки, системи резервного копіювання та відновлення даних, а також персонал для підтримки та обслуговування цих систем.

4. **Водопостачання та водовідведення:**

- Водозабірні станції та водосховища:

Забезпечують постачання прісної води для населення та промисловості. Споруди для збору та очищення води з природних джерел, таких як річки, озера або джерела. Водосховища використовуються для зберігання води та регулювання її потоку.

- Водопровідні мережі та насосні станції:

Транспортують очищену прісну воду з водозабірних станцій до споживачів. Трубопровід, насосні станції та регуляторні споруди для підтримання тиску та потоку води по мережі.

- Каналізаційні системи та очисні споруди:

Відведення та очищення стічних вод для запобігання забрудненню довкілля та забезпечення гігієнічних умов. Системи трубопроводів та каналізаційні колектори для відведення стічних вод від споживачів до очисних

споруд. Очисні споруди використовуються для очищення стічних вод від забруднень перед їхнім випуском в навколишнє середовище.

5. **Медична інфраструктура:**

- Лікарні та медичні центри:

Надання екстреної та планової медичної допомоги, госпіталізація хворих, проведення складних медичних процедур та операцій. Будівлі, устаткування для діагностики та лікування, лікарський персонал, апарати штучної вентиляції легень, інтенсивної терапії тощо.

- Аптечні мережі та лабораторії:

Забезпечення населення медикаментами та лікарськими засобами, проведення лабораторних досліджень та аналізів. Аптечні заклади для дистрибуції лікарських засобів, лабораторії для аналізів крові, сечі, біологічних зразків тощо, а також устаткування для проведення досліджень.

- Амбулаторії та інші медичні установки:

Надання первинної медичної допомоги, консультування пацієнтів, ведення медичної документації. Медичні кабінети, кабінети лікарів загальної практики, спеціалізовані кабінети для прийому лікарями-спеціалістами (наприклад, кардіологів, офтальмологів тощо), устаткування для проведення основних медичних процедур та обстежень.

6. **Фінансова інфраструктура:**

- Банки та фінансові установки:

Надання фінансових послуг, таких як зберігання грошових коштів, видача кредитів, обслуговування платіжних операцій, інвестиційні послуги тощо. Фінансові установи, такі як комерційні банки, кредитні спілки, страхові компанії, інвестиційні фонди та інші фінансові інститути. Кожна з цих установ має свою власну мережу філій та відділень, а також інформаційні системи для обробки та зберігання фінансових даних.

- Фондові ринки та біржі:

Місце торгівлі цінними паперами, такими як акції, облігації, фьючерси, опціони та інші фінансові інструменти. Фондові біржі, де здійснюються

торгівельні операції з цінними паперами. Це можуть бути традиційні біржі або електронні торгові платформи.

Такі ринки мають свої торгові системи, біржові торговельні майданчики, а також інформаційні системи для публікації та обробки торговельної інформації.

В свою чергу об'єкти критичної інфраструктури формують різні сектори критичної інфраструктури, які представляють собою певні групи об'єктів зі схожими характеристиками, функціональною спрямованістю або галузевою приналежністю.

Класифікація об'єктів у сектори допомагає уряду та організаціям, та формуванням краще розуміти специфіку загроз та ризиків, які вони можуть зазнати, і визначати ефективні стратегії захисту.

Наприклад, сектор енергетики включає в себе об'єкти, пов'язані з виробництвом, передачею та розподілом електроенергії, газу та нафти.

Сектор транспорту включає дороги, залізниці, аеропорти та порти.

Сектор інформаційної інфраструктури охоплює мережі зв'язку та інформаційні технології. Кожен з цих секторів має свою власну важливість для економіки та суспільства і може бути підданий впливу різних загроз (Додаток А).

Сектори критичної інфраструктури та організацію захисту їх функцій і послуг.

Основні положення:

1. Для забезпечення безпеки критичної інфраструктури, яка виконує важливі життєво важливі функції або надає специфічні послуги, визначаються окремі сектори критичної інфраструктури.

2. У кожному секторі критичної інфраструктури розробляються специфічні підходи до захисту, які відповідають державній політиці у сфері безпеки цієї інфраструктури. Секторальні органи займаються цим захистом.

3. Перелік секторів критичної інфраструктури та відповідальних за них суб'єктів управління формує Кабінет Міністрів України.

Якщо потрібно, цей перелік може змінюватися відповідно до критеріїв критичності, які визначені законом.

4. Серед життєво важливих функцій і послуг, порушення яких може негативно вплинути на національну безпеку, включають:

- Надання важливих адміністративних послуг;
- Енергозабезпечення, включаючи постачання тепла;
- Водопостачання та водовідведення;
- Продовольче забезпечення;
- Охорона здоров'я та фармацевтична промисловість;
- Інформаційні та електронні комунікації;
- Фінансові послуги;
- Транспорт;
- Оборона та безпека держави;
- Правопорядок та судочинство;
- Цивільний захист та рятувальні служби;
- Космічна діяльність
- Хімічна промисловість;
- Наукові дослідження.

1.3.Обгрунтування важливості захисту критичної інфраструктури для національної безпеки.

За період з 2022 по 2024 рік Україна зазнала численних атак на свою критичну інфраструктуру, що включає енергетичні об'єкти, державні мережі, транспортні системи та громадські місця. Ці атаки включають ракетні удари, кібератаки, дронові атаки та теракти. Розглянемо детальніше кожен рік для кращого розуміння важливості охорони таких об'єктів.

Жовтень 2022 року: Вся країна зазнала масованих ракетних ударів, спрямованих на електростанції. Ці атаки призвели до масштабних пошкоджень електромереж та перерв у постачанні електроенергії, але інформація про втрати серед цивільного населення відсутня.

Листопад 2022 року: Київ постраждав від кібератаки, яка була спрямована на державні мережі. Атака спричинила перебої у роботі урядових систем, але втрат серед цивільного населення не було.

Грудень 2022 року: Ракетні удари по Києву, Харкову та Львову пошкодили енергетичну інфраструктуру та системи водопостачання, що призвело до тривалих відключень світла і води.

Лютий 2023 року: Дніпропетровська та Запорізька області зазнали ракетних ударів, які завдали шкоди електростанціям. Це призвело до значних перебоїв у постачанні електроенергії.

Квітень 2023 року: Харків зазнав кібератаки, спрямованої на банківські системи, що спричинило збої у фінансових транзакціях і доступі до банківських послуг.

Травень 2023 року: Харків знову став ціллю ракетних ударів, які пошкодили енергетичну та транспортну інфраструктуру. Інформація про втрати серед населення не надається.

Серпень 2023 року: Одеська область постраждала від атак дронів, які завдали шкоди портам та енергетичним мережам, що спричинило перебої в роботі портів та електромереж.

28 січня 2024 року: Полтавська, Донецька, Запорізька та Дніпропетровська області зазнали атак дронів і ракет. Постраждала критична інфраструктура, але втрат серед цивільного населення не було.

22 березня 2024 року: Запоріжжя зазнало масованого ракетного обстрілу, який призвів до руйнування Дніпровської ГЕС та загибелі трьох осіб, понад 20 осіб отримали поранення.

8 травня 2024 року: Атаки на Київську та Львівську області крилатими ракетами пошкодили енергетичну інфраструктуру та цивільні об'єкти. Було поранено двох осіб.

1 червня 2024 року: Різні регіони України зазнали масованих атак дронами і ракетами, що завдали шкоди енергетичній інфраструктурі.

Квітень 2024 року: Київ та Львів стали ціллю теракту, внаслідок якого загинуло 5 осіб, а 15 отримали поранення. Теракт був спрямований на громадські місця, спричинивши значні людські втрати.

Захист критичної інфраструктури є ключовим елементом забезпечення національної безпеки з кількох причин. Економічна стабільність залежить від ефективного функціонування різних галузей економіки, які мають тісний зв'язок з критичною інфраструктурою.

Ось як це працює:

Енергетика: Енергетичні системи є серцем економіки, оскільки забезпечують електроенергією не лише підприємства, а й домогосподарства. Пошкодження або перебої в енергопостачанні можуть призвести до зупинки виробництва, що в свою чергу призведе до втрати прибутку, до зростання вартості продукції через додаткові витрати на енергію, що може вплинути на ціни на товари і послуги та призвести до збільшення інфляції та збільшення ризику безробіття.

Електроенергія необхідна також для задоволення побутових потреб населення, таких як освітлення, обігрів, охолодження, приготування їжі тощо. Перебої в енергопостачанні можуть призвести до дискомфорту для жителів та погіршення їхнього життя.

Транспортний сектор: відіграє критичну роль у глобальній економіці, забезпечуючи рух товарів, послуг та людей. Пошкодження або перешкоди в роботі транспортної інфраструктури можуть спричинити перерви у постачанні, затримки в поставках та підвищення вартості транспортування.

Ось детальніше, чому ефективне функціонування транспортної інфраструктури є настільки важливим:

Транспорт дозволяє пересувати товари від виробника до споживача. Без ефективного транспортного сектору, постачання товарів може бути ускладненим або зовсім зупинитися, що призведе до нестачі товарів на ринку та втрати прибутку для підприємств.

Транспортний сектор забезпечує можливість подорожей для людей як для особистих, так і для професійних цілей. Будь-які обмеження або перешкоди в роботі транспортної інфраструктури можуть призвести до незручностей для пасажирів, збоїв у графіку та втрати часу.

Для багатьох галузей промисловості, особливо для виробництва, важлива є постійна доступність сировини та матеріалів. Транспортний сектор забезпечує перевезення цих матеріалів від постачальників до виробників. Пошкодження транспортної інфраструктури може призвести до зупинки виробництва через нестачу сировини.

Перерви у роботі транспортної інфраструктури можуть призвести до затримок у поставках, що збільшує вартість транспортування та може призвести до зростання цін на товари і послуги для споживачів. Це також може вплинути на конкурентоспроможність компаній і загальну економічну стабільність.

Комунікації: Інформаційні мережі є основою сучасної економіки, вони забезпечують зв'язок між бізнесом, клієнтами та партнерами. Пошкодження комунікаційної інфраструктури може призвести до збоїв у виробництві, втрати контактів із клієнтами, а також погіршення комунікації в екстрених ситуаціях.

Інформаційні мережі дозволяють бізнесу підтримувати зв'язок зі своїми клієнтами та партнерами. Це включає в себе спілкування електронною

поштою, телефонні дзвінки, відеоконференції та інші засоби комунікації. Пошкодження комунікаційної інфраструктури може призвести до перерв у спілкуванні, втрати замовлень та партнерів, а також порушення ділових відносин.

Багато підприємств використовують інформаційні технології для автоматизації та оптимізації процесів виробництва. Це включає в себе системи автоматизації виробництва, системи управління ланцюгами постачання, моніторингу якості, інвентаризації та багато іншого.

Виробництво часто залежить від вчасного отримання необхідних матеріалів, компонентів та інформації. Збої в комунікаційній інфраструктурі можуть призвести до затримок у поставках матеріалів, що може вплинути на вчасність виробництва та виконання замовлень.

Якщо виробничі процеси зупиняються через збої в комунікаційній інфраструктурі, це може призвести до втрати продуктивності. Зупинка виробництва може призвести до втрати часу, ресурсів та грошей, що може негативно вплинути на фінансові результати підприємства.

Важливим аспектом інфраструктури комунікацій є її використання в екстрених ситуаціях, таких як природні катастрофи, терористичні атаки чи інші надзвичайні події. Комунікаційні засоби дозволяють органам управління та рятувальним службам координувати дії та надавати необхідну інформацію громадськості для забезпечення безпеки та реагування на небезпеку.

Інформаційні технології стимулюють інновації у багатьох галузях економіки. Вони дозволяють швидко обмінюватися ідеями, розробляти нові продукти та послуги, впроваджувати нові методи виробництва та управління. Збої у комунікаційній інфраструктурі можуть ускладнити співпрацю між компаніями, затримати впровадження нових технологій та інновацій можуть уповільнити темпи розвитку нових технологій, що може призвести до втрати конкурентоспроможності.

Збої у роботі комунікаційної інфраструктури можуть призвести до перерв у роботі команд, які працюють над новими технологіями та

інноваціями. Це може призвести до затримок у випуску нових продуктів на ринок, втрати можливостей для вдосконалення і розширення бізнесу.

У сучасному світі швидкість впровадження нових технологій і інновацій є ключовим фактором для успіху компаній та економік в цілому. У комунікаційній інфраструктурі можуть уповільнити цей процес та підірвати конкурентоспроможність країни або регіону на міжнародному ринку.

Фінанси: Фінансовий сектор грає ключову роль у розвитку економіки, забезпечуючи капітал для інвестицій та функціонування бізнесу.

Фінансові установи, такі як банки та інвестиційні компанії, надають кредити та інвестиції для розвитку бізнесу, створення нових підприємств та реалізації інноваційних проектів.

Пошкодження фінансової інфраструктури може призвести до скорочення кредитування та інвестицій, що ускладнить розвиток підприємств та економіки в цілому, до скорочення кредитування та інвестицій, може призвести до зупинки роботи банків та інших фінансових установ, призведе до фінансових труднощів для підприємств та населення. Наприклад, люди можуть мати проблеми з доступом до своїх банківських рахунків або отриманням кредитів може призвести до втрати вкладів для банківських клієнтів.

Якщо банк, де зберігаються гроші, стає неспроможним виконувати свої функції через технічні або інші проблеми, це може призвести до втрати заощаджень для клієнтів, може спричинити паніку на ринках, втрату довіри до фінансових установ та загрозу фінансовій стабільності.

Соціальна стабільність: Багато об'єктів критичної інфраструктури надають послуги, які є життєво важливими для населення, такі як електропостачання, водопостачання, медичні послуги тощо.

Об'єкти критичної інфраструктури, такі як системи електропостачання, водопостачання та медичні заклади, надають послуги, які є життєво важливими для населення. Без їх неперервної роботи може загрожувати безпека та здоров'я громадян, а також порушуватися звичний порядок життя.

Надійна робота критичної інфраструктури сприяє збереженню соціального порядку, оскільки вона забезпечує громадянам доступ до необхідних ресурсів та послуг. Це сприяє зменшенню напруги та конфліктів у суспільстві.

Пошкодження або перебої в роботі критичної інфраструктури можуть призвести до виникнення гуманітарних криз, таких як перерви в електропостачанні, відключення водопостачання чи недоступність медичних послуг. Це може призвести до екстрених ситуацій та загострення соціальних проблем.

Оборонна готовність: Багато об'єктів критичної інфраструктури мають стратегічне значення для оборони країни, так як вони можуть використовуватися для забезпечення військової мобілізації, комунікації та ведення оборонних операцій.

Об'єкти, такі як енергетичні мережі, транспортна інфраструктура, комунікаційні системи та водопостачання, мають велике стратегічне значення для оборони країни. Вони є основою функціонування військових структур, забезпечують важливі ресурси та послуги для військових задач та операцій.

Критична інфраструктура грає ключову роль у забезпеченні військової мобілізації. Наприклад, транспортні мережі важливі для переміщення військ та обладнання до місць концентрації, а енергетичні системи - для забезпечення роботи військово-промислових об'єктів.

Інформаційні системи та комунікаційна інфраструктура дозволяють забезпечити зв'язок між військовими підрозділами, координувати дії та передавати важливі команди та інформацію. Вони є невід'ємною частиною ведення оборонних операцій.

Пошкодження чи зупинка роботи критичної інфраструктури може серйозно ускладнити здатність країни відстоювати себе в разі військової агресії. Недоступність ключових ресурсів та послуг може значно обмежити можливості оборони та вразити ефективність військової складової.

Боротьба з тероризмом та кіберзагрозами: Об'єкти критичної інфраструктури можуть бути об'єктом терористичних атак або кібератак, спрямованих на національну безпеку.

Енергетичні мережі, транспортні вузли чи водопостачання, можуть стати потенційними цілями для терористичних груп.

Крім традиційних терористичних атак, критична інфраструктура також піддається кіберзагрозам. Кібератаки можуть спрямовуватися на інформаційні системи, електронні мережі та критичні технологічні системи, що може призвести до порушення роботи об'єктів інфраструктури та втрати конфіденційної інформації.

Захист критичної інфраструктури від терористичних атак та кіберзагроз включає в себе різноманітні заходи, такі як підвищення фізичної охорони об'єктів, застосування сучасних технологій кібербезпеки, розвиток імунітету до кібератак та підвищення обізнаності персоналу щодо можливих загроз.

Ефективна боротьба з тероризмом та кіберзагрозами передбачає не лише запобігання можливим атакам, але й швидке реагування у разі їхнього виникнення. Це включає в себе вчасне виявлення потенційних загроз, швидке реагування на інциденти та відновлення роботи інфраструктури після атаки.

Міжнародна привабливість: Країни, які мають ефективно захищену критичну інфраструктуру, є більш привабливими для інвесторів та міжнародних партнерів.

Інвестори шукають країни з надійною та стабільною інфраструктурою, оскільки це забезпечує їм високий рівень впевненості у безпеці їхніх інвестицій. Країни з ефективно захищеною критичною інфраструктурою вважаються більш привабливими для інвесторів, що може призвести до збільшення обсягів інвестицій та розвитку бізнесу.

Країни, які демонструють високий рівень захисту критичної інфраструктури, зазвичай мають більшу ймовірність налагодження міжнародних партнерств та співпраці. Це може включати торговельні угоди,

науково-технічну співпрацю, обмін технологіями та інші форми співробітництва.

Ефективний захист критичної інфраструктури сприяє стабільному функціонуванню економіки. Це стимулює підприємництво, збільшує рівень виробництва та залучає нові інвестиції. В результаті цього економіка країни зростає, а її позиції на міжнародній арені підвищуються.

Країни з ефективно захищеною критичною інфраструктурою відомі своєю надійністю та стабільністю. Це підвищує їхній престиж на міжнародній арені та сприяє покращенню їхнього міжнародного образу.

Отже, захист критичної інфраструктури є важливим завданням для забезпечення національної безпеки, оскільки він допомагає забезпечити економічну та соціальну стабільність, зберегти оборонну готовність та запобігти різноманітним загрозам.

РОЗДІЛ 2. АНАЛІЗ ЗАГРОЗ ТА РИЗИКІВ ДЛЯ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

2.1. Інформаційні загрози: кібератаки, кібершпигунство

Наразі в Україні гостро постає проблема інформаційної безпеки та комп'ютерної злочинності, тоді як правова база та судова практика не відповідають вимогам реального життя. При цьому існують так звані комп'ютерні злочини – незаконні дії, в яких інформаційно-обчислювальні системи стають об'єктом або інструментом злочинних посягань. Усі відомі в світі види таких злочинів, як комп'ютерне шахрайство, саботаж, шпигунство та крадіжки програм, вже реєструються в Україні.

1 вересня 2001 року набув чинності Кримінальний кодекс України, який містить розділ XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж». У ньому вперше визначені та юридично оформлені існуючі суспільно небезпечні діяння у цій сфері. Однак методичні рекомендації щодо їх розслідування поки що відсутні, а судова практика є недостатньою.

Слід зазначити, що закони самі по собі, а також організаційно-технічні заходи, не можуть системно захистити інформаційні системи від злочинних посягань. Тому державі необхідно не лише реагувати на існуючі суспільно небезпечні дії в сфері інформатизації, як це вже зроблено у сфері програмно-апаратних заходів захисту, але й формувати адекватну політику кібербезпеки, враховуючи реалії та прогнозовані тенденції розвитку в кібернетичній сфері.

За останні десятиліття інформаційні технології стали невід'ємною частиною повсякденного життя кожної людини. Важливо відзначити, що активний розвиток цих технологій пов'язаний не лише з розробкою новітніх рішень, але й із створенням найбільш досконалого та універсального

програмного забезпечення. Ці технології успішно використовуються шпигунами у їх незаконній шпигунській діяльності.

Досліджуючи поняття та зміст кібершпигунства, перш за все зазначу, що до цієї категорії входять два окремі поняття: шпіон «шпигун», шпіонаж, шпіонство, шпіонити; – р. болг. шпибн, бр. шпіен, п. (рідк.) szpion, ч. (розм.) spion, слц. spion, вл. spion, м. иіпион, схв. шпщун, слн. spi-jon; – запозичення з німецької мови; н. Spion п «шпіон, шпигун за посередництвом французь-кої «і та іспанської (фр. espion. icп. spiопе «тс.») запозичене з італійської; іт. spiопе «шпигун» утворене від spїаге «шпіонити, вистежу вати, підстерігати», джерелом якого є германські мови (пор. пгер. speph-де «уважно, гостро дивитися» і генетично, пов'язані з ним двн. spehоп, spiohопте.«стежити, вистежувати [10, с.404] та терміни – «кібер» («кібернетичне») [11, с. 168], утворюючи сучасне слово «кібершпигунство»

Отже, для проведення ґрунтовного дослідження цієї категорії, розглянемо її окремо. У словнику української мови "шпигунство"- це злочинна діяльність, яка полягає у таємному збиранні відомостей або викраданні матеріалів, що становлять державну таємницю, з метою передачі їх іншій державі . Водночас термін "кібернетичний" відноситься до кібернетики та описує те, що створено або працює на основі принципів і методів науки кібернетики.

«Кібершпигунство», або комп'ютерний шпіонаж (інколи використовується термін «кіберрозвідка»), означає несанкціоноване отримання інформації з метою здобуття особистої, економічної, політичної чи військової переваги. Це досягається шляхом зламу систем комп'ютерної безпеки, використання шкідливого програмного забезпечення, зокрема "троянських коней" та шпигунських програм. Кібершпигунство може проводитися дистанційно через Інтернет або шляхом фізичного проникнення в комп'ютери та мережі підприємств звичайними шпигунами ("кротами") чи хакерами. Таким чином, кібершпигунство є злочинною діяльністю, що включає таємне вистежування, пошук, збирання, викрадання та передачу

інформації, яка становить державну таємницю, якщо ці дії здійснюються іноземцем або особою без громадянства із використанням кібернетичного простору.

У Кримінальному кодексі України шпигунство визначено як передача або збирання з метою передачі іноземній державі, іноземній організації або їх представникам відомостей, що становлять державну таємницю, якщо ці дії здійснені іноземцем або особою без громадянства (ст. 114 КК України).

Основним об'єктом шпигунства (включаючи кібершпигунство) є кібернетична загроза зовнішній безпеці України, її суверенітету, територіальній цілісності та недоторканності, обороноздатності, державній, економічній чи інформаційній безпеці. Кібернетична загроза (кіберзагроза) включає наявні та потенційні явища і фактори, які створюють небезпеку для інтересів людини, суспільства і держави через порушення доступності, цілісності, достовірності, автентичності режиму доступу до інформації, що циркулює в критичних об'єктах національної інформаційної інфраструктури.

Згідно аналізу останніх досліджень і публікацій Держспецзв’язку, кількість кібератак у 2022 році було зафіксовано 2194 кіберінциденти, з яких 1048 мали високий або критичний рівень. У 2023 році загальна кількість кіберінцидентів становила 2554, з яких лише 367 були серйозними[10].

Перші місяці цього року демонструють збільшення кількості кібератак, які здійснюють російські хакери на українські інформаційні системи. Тому варто очікувати, що 2024 рік для нашої країни буде важчим з точки зору ведення кібервійни. У першому кварталі 2024 року Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA, серед іншого, вжито заходів з недопущення реалізації зловмисного задуму, який полягав у проведенні деструктивного впливу, у відношенні трьох українських організацій урядового та енергетичного сектору.

Однією з найактивніших загроз було угруповання найманців UAC-0050, пов'язаних з російськими правоохоронними органами. Вони оголосили про завершення своєї "професійної" діяльності під назвою DaVinci Group за кілька

днів до російського вторгнення у 2022 році, але останнім часом знову активно нагадують про себе.

Станом на 22 лютого 2024 року було виявлено і досліджено щонайменше 15 кампаній, під час яких зловмисники використовували п'ять видів шкідливих програм: REMCOS RAT, QUASAR RAT, VENOM RAT, REMOTE UTILITIES та LUMMASTEALER. Незважаючи на те, що лише невелика частина їхньої діяльності оприлюднюється в Telegram-каналі, їх тактика нагадує діяльність брокерів первинного доступу.

Через масовість атак і використання програм, призначених для викрадення автентифікаційних даних, скомпрометовані логіни, паролі та сертифікати можуть створювати технічні передумови для несанкціонованого доступу до інформаційно-комунікаційних систем організацій, що дозволить розвивати атаки на їхні внутрішні ресурси.

Також, команда реагування на комп'ютерні надзвичайні події України CERT-UA, згідно з Законом України "Про основні засади забезпечення кібербезпеки України", виявила, що однією з найбільших "кіберзагроз" є UAC-0010 (Armageddon). Ця загроза походить від колишніх "офіцерів" ГУ СБУ в АР Крим, які у 2014 році зрадили військовій присязі і стали служити ФСБ Російської Федерації. Головною метою цієї групи є "кібершпигунство" у відношенні до безпеки та оборони України. Згідно з наявною інформацією, кількість одночасно інфікованих комп'ютерів, переважно у системах державних органів, може сягати кількох тисяч.

Поняття "кіберзагроза" у сфері кібербезпеки стосується як наявних, так і потенційно можливих явищ і чинників, що загрожують життєво важливим національним інтересам України в кіберпросторі, завдаючи негативного впливу на його стан. Хакерська атака, або кібератака, є спробою реалізації кіберзагрози. Це дії зловмисників (хакерів) або шкідливих програм, спрямовані на захоплення інформаційних даних віддаленого комп'ютера, отримання повного контролю над його ресурсами або виведення системи з ладу.

Таким чином, під "кібератакою" розуміють атаку на інформаційну інфраструктуру, яка є сукупністю пов’язаних між собою дій зловмисника (ініційованих ним процесів), що приводять до реалізації загроз для інформаційних ресурсів шляхом використання вразливостей певної інформаційної системи, як частини інформаційної інфраструктури.

Умовно можна розрізняти два типи кібератак в залежності від місця знаходження зловмисника під час атаки, що має значення для виявлення осіб, відповідальних за атаку, та ступеня їх дії:

Локальне проникнення (local penetration) – зловмисник знаходиться всередині об’єкта та використовує прямий доступ до інформаційної системи.

Віддалене проникнення (remote penetration) – зловмисник знаходиться поза системою та використовує віддалений доступ для здійснення атаки на інформаційні ресурси.

Найбільш розповсюдженими видами є віддалені (зовнішні) кібератаки до яких входять:

Фішинг. Це вид кіберзлочину, в якому зловмисники намагаються отримати конфіденційну інформацію, таку як логіни, паролі, дані кредитних карток або інші персональні дані, обманним шляхом. Зазвичай це робиться шляхом маскування під надійне джерело через електронну пошту, повідомлення в соцмережах, телефонні дзвінки або вебсайти. Зловмисники використовують фішинг для того, щоб отримати доступ до особистих даних у корпоративних або особистих мережах.

Систематичні фішинг-атаки почалися в мережі America Online (AOL) в 1995. Щоб викрасти легітимні облікові дані, зловмисники зв'язувалися з жертвами через AOL Instant Messenger (AIM), видаючи себе за співробітників AOL, які перевіряють паролі користувачів. Термін «фішинг» з'явився в групі новин Usenet, яка зосереджувалася на інструменті AOHell, який автоматизував цей метод, і так ім'я закріпилося. Після того, як AOL в 1997 році ввела контрзаходи, кіберзлочинці зрозуміли, що можуть використовувати таку ж техніку в інших галузях, зокрема й фінансових установах.

Одна з перших великих, хоча і невдалих, спроб була в 2001 році. Зловмисники, скориставшись хаосом від терористичних атак 9/11, розіслали потерпілим електронну розсилку нібито для перевірки посвідчення особи. Отримані дані використовувались для крадіжки банківських даних.

Вже у 2005 році за допомогою фішингу кіберзлочинці викрали у користувачів США понад 900 мільйонів доларів США.

Відповідно до дослідження глобального фішингу APWG, у 2016 році спостерігалося понад 250 тисяч унікальних фішингових атак, під час яких використовувалось рекордне число доменних імен, зареєстрованих зловмисниками, перевищуючи позначку в 95 тисяч. В останні роки кіберзлочинці намагалися зосередитися на банківських та фінансових послугах, користувачах електронного банкінгу, соціальних мереж, а також облікових даних електронної пошти.

Пропоную розглянути також види фішингу :

Смішинг (англ. SMiShing — від «SMS» і «фішинг») — це вид фішингу, який здійснюється через SMS. Шахраї надсилають жертві повідомлення з посиланням на фішинговий сайт і закликають відвідати цей сайт.

Фішинг через SMS або смішинг схожий на фішинг через електронну пошту, але в цьому випадку зловмисники використовують текстові повідомлення для доставки своїх «приманок». Смішинг-атаки зазвичай закликають користувача перейти за посиланням, зателефонувати на вказаний номер або зв'язатися через електронну адресу, зазначену в повідомленні.

Жертву просять надати особисті дані, які можуть включати інформацію для входу на інші сайти або сервіси. Через особливості мобільних браузерів, URL-адреси можуть відображатися не повністю, що ускладнює ідентифікацію підробленої сторінки входу. Оскільки більшість сучасних мобільних телефонів мають швидке підключення до інтернету, шкідливі посилання, надіслані в SMS, можуть мати такий же ефект, як і ті, що надсилаються електронною поштою. Смішингові повідомлення можуть надходити з незвичних або незрозумілих телефонних номерів.

Вішинг (від англ. "voice" — «голос» і "fishing" — «рибальство») — це вид телефонного шахрайства, який полягає у виманюванні реквізитів банківських карток або іншої конфіденційної інформації, а також у примушуванні до переказу грошей на рахунки злочинців. Це один з найпоширеніших методів крадіжки грошей з рахунків громадян. Разом з іншими шахрайськими схемами вішинг вивчається в рамках соціальної інженерії.

Вішинг найчастіше використовується для заволодіння коштами на банківських рахунках жертв, але також може застосовуватися для проникнення в інформаційні системи приватних або державних установ і крадіжки конфіденційної інформації.

Схема надзвичайно проста: шахраї телефонують із незнайомого номера і під різними приводами намагаються:

- вивідати дані платіжної картки (номер, дату завершення дії, PIN-код тощо) та одноразові паролі з банківських sms-повідомлень;
- змусити зняти ліміти на операції по платіжній картці;
- відключити перевірку коду безпеки картки CVV2;
- перерахувати кошти на картку шахраїв.

Залякування. Шахраї дзвонять жертві і представляючись співробітниками правоохоронних органів (хоча такими вони не є) повідомляють, що хтось із рідних потрапив у дорожньо-транспортну пригоду, скоїв кримінальний злочин тощо. Гроші вимагають на хабар за невідкриття кримінальної справи або щоб відкупитись від постраждалих.

Виграш. Шахраї повідомляють про якісь виграші, перерахунки пенсій чи соціальних виплат, повернення відсотків за кредитом. Обман спрацьовує, тому що злочинці зазвичай представляються працівниками банків (у 94 % випадків зловмисники грають роль саме банківських службовців[джерело?]), Пенсійного фонду, СБУ, поліції. Шахраї намагаються вивідати реквізити банківської картки для нібито перерахунку коштів.

Кетфішинг (з англ. catfish — сом, дослівно «Ловля сома», «риболовля на сома» — це вид шахрайства, коли людина створює вигаданий несправжній акаунт чи сторінку в соціальних мережах або на сайтах знайомств, зазвичай націлюючись на конкретну жертву. Ця практика може використовуватися для отримання різного типу вигоди, вивідування інформації, щоб якимсь чином скомпрометувати жертву, як спосіб навмисно засмутити жертву або для виконання бажання.

Про кетфішинг були створені телевізійні шоу, в яких часто фігурували жертви, які хотіли знайти свого шахрая. Цілями зловмисників також ставали знаменитості, що привернуло увагу преси до явища кетфішингу.

Ата́ка «злий двійни́к» (англ. Evil twin) — різновид фішинга, вживана в бездротових комп'ютерних мережах.

Зловмисник створює копію бездротової точки доступу, що знаходиться в зоні досяжності користувача, замінюючи справжню точку доступу своєю підробкою. Коли користувач підключається до цієї підробленої точки, зловмисник отримує доступ до конфіденційної інформації користувача.

Виявити і задокументувати факт крадіжки інформації при такій атаці дуже складно. Однак, зростання популярності бездротових мереж робить цю загрозу все більш реальною. Для атаки на відкриту бездротову мережу цим методом не потрібно попередньо зламувати захищену мережу і отримувати пароль.

У 2024 році фішинг залишається однією з головних загроз кібербезпеці в Україні. Зокрема, кількість фішингових атак продовжує зростати, відображаючи загальносвітову тенденцію. За даними звіту Cybersecurity Ventures, у 2023 році було виявлено значне зростання кількості шкідливих URL-адрес на 61%, що відповідає 255 млн фішингових атак за рік (Website Rating).

Україна також стикається зі збільшенням кількості кібератак через геополітичну нестабільність. Близько третини глобального потоку шкідливих email-розсилок надходить з Росії, і ці атаки часто спрямовані на українські

організації та інфраструктуру. Використання шкідливих програм та методів соціальної інженерії значно ускладнює захист даних.

SQL ін'єкція. Один з поширених способів злому сайтів та програм, що працюють з базами даних, заснований на впровадженні в запит довільного SQL-коду.

Впровадження SQL, залежно від типу СКБД та умов впровадження, може дати можливість тій людині, що атакує, виконати довільний запит до бази даних (наприклад, прочитати вміст будь-яких таблиць, видалити, змінити або додати дані), отримати можливість читання та/або запису локальних файлів та виконання довільних команд на сервері.

Атака типу впровадження SQL може бути можлива за некоректної обробки вхідних даних, що використовуються в SQL-запитах.

SQL-ін'єкція може мати різні види, залежно від того, яким чином вразливість експлуатується і які атаки можуть бути здійснені зловмисником. Ось деякі типові види SQL-ін'єкцій:

SQL Injection в параметрах запитів: Це найбільш поширений вид SQL-ін'єкції, коли зловмисник вводить SQL-код безпосередньо в параметри запиту до веб-додатка через форми вводу, URL-параметри або інші вхідні дані. Наприклад:

SELECT * FROM users WHERE username = '$_POST['username']';

Якщо значення $_POST['username'] не екранується або не обробляється належним чином, зловмисник може вставити SQL-код, щоб отримати доступ до даних або змінити їх.

Blind SQL Injection: В даному випадку зловмисник використовує техніки тестування на "сліпоту" (blind testing), щоб визначити наявність і структуру даних без прямого витягування їх. Зазвичай використовується у випадках, коли немає прямого виводу помилок або результатів запиту.

Time-Based SQL Injection: Цей вид ін'єкції використовується для створення затримок у відповіді сервера, які дозволяють зловмиснику виявити

наявність і експлуатувати вразливість шляхом вставки затримок (наприклад, затримка на певну кількість секунд) у SQL-запити.

Second-Order SQL Injection: Цей тип ін'єкції виникає, коли введені дані не відразу використовуються у SQL-запитах, але зберігаються в базі даних і використовуються пізніше. Зловмисник може модифікувати ці дані, щоб вразити інші користувачі або саму систему.

Схема атаки SQL-ін'єкції включає такі етапи:

Збор інформації: Зловмисник вивчає структуру бази даних і збирає необхідну інформацію про таблиці, колонки і дані.

Створення SQL-ін'єкційного виразу: Зловмисник створює SQL-код, який вставляється в веб-запит з метою виконання небажаних дій, таких як витягування даних, модифікація або видалення.

Експлуатація вразливості: SQL-ін'єкція виконується, і зловмисник отримує доступ до бази даних або здійснює інші дії, що можуть включати витягування конфіденційної інформації або завдання шкоди.

Приховання слідів: Після атаки зловмисник може намагатися приховати свій слід або залишити пастку для подальшого використання.

Міжсайтові сценарії (XSS). Є типом кібератаки, яка полягає в впровадженні веб-сторінку зловмисного JavaScript-коду (або інших сценаріїв), який виконується у веб-браузері іншого користувача. Основна ідея XSS-атак полягає в тому, що зловмисник використовує недостатньо фільтровані або оброблені вхідні дані (такі як текстові поля, URL-параметри або дані з куки) для впровадження коду на сторінці, яку побачить інший користувач.

Види XSS-атак:

Stored XSS (збережені XSS):Це найпоширеніший тип XSS-атак. Зловмисник вводить зловмисний код, який зберігається на сервері, наприклад, у коментарях, форумах або базі даних. Користувачі, які переглядають вразливу сторінку, отримують зловмисний код, який виконується у їх браузерах.

Reflected XSS (відображені XSS): В цьому випадку зловмисний код вставляється у відповідь веб-сервера і потрапляє до браузера користувача як частина URL-адреси або форми. Наприклад, зловмисник може створити спеціальне посилання, яке містить зловмисний код, і надіслати його потенційної жертві через електронну пошту або соціальні мережі. Коли користувач переходить за цим посиланням, зловмисний код виконується у його браузері.

DOM-based XSS: Цей тип XSS-атак відбувається на стороні клієнта і викликається через модифікацію DOM (Document Object Model). Зловмисник використовує вразливість у JavaScript-коді, що виконується на клієнтській стороні, наприклад, через неправильну обробку URL-параметрів або інших вхідних даних.

Наслідки XSS-атак: Крадіжка сесійних ідентифікаторів: Зловмисники можуть красти cookie-файли або сесійні ідентифікатори, що дозволяє їм отримати доступ до авторизованих сеансів користувачів. Видалення або модифікація вмісту сторінки: Зловмисник може видаляти або змінювати вміст сторінки, що може призвести до розповсюдження дезінформації або псевдо-реклами. Перенаправлення на зловмисний сайт: Користувачі можуть бути перенаправлені на фішингові або зловмисні сайти, де їм можуть намагатися вибрати конфіденційні дані.

Заходи захисту від XSS-атак:

Екранування вхідних даних: Всі вхідні дані, які вставляються у веб-сторінку (наприклад, введені користувачем дані), мають бути екрановані таким чином, щоб забезпечити, що вони не містять JavaScript-коду чи інших виконуваних сценаріїв.

Валідація і фільтрація вхідних даних: Перевірка введених даних на відповідність очікуваному формату і фільтрація потенційно небезпечних символів.

Використання безпечних API для вставки HTML-коду: Замість прямого вставлення HTML-коду через innerHTML, використовуйте безпечні методи

для вставки тексту чи інших даних, які не будуть інтерпретовані як HTML або JavaScript.

Використання HTTP заголовків для захисту від XSS: Налаштування HTTP заголовків, таких як Content Security Policy (CSP), що обмежує виконання JavaScript-коду на сторінці.

Регулярне оновлення і захист від XSS: Важливо регулярно оновлювати програмне забезпечення, включаючи браузери та веб-сервери, і вчасно застосовувати патчі і оновлення безпеки.

Аналізатори протоколів, також відомі як сніфери (sniffers). Є потужними інструментами для отримання і аналізу мережевого трафіку в реальному часі. Вони працюють на рівні мережевого інтерфейсу, дозволяючи отримувати доступ до всіх пакетів даних, що проходять через мережеву карту, на якій вони встановлені.

Основні функції аналізаторів протоколів:

Захоплення трафіку: Аналізатори протоколів можуть захоплювати усі пакети даних, що пересилаються по мережі, включаючи текстову і графічну інформацію, аудіо та відео.

Аналіз протоколів: Вони розуміють структуру різних мережевих протоколів, таких як TCP/IP, UDP, HTTP, FTP тощо.

Здатні розбирати заголовки пакетів і тіла даних для виявлення інформації про джерело, призначення, тип даних та інші параметри протоколу.

Фільтрація і сортування трафіку: Вони мають можливості фільтрації, що дозволяють вибирати тільки певні типи пакетів за заданими критеріями, такими як IP-адреса, порт, протокол і т. д.

Детальний аналіз і візуалізація: Після захоплення трафіку аналізатори можуть представляти дані у вигляді графіків, діаграм або таблиць, що полегшує візуальне розуміння і аналіз мережевої активності.

Виявлення уразливостей і атак: Аналізатори протоколів можуть виявляти потенційно небезпечні ситуації, такі як відкриті порти, неправильна конфігурація протоколів, відсутність шифрування тощо.

Небезпека отримання конфіденційної інформації: Однією з найбільш небезпечних аспектів використання аналізаторів протоколів є можливість отримання конфіденційної інформації, такої як логіни, паролі, сесійні токени і інші чутливі дані.

Якщо мережевий трафік не зашифрований або якщо використовуються незахищені протоколи, зловмисники можуть захоплювати ці дані і використовувати для незаконного доступу до систем і акаунтів.

Перехоплення каналу зв'язку (Man-in-the-Middle або MITM). Є серйозною кібератакою, в якій зловмисник вставляється між двома спілкуючимися сторонами і перехоплює весь або частину їхнього комунікаційного потоку. Це дозволяє зловмиснику не тільки отримати доступ до передаваної інформації, але й може надати можливість модифікувати дані або навіть ініціювати фальшиві комунікації в обох напрямках.

Як працює MITM атака:

Перехоплення трафіку: Зловмисник впроваджується між двома легітимними сторонами комунікації, наприклад, між клієнтом і сервером. Він отримує доступ до усіх передаваних даних, які пролітають через нього.

Аналіз і модифікація даних: Зловмисник може переглядати, записувати і навіть змінювати дані, що передаються між сторонами. Це особливо небезпечно в контексті незахищених протоколів, таких як HTTP, де дані передаються у незашифрованому вигляді.

Фальшиві атаки і запити: Зловмисник може вставляти свої власні дані у комунікаційний потік, що може призвести до виклику фальшивих запитів або передачі фальшивих даних між сторонами.

Потенційні наслідки MITM атаки:

Крадіжка конфіденційної інформації: Зловмисник може зловживати доступом до конфіденційної інформації, такої як паролі, сесійні токени, особисті дані і бізнес-інформація.

Маніпуляція з комунікацією: Зловмисник може модифікувати дані, що передаються між сторонами, що може призвести до втрати цілісності даних або виклику некоректної реакції систем.

Атаки на безпеку мережі: Використовуючи MITM атаку, зловмисник може втручатися в безпеку мережі, наприклад, встановлюючи фальшиві сертифікати SSL для здійснення атаки типу SSL Stripping.

Атака на відмову в обслуговуванні (Denial of Service, DoS). Є однією з найпоширеніших і небезпечних атак у світі кібербезпеки. Основна мета DoS-атаки — зробити певний ресурс недоступним для користувачів, шляхом перевантаження його ресурсів або експлуатації слабких місць у системі.
Основні типи DoS атак:

Флуд атаки (Flood Attacks):

UDP Flood: Злмовмисник надсилає великий обсяг UDP-пакетів до певного порту на цільовому сервері, що призводить до перевантаження ресурсу.

ICMP Flood: Використовується ICMP-пакети (Ping) для перевантаження мережевого обладнання, викликаючи його переповнення.

Син Flood (SYN Flood):

Нападник надсилає величезну кількість SYN-пакетів (початкова фаза TCP-з'єднання) до цільового сервера, але не завершує процес з'єднання, що призводить до заповнення таблиць з'єднань і блокування серверу.

HTTP Flood:

Зловмисник надсилає велику кількість HTTP-запитів до веб-сервера, що призводить до перевантаження його обробки запитів і зниження продуктивності або відмови в обслуговуванні.

Додаткові типи DoS атак:

Amplification Attacks: Атаки, при яких зловмисник посилає невеликі запити до сервера, який відповідає великим обсягом даних, що перевантажує цільовий сервер.

Application Layer Attacks: Напади на рівні прикладного програмного забезпечення, такі як атаки на веб-додатки, що дозволяють завантажити сервер великим обсягом HTTP-запитів або SQL-запитів.

DDoS атака (Distributed Denial of Service)

DDoS атака є підтипом DoS, що відрізняється тим, що атака проводиться з множини комп'ютерів, що можуть бути розташовані в різних частинах світу. Це значно ускладнює захист і виявлення атаки.

Особливості DDoS атак:

Розподілене джерело: В атаці бере участь велика кількість інфікованих пристроїв, часто в рамках ботнету (мережі заражених комп'ютерів).

Складність виявлення: Розподілена природа атаки ускладнює виявлення та блокування трафіку атаки, оскільки він приходить з різних IP-адрес.

Великі обсяги трафіку: DDoS атаки часто використовують величезний обсяг трафіку для досягнення мети, що включає син Flood, UDP Flood, HTTP Flood та інші типи атак.

Як працює DDoS атака:

Інфікування ботнету: Зловмисник створює або використовує вже існуючий ботнет, інфікуючи комп'ютери з використанням вірусів, троянів або експлойтів.

Керування ботнетом: Зловмисник віддає команду ботнету через командно-контрольний сервер (C&C server), який координує всі інфіковані пристрої.

Реалізація атаки: Ботнет надсилає величезну кількість трафіку до цільового сервера, перевантажуючи його мережеві ресурси або процесорний час.

Приклади DDoS атак:

Атака на компанію GitHub у 2018 році: Один з найвідоміших прикладів DDoS атаки, що перевищив 1,3 Tbps, використовуючи DNS Amplification.

Атака на українські банки у 2016 році: Використання DDoS атак для паралізації банківських систем, що вплинуло на фінансові операції.

Спам e-mail (Mailbombing)–вважається найстарішим методом атак, хоча суть його проста і примітивна: велика кількість поштових повідомлень роблять неможливими роботу з поштовими скриньками, а іноді і з цілими поштовими серверами.Основні характеристики спам e-mail атаки:

Масове відправлення повідомлень: Зловмисники використовують спеціалізовані програми, які автоматизують процес створення і відправлення великої кількості електронних листів до жертви або до цільового сервера.

Цільовість: Жертвою може бути конкретний користувач (наприклад, на рівні індивідуальних конфліктів), або ціль може бути націлена на цілий домен або інфраструктуру поштового сервера.

Використання анонімних поштових серверів: Деякі програми для Mailbombing можуть використовувати анонімні поштові сервери для відправлення електронних листів. Це дозволяє зловмисникам ховати свій реальний IP-адрес відправника і ускладнює виявлення та блокування атак.

Приховування ідентичності: Деякі програми також можуть маскувати ідентифікатори відправника, щоб зробити важче виявлення та ідентифікацію зловмисників.

Потенційні наслідки спам e-mail атаки:

Перевантаження поштових серверів: Велика кількість непохідних повідомлень може перевантажити ресурси поштових серверів, що призводить до зниження їх ефективності або навіть до тимчасової відмови у роботі.

Втрата робочого часу: Отримання великої кількості непотрібних повідомлень може витрачати час користувачів на фільтрацію і видалення спаму.

Зниження продуктивності: Велика кількість спаму може заважати користувачам працювати з електронною поштою, знижуючи їх продуктивність.

2.2. Фізичні загрози: терористичні акти, природні катастрофи.

Фізичні загрози для об'єктів критичної інфраструктури є серйозною проблемою, що може мати далекосяжні наслідки для суспільства в цілому. Ці загрози можуть бути викликані різними факторами, такими як терористичні акти, природні катастрофи, техногенні аварії та інші небезпечні події.

Терористичні акти

Один із найбільш серйозних типів загроз для критичної інфраструктури — це терористичні акти. Терористи можуть впроваджувати вибухові пристрої на об'єкти інфраструктури, такі як залізничні колії, аеропорти, електростанції та водозабірні споруди. Вибухи призводять до руйнування інфраструктури, масових знищень і загрози для життя людей. Прикладами таких атак можуть бути теракти на транспортні мережі, що призводять до великої кількості жертв і великих економічних втрат.

Мінування об'єктів критичної інфраструктури: Залізничні, авіаційні, водний і автомобільний транспорт: Терористи можуть встановлювати вибухові пристрої на рейках залізниць, на аеродромах або в аеропортах, на суднах або у водоймах, а також на автомобільних дорогах. Вибухи можуть спричиняти руйнування транспортних мереж, втрати людських життів і майнові збитки.

Залізничні колії, автомобільні дороги: Такі дії можуть призвести до інцидентів на залізничних переїздах або на автомобільних дорогах, які можуть стати великою проблемою для економіки країни..

Дії терориста-смертника: автомобіль-фугас на об'єктах критичної інфраструктури і в місцях масового скупчення людей: Такі атаки зазвичай спрямовані на максимальні людські жертви і шкоду інфраструктурі.

Застосування вибухових пристроїв у поштових посилках або бандеролях:

Включаючи хімічну зброю масового зниження: Цей метод може бути використаний для нападу на конкретних осіб або організації, що може призвести до великих людських жертв і паніки в громадськості.

Збройне захоплення заручників:

На об'єктах критичної інфраструктури захоплення заручників може бути використане для вимагання політичних, фінансових або ідеологічних вимог. Збройне захоплення заручників на об'єктах критичної інфраструктури є однією з найбільш серйозних загроз безпеці, оскільки воно може мати негативний вплив на безпеку людей, економіку та соціальну стабільність. Такий вид нападу часто використовується для досягнення різноманітних цілей, включаючи політичні, фінансові або ідеологічні мотиви.

Сценарії збройного захоплення заручників:

Політичні мотиви: Збройне захоплення заручників може бути спрямоване на привернення уваги до політичних проблем або вимагання політичних змін. Такі заходи можуть виконуватися як групами з радикальних політичних організацій або інших державних або недержавних структур, що мають політичні мотиви.

Фінансові вимоги: Захоплення заручників може бути використане для вимагання викупу або інших матеріальних вигод. Такі акти можуть бути спрямовані на отримання фінансового викупу від держави, підприємства або індивідуальних осіб.

Ідеологічні мотиви: Захоплення заручників також може мати ідеологічні мотиви, наприклад, відстоювання певних політичних, релігійних або етнічних поглядів. Це може включати терористичні організації або індивідуальні групи, які використовують такі методи для досягнення своїх цілей.

Наслідки збройного захоплення заручників на критичну інфраструктуру. В першу чергу, такі події створюють серйозну загрозу для життя та здоров'я заручників, персоналу об'єкта та навколишніх мешканців.

Захоплення заручників може призвести до припинення нормальної роботи об'єкта критичної інфраструктури, що може мати далекосяжні економічні наслідки і призвести до великих втрат.

Такі події спричиняють паніку серед населення, психологічні травми для учасників і свідків події, а також викликають значний рівень страху і непевності в суспільстві.

Природні катастрофи

Іншим серйозним ризиком є природні катастрофи, такі як землетруси, урагани, повені та лісові пожежі. Ці природні явища можуть призвести до значних руйнувань інфраструктури. Наприклад, повені можуть затопити електростанції або важливі транспортні маршрути, що призведе до зупинки виробничих процесів і втрати електроенергії для населення і промисловості.

. До загроз природного характеру можна віднести такі їх види:

– метеорологічні (снігопади, ожеледь, хуртовини, зливи, градобій, заморозки, засухи);

– гідрологічні (повені, селі, паводки, підтоплення);

– геологічні (небезпечні екзогенні геологічні процеси - зсуви, просідання та карст);

– геліофізичні (пожежі).

Проаналізувавши найбільші прояви впливу природних катастроф на об’єкти критичної інфраструктури хотів би виділити:

Листопад 2000 року, наслідки обледеніння

У листопаді 2000 року значні обледеніння спричинили серйозні матеріальні збитки і проблеми з інфраструктурою в багатьох регіонах. Ось деталі: Понад 20 тисяч ліній електропередач було пошкоджено через обледеніння, 307 тисяч залізобетонних опор стали непридатними для подальшої експлуатації, 34 тисяч тонн дроту стали непридатними для використання, 2000 сільських телефонних станцій було відключено.

Це обледеніння мало серйозний вплив на електропостачання, зв'язок і забезпечення населення електроенергією.

Січень 2014 року, наслідки снігопаду та обледеніння

В останній декаді січня 2014 року сильний снігопад, сніг і дощ разом з поривами вітру значно ускладнили життя населення та функціонування інфраструктури:

Внаслідок обледеніння та снігопаду було пошкоджено повітряні лінії електропередач. Спрацювання систем автоматичного захисту ЛЕП призвело до відключення електропостачання. Було знеструмлено 1605 населених пунктів. На автошляхах через снігові замети було ускладнено або повністю припинено рух автотранспорту на значних територіях України.

Ці приклади ілюструють, як природні явища, такі як обледеніння і снігопади, можуть суттєво вплинути на життя та економіку регіонів, особливо коли вони впливають на критичну інфраструктуру.

Серед гідрологічних загроз за серйозністю наслідків для критичної інфраструктури слід паводки.

Зокрема, найбільш масштабний за останні роки паводок в Україні у 2008 р. спричинив пошкодження понад 500 автомобільних мостів, розмивання 1660 км автомобільних доріг різного значення тощо.

Значну загрозу для функціонування та безпеки критичної інфраструктури становлять небезпечні екзогенні геологічні процеси (підтоплення, просідання, карст, зсуви). Так, до 20% залізничних колій знаходяться під впливом регіонального підтоплення земель, близько 40% - перебувають у зонах карстових загроз, до 11% - на територіях можливої активізації зсувних процесів.

До 59% магістральних газопроводів перебувають в умовах можливого прояву карсту, до 21% - у зонах прояву регіонального підтоплення земель. Активізація небезпечних екзогенних геологічних процесів загрожує екологічній безпеці в районах розміщення об’єктів підвищеної небезпеки, захисних гребель і дамб шламосховищ і ставків-відстійників, ускладнення інженерно-геологічних умов експлуатації промислових споруд та інженерних мереж промислово-міських агломерацій.

Техногенні аварії

Техногенні аварії, такі як вибухи на промислових об'єктах, аварії на ядерних електростанціях або хімічні розливи, також становлять серйозну загрозу. Ці події можуть мати далекосяжні наслідки для оточуючого середовища, здоров'я людей і навколишнього регіону.

Техногенні аварії на об'єктах критичної інфраструктури є серйозною загрозою, оскільки вони можуть мати значний вплив на навколишнє середовище, здоров'я людей і економіку. Ось детальніше про деякі з найбільш розповсюджених техногенних аварій:

Вибухи на промислових об'єктах, таких як заводи, заводи, склади хімічних речовин або нафтопереробні підприємства, можуть призвести до масштабних наслідків:

Вибухи часто супроводжуються значним тиском та тепловим випромінюванням, що може призвести до руйнування будівель та інфраструктури навколишніх об'єктів.

Хімічні речовини, що можуть бути присутні в промислових процесах, можуть бути випущені в атмосферу внаслідок вибуху, що призводить до забруднення навколишнього середовища та загрози здоров'ю людей.

Аварії на атомних електростанціях можуть мати катастрофічні наслідки через випуск радіоактивних матеріалів:

Випуск радіоактивних речовин може призвести до серйозного забруднення атмосфери і ґрунтів, що призводить до радіаційного забруднення інфраструктури та населених пунктів. У разі серйозної аварії може знадобитися евакуація територій, що має значний соціальний і економічний вплив.

Аварії на промисловостях також становлять значну загрозу:

Випуск хімічних речовин може спричинити серйозні наслідки для здоров'я людей і навколишнього середовища.

Хімічні речовини можуть взаємодіяти з іншими речовинами або зовнішніми чинниками, що призводить до пожеж і вибухів, що є надзвичайно небезпечними.

Ці техногенні аварії потребують комплексного підходу до моніторингу, запобігання та реагування з метою зменшення ризиків для людей, навколишнього середовища і економіки.

Техногенні аварії на об'єктах критичної інфраструктури є серйозною загрозою, яка вимагає комплексного підходу до моніторингу, запобігання та реагування з метою зменшення ризиків для людей, навколишнього середовища і економіки.

Ось основні аспекти цього підходу:

Належне функціонування систем моніторингу дозволяє вчасно виявляти можливі відхилення або небезпеки. Вони включають в себе системи виявлення викидів, радіаційні монітори, системи моніторингу хімічних речовин тощо.

Ці дані необхідні для оперативної реакції на аварійні ситуації і для визначення масштабів забруднення.

Фізичні загрози для об'єктів критичної інфраструктури не лише призводять до значних матеріальних збитків і втрат людських життів, але й порушують звичний ритм функціонування суспільства. Вони можуть спричиняти паніку, великі соціальні та економічні втрати, а також призводити до значних викликів для систем здоров'я, правопорядку і громадської безпеки.

У зв'язку з цим важливо розвивати та впроваджувати ефективні стратегії захисту інфраструктури, включаючи підвищення обізнаності про загрози, розробку планів надзвичайних ситуацій і вдосконалення технологічних засобів безпеки.

Тільки комплексний підхід може забезпечити ефективний захист від фізичних загроз для об'єктів критичної інфраструктури і зберегти стабільність суспільства в умовах надзвичайних подій.

2.3. Соціально-економічні загрози: економічні кризи, соціальні протести.

Соціально-економічні загрози, такі як економічні кризи та соціальні протести, можуть мати значний вплив на об'єкти критичної інфраструктури (КІ), що включає системи, необхідні для підтримки основних функцій суспільства. Розглянемо вплив цих загроз на різні аспекти критичної інфраструктури.

Економічні кризи

Енергетичний сектор часто стає жертвою бюджетних скорочень під час економічних криз. Зменшення інвестицій у модернізацію та обслуговування енергетичних об'єктів призводить до зниження якості послуг та збільшення частоти аварій. Ці наслідки відчутно позначаються на всіх аспектах економічного та соціального життя країни, адже стабільне постачання енергії є фундаментом для функціонування інших секторів критичної інфраструктури. Розглянемо детальніше вплив економічних криз на енергетичний сектор на прикладах різних країн.

Недостатнє фінансування призводить до зниження якості обслуговування енергетичних об'єктів, що спричиняє перебої в постачанні електроенергії. В результаті, споживачі – як промислові, так і побутові – відчувають негативні наслідки у вигляді частих відключень електроенергії.

Відсутність інвестицій у модернізацію та обслуговування обладнання підвищує ризик аварій та технічних збоїв. Це особливо небезпечно для великих промислових об'єктів, які потребують стабільного постачання енергії для безперебійної роботи.

Перебої в енергопостачанні можуть спричинити значні економічні втрати. Підприємства змушені зупиняти виробництво, що веде до втрати прибутків і робочих місць. Домогосподарства також зазнають збитків через псування продуктів харчування та пошкодження електроприладів.

Постійні перебої в енергопостачанні можуть викликати соціальне напруження та незадоволення населення. Це може призвести до протестів та інших форм соціального невдоволення, що додатково ускладнює ситуацію в країні.

Пропоную розглянути на приклади впливу економічних криз на енергетичний сектор України.

Україна неодноразово зазнавала серйозних економічних труднощів, що мали руйнівний вплив на всі аспекти критичної інфраструктури, зокрема й на енергетичний сектор. Економічні кризи 2008-2009 та 2014-2015 років стали серйозними випробуваннями для енергетичної системи країни. Зменшення інвестицій у модернізацію та обслуговування енергетичних об'єктів призвело до зниження якості послуг та збільшення частоти аварій.

Криза 2008-2009 років

Світова фінансова криза 2008-2009 років суттєво вплинула на економіку України. Значне падіння ВВП, скорочення промислового виробництва та дефіцит бюджету призвели до скорочення інвестицій у енергетичний сектор. Одним з наслідків стало погіршення стану електромереж та енергетичної інфраструктури загалом.

Під час цієї кризи, багато енергетичних компаній, як державних, так і приватних, зіткнулися з браком фінансування для модернізації та ремонту обладнання. Це призвело до частих аварій та перебоїв у постачанні електроенергії. Наприклад, у деяких регіонах України спостерігалися перебої в енергопостачанні, що негативно впливало на життєдіяльність населення та роботу промислових підприємств.

Криза 2014-2015 років

Економічна криза, спричинена політичною нестабільністю та військовими діями на сході України у 2014-2015 роках, ще більше загострила проблеми енергетичного сектору. Однією з найгостріших проблем стало пошкодження та руйнування енергетичної інфраструктури в зоні конфлікту. Багато електростанцій, підстанцій та ліній електропередач було зруйновано

або пошкоджено, що призвело до серйозних перебоїв у постачанні електроенергії.

Ця криза також спричинила дефіцит ресурсів для обслуговування та модернізації енергетичних об'єктів. Зменшення інвестицій та бюджетних коштів призвело до зниження якості обслуговування електромереж, що збільшило ризик аварій та технічних збоїв. Наприклад, у 2014 році Україна зіткнулася з серією масштабних відключень електроенергії, викликаних дефіцитом вугілля для електростанцій та зниженням виробничих потужностей.

Під час економічних криз енергетичні компанії були змушені скорочувати витрати на обслуговування та модернізацію обладнання, що призводило до зниження якості послуг. Часті перебої в енергопостачанні негативно впливали на побутових та промислових споживачів. Наприклад, у 2014 році у багатьох регіонах України спостерігалися регулярні відключення електроенергії, що ускладнювало життя громадян та роботу підприємств.

Недостатнє фінансування обслуговування енергетичних об'єктів підвищувало ризик аварій та технічних збоїв. У 2015 році в Україні відбулося кілька значних аварій на електростанціях та підстанціях, що призвело до масових відключень електроенергії. Це ще раз підтвердило необхідність інвестування у модернізацію енергетичної

Перебої в енергопостачанні мали серйозні економічні наслідки. Підприємства були змушені зупиняти виробництво, що призводило до втрати прибутків та робочих місць. Наприклад, у 2014 році багато промислових підприємств на сході України змушені були зупинити виробництво через нестабільне енергопостачання, що призвело до значних економічних втрат.

Постійні перебої в енергопостачанні викликали соціальне напруження та незадоволення населення. Це призводило до протестів та інших форм соціального невдоволення. У 2015 році в деяких регіонах України відбувалися акції протесту через часті відключення електроенергії, що додатково ускладнювало ситуацію в країні.

Приклад Іспанії

Під час економічної кризи 2008-2009 років Іспанія зіткнулася зі значними фінансовими труднощами, що призвело до скорочення бюджетів у багатьох секторах, включаючи енергетичний. Зниження інвестицій у електромережі та генераційні потужності спричинило часті збої у постачанні електроенергії. Недостатнє фінансування не дозволяло проводити своєчасну модернізацію та обслуговування обладнання, що призвело до підвищення ризику аварій та перебоїв.

Одним із яскравих прикладів є місто Барселона, де у 2007 році відбувся масштабний блекаут, який тривав понад 24 години і вплинув на життя сотень тисяч людей. Причиною аварії стало недостатнє обслуговування та застарілість обладнання, яке не витримало навантаження. Економічна криза лише поглибила ці проблеми, адже уряд та приватні компанії були змушені скорочувати витрати на інфраструктуру.

Приклад Греції

Греція також зазнала серйозних економічних труднощів під час фінансової кризи, що почалася у 2009 році. Скорочення державного фінансування енергетичних об'єктів призвело до дефіциту ресурсів для їх обслуговування та модернізації. Це спричинило часті перебої в постачанні електроенергії, що негативно вплинуло як на промисловість, так і на побутових споживачів.

Наприклад, влітку 2011 року Греція зіткнулася з серією відключень електроенергії через неспроможність енергетичних компаній забезпечити належний рівень обслуговування та модернізації своїх об'єктів. Це було особливо критично під час туристичного сезону, коли навантаження на енергосистему значно зростає. Відсутність інвестицій у нові технології та оновлення старих інфраструктурних об'єктів призвела до зниження надійності постачання енергії та збільшення кількості аварійних ситуацій.

Вплив економічної кризи на транспортний сектор України (2022-2024 роки)

Зменшення інвестицій

Економічні кризи, особливо ті, що супроводжуються військовими конфліктами, завжди призводять до значного зниження інвестицій у критичні сектори економіки. Транспортний сектор України не є винятком. З 2022 року країна зіткнулася з гострою нестачею інвестицій через бюджетний дефіцит, спричинений військовими діями та економічною нестабільністю.

Недостатність фінансування особливо відчувається у транспортному секторі, який потребує постійних вливань коштів для модернізації та підтримки інфраструктури. Наприклад, за останні два роки значно скоротилися капітальні інвестиції в ремонт та будівництво доріг, модернізацію залізничної інфраструктури, а також оновлення парку громадського транспорту. Відсутність належного фінансування призводить до занедбаності та деградації існуючої інфраструктури, що негативно впливає на економічний розвиток країни та добробут населення.

Погіршення умов роботи

Зниження інвестицій у транспортну інфраструктуру безпосередньо впливає на умови роботи всіх видів транспорту. Погіршення якості обслуговування доріг, залізниць, аеропортів та портів створює передумови для аварій та збоїв у транспортних мережах, що, у свою чергу, знижує ефективність економічної діяльності та якість життя населення.

Автомобільні дороги: Відсутність належного ремонту та обслуговування призводить до утворення ям та інших дефектів на дорогах. Це не лише збільшує ризик дорожньо-транспортних пригод, але й спричиняє зростання витрат на обслуговування транспортних засобів, які часто пошкоджуються на поганих дорогах.

Під час економічної кризи 2022-2024 років Україна зіштовхнулася зі значними проблемами у сфері дорожнього будівництва та ремонту. Недостатнє фінансування призвело до занедбаності багатьох ключових магістралей, що з'єднують регіони країни. Це, у свою чергу, вплинуло на економічну активність та мобільність населення.

Залізничний транспорт: Застаріла інфраструктура та недостатній рівень обслуговування рухомого складу спричиняють часті поломки та затримки у графіку руху поїздів. Це негативно впливає на вантажні та пасажирські перевезення, підвищуючи вартість логістичних послуг та знижуючи конкурентоспроможність залізничного транспорту. Багато ділянок залізничних колій потребують капітального ремонту, а рухомий склад – модернізації. Це призвело до збільшення кількості аварій та затримок у перевезеннях, що негативно позначилося на економіці країни та міжнародних торговельних зв'язках.

Аеропорти та морські порти: Недостатня технічна підтримка аеропортів та морських портів призводить до затримок у обслуговуванні літаків та суден, що негативно впливає на міжнародні перевезення. Погіршення умов роботи в аеропортах та портах також створює додаткові ризики для безпеки перевезень.

Зменшення інвестицій у розвиток аеропортів та морських портів призвело до зниження їхньої пропускної спроможності. Це негативно вплинуло на експортно-імпортні операції та зменшило доходи від міжнародних перевезень. Наприклад, обмеження фінансування аеропортів спричинило зниження якості обслуговування пасажирів та вантажів, що вплинуло на конкурентоспроможність українських авіакомпаній.

Вплив економічної кризи на комунальні послуги в Україні (2022-2024 роки)

Недостатність фінансування

Економічна криза, особливо в умовах військових конфліктів та високого рівня нестабільності, має значний вплив на фінансування комунальних послуг в Україні. В умовах обмежених ресурсів, багато місцевих бюджетів стикаються з серйозними проблемами у фінансуванні критичних комунальних інфраструктур, таких як водопостачання, водовідведення та теплопостачання.

Водопостачання: Під час економічних криз, відсутність достатнього фінансування призводить до недостатньої модернізації та обслуговування

водопровідних систем. Це призводить до зниження якості води, частих поривів труб, а також до збільшення витрат на ремонт. Наприклад, у 2023 році в кількох українських містах спостерігалися випадки погіршення якості води через старіння інфраструктури та відсутність коштів на її оновлення.

Водовідведення: Недостатність фінансування також вплинула на системи водовідведення. Багато комунальних підприємств не мають достатніх ресурсів для ефективного обслуговування та модернізації систем каналізації, що призводить до частих забруднень і проблем з відведенням стічних вод. Наприклад, в Києві та інших великих містах під час кризи 2022-2024 років спостерігалися випадки затоплень та забруднення територій через збої у роботі систем водовідведення.

Теплопостачання: Теплопостачання також постраждало від зменшення фінансування. Старі котельні та тепломережі часто не модернізуються, що призводить до підвищення витрат на енергію і частих аварій. У зимовий період 2022-2023 років, в умовах економічної кризи та дефіциту бюджету, в Україні виникли проблеми з забезпеченням стабільного теплопостачання, що особливо відчували мешканці багатоповерхових будинків та соціальні установи.

Зниження рівня обслуговування

Зростання числа аварій: Нестача фінансування прямо веде до зниження якості обслуговування комунальних послуг. Внаслідок цього зростає кількість аварій і технічних збоїв. У багатьох містах України під час кризи 2022-2024 років стали частими випадки перебоїв у водопостачанні, збоїв у системах водовідведення і проблеми з теплопостачанням.

Приклади аварій:

Водопостачання: У 2023 році в Харкові через аварії на старих водопровідних мережах відбулися великі перебої у водопостачанні, що спричинило затримки у постачанні води до житлових будинків і комерційних установ.

Водовідведення: У Львові та Одесі зафіксовані випадки забруднення територій через аварії в системах каналізації, що призвело до екологічних проблем і збільшення витрат на очистку.

Теплопостачання: У Києві та Дніпрі відзначалося підвищення аварійності на тепломережах, що створило проблеми для забезпечення стабільного теплопостачання в зимовий період, а також підвищило витрати на енергоносії.

Зниження рівня обслуговування: В умовах обмежених ресурсів комунальні служби змушені скорочувати витрати, що призводить до зниження рівня обслуговування. У багатьох містах України спостерігалося погіршення якості комунальних послуг, збільшення часу реагування на аварійні ситуації та затримки у виконанні ремонтних робіт.

Приклади зниження рівня обслуговування:

У 2024 році в Одесі затримки в ремонті водопровідних труб призвели до тривалих перебоїв у постачанні води, що вплинуло на повсякденне життя мешканців.

У Запоріжжі зниження рівня обслуговування систем водовідведення призвело до частих проблем з очищенням стічних вод, що погіршило екологічну ситуацію в місті.

Львові та інших містах проблеми з теплопостачанням через зниження якості обслуговування тепломереж створили труднощі для мешканців, особливо в умовах холодної погоди.

Вплив економічної кризи на охорону здоров'я в Україні (2022-2024 роки)

Дефіцит ресурсів

Економічні кризи часто супроводжуються серйозними фінансовими труднощами для державних та приватних медичних установ. В Україні, з початком військового конфлікту та економічної нестабільності, система охорони здоров'я зазнала значних труднощів через дефіцит ресурсів, що вплинуло на якість медичних послуг.

Фінансові ресурси: Обмежені бюджетні кошти та зменшення державних витрат на охорону здоров'я призводять до значного дефіциту фінансування для медичних установ. Це обмежує можливості для закупівлі медикаментів, медичного обладнання та оплати праці медичних працівників. Наприклад, у 2023 році у багатьох лікарнях України були виявлені проблеми з недостатньою кількістю медикаментів та медичного обладнання, що погіршило якість надання медичних послуг.

Матеріальні ресурси: Дефіцит матеріальних ресурсів, таких як медичне обладнання та інструменти, також негативно позначається на ефективності медичних послуг. У 2022-2024 роках спостерігалося зниження якості медичного обслуговування через застаріле або недостатньо забезпечене обладнання в лікарнях. Наприклад, у 2024 році у кількох областях України лікарні стикнулися з проблемами у забезпеченні сучасними діагностичними апаратами, що вплинуло на точність діагностування та ефективність лікування.

Відсутність сучасного медичного обладнання, як-от МРТ та КТ-апарати, у регіональних лікарнях призвела до зниження якості діагностики та лікування.

Нестача основних ліків і вакцин через дефіцит фінансування вплинула на лікування хронічних захворювань та профілактичні програми.

Закриття медичних закладів

Економічні кризи можуть також призвести до необхідності закриття малоефективних або малоприбуткових медичних закладів. Це викликане скороченням фінансування та необхідністю оптимізації витрат, що може мати серйозні наслідки для доступності медичних послуг.

Закриття лікарень: В умовах економічної кризи багато медичних закладів, особливо ті, що знаходяться в менш населених або економічно слабших регіонах, стикаються з необхідністю закриття через фінансові

труднощі. Наприклад, у 2023 році в ряді малих міст і сіл України було закрито кілька лікарень через зниження фінансування та нерентабельність.

Закриття амбулаторій: Закриття або скорочення роботи амбулаторій і поліклінік також є результатом економічної кризи. Це може призвести до збільшення навантаження на більші медичні установи та погіршення доступу до медичних послуг для населення. У 2024 році в кількох регіонах України спостерігалося закриття амбулаторій, що зменшило доступність первинної медичної допомоги для мешканців віддалених районів.

У Львівській області були закриті кілька лікарень через нестачу фінансування та низьку рентабельність.

В Одеській області було скорочено кількість поліклінік, що призвело до збільшення черг та навантаження на залишені медичні заклади.

Соціальні протести

Вплив соціальних протестів на енергетичну інфраструктуру в Україні

Фізичне пошкодження

Соціальні протести, які виникають у відповідь на політичні, економічні або соціальні невдоволення, можуть суттєво вплинути на об'єкти критичної інфраструктури, зокрема на енергетичну інфраструктуру. В Україні в період соціальних протестів було зафіксовано випадки фізичного пошкодження енергетичних об'єктів, що мало серйозні наслідки для забезпечення енергетичних потреб країни.

Приклад 1: Протести в 2021 році

У 2021 році в Україні відбулися численні акції протесту, які часто супроводжувалися насильством і агресією. В одному з таких випадків, протести в Києві призвели до атак на енергетичні об'єкти. Протестувальники пошкодили підстанцію, що спричинило значні перебої в електропостачанні в центральних районах міста. Пошкодження обладнання потребувало термінового ремонту, що в свою чергу викликало додаткові витрати і затримки в відновленні нормальної роботи електричних мереж.

Приклад 2: Протести в 2022 році

У 2022 році, під час масових протестів на сході України, відбулися напади на енергетичну інфраструктуру в зонах конфлікту. Внаслідок таких нападів були пошкоджені лінії електропередач і трансформаторні підстанції, що призвело до тривалих відключень електроенергії в постраждалих регіонах. Згідно з даними, кілька міст і селищ залишилися без електрики на кілька днів, що негативно вплинуло на повсякденне життя мешканців та роботу підприємств.

Збої у постачанні

Соціальні протести можуть також спричинити збої у постачанні енергії, блокуючи доступ до ключових енергетичних об'єктів або перешкоджаючи нормальному функціонуванню енергетичних систем.

Приклад 1: Блокування доступу до енергетичних об'єктів у 2023 році

У 2023 році, під час масових акцій протесту в Одесі, протестувальники блокували дороги, що ведуть до важливих енергетичних об'єктів, таких як електростанції і підстанції. Це ускладнило доставку необхідних ресурсів та обслуговування обладнання. Блокування доступу спричинило перебої у постачанні електроенергії в регіоні, що негативно вплинуло на життєдіяльність мешканців і роботу підприємств.

Приклад 2: Протести на сході України в 2024 році

Під час протестів на сході України в 2024 році протестувальники перекрили основні транспортні артерії, які використовуються для доставки пального на електростанції. Це призвело до дефіциту пального для генераторів, що в свою чергу спричинило перебої в постачанні електроенергії. В результаті, в кількох містах та селищах спостерігалися тривалі відключення електроенергії, що негативно вплинуло на економічну діяльність та соціальне середовище.

Вплив соціальних протестів на комунальні послуги

Соціальні протести можуть істотно вплинути на комунальні послуги, що включають водопостачання, теплопостачання, газопостачання та інші життєво

важливі послуги. Вплив може проявлятися через перерви у наданні послуг і фізичне пошкодження об'єктів комунальної інфраструктури.

Акції протесту можуть значно порушити стабільність надання комунальних послуг. Основні механізми впливу включають:

Блокування транспортних шляхів:

Протести часто супроводжуються блокуванням основних транспортних маршрутів. Це може ускладнити або навіть перешкодити доставці необхідних ресурсів та матеріалів до об'єктів комунальної інфраструктури. Наприклад, затримки в постачанні пального або сировини для обслуговування водопровідних і теплових систем можуть призвести до перебоїв у водопостачанні або опаленні.

Перекриття доступу до об'єктів інфраструктури:

Протестувальники можуть блокувати або перекривати доступ до важливих об'єктів комунальної інфраструктури, таких як насосні станції, котельні та водозабірні станції. Це ускладнює проведення планових і термінових ремонтних робіт, а також може призвести до затримок у відновленні надання послуг після аварій.

Затримки у виконанні обслуговувальних робіт:

Протести можуть заважати виконанню планових і термінових обслуговувальних робіт, таких як ремонт трубопроводів або обслуговування систем опалення. Це може негативно вплинути на якість надання послуг, оскільки затримки можуть призвести до збільшення кількості аварій або збоїв у постачанні комунальних послуг.

Фізичне пошкодження об'єктів комунальної інфраструктури є ще однією формою впливу соціальних протестів, що може мати серйозні наслідки для стабільності надання комунальних послуг:

Пошкодження водопровідних і каналізаційних систем:

Протестувальники можуть завдати шкоди водопровідним і каналізаційним системам, що призводить до витоків води, забруднення

навколишнього середовища і зниження якості води. Пошкодження трубопроводів і насосних станцій потребує термінового ремонту, що може бути ускладнено в умовах соціального напруження.

Пошкодження котелень і насосних станцій:

Протести можуть призвести до пошкодження об'єктів, що забезпечують теплопостачання і водопостачання, таких як котельні та насосні станції. Пошкодження такого обладнання може спричинити тимчасове припинення постачання тепла або води, що негативно вплине на комфорт і безпеку населення.

Пошкодження газових мереж:

Газові мережі також можуть постраждати від протестів, що веде до витоків газу і підвищеного ризику вибухів. Пошкодження газових трубопроводів вимагає термінового реагування і відновлення, оскільки витоки газу можуть створювати небезпеку для мешканців і навколишнього середовища.

2.4. Загрози воєнного характеру.

Енергетичний сектор України під час економічної та військової кризи 2022-2024 років

З 2022 року Україна зіткнулася з одночасною економічною та військовою кризою, спричиненою повномасштабним вторгненням Росії. Ці події мали руйнівний вплив на всі аспекти критичної інфраструктури, зокрема на енергетичний сектор. Масовані атаки на енергетичну інфраструктуру, брак ресурсів та складні економічні умови значно погіршили ситуацію, що призвело до зниження якості послуг, частих аварій та серйозних економічних втрат.

Масовані атаки на енергетичну інфраструктуру

З початку вторгнення у лютому 2022 року російські війська здійснили численні атаки на енергетичні об'єкти України, включаючи електростанції, підстанції, трансформатори та лінії електропередач. Ці атаки мали катастрофічні наслідки, зокрема знищення чи серйозне пошкодження ключових об'єктів енергетичної інфраструктури.

Наприклад, у жовтні 2022 року російські війська здійснили ракетний обстріл Київської області, що призвело до знищення однієї з великих підстанцій. Це спричинило масові відключення електроенергії у столиці та прилеглих районах, залишивши мільйони людей без світла.

Також у листопаді 2022 року відбулася атака на Запорізьку атомну електростанцію, яка є найбільшою в Європі. В результаті пошкодження критичних компонентів станції було знижено її потужність, що вплинуло на стабільність енергопостачання в багатьох регіонах України.

Економічні наслідки

Економічна криза, викликана війною, ще більше загострила ситуацію. Зменшення бюджетних надходжень, інфляція, дефіцит ресурсів та збільшення витрат на військові потреби призвели до скорочення фінансування на

модернізацію та обслуговування енергетичних об'єктів. Це поглибило проблеми, що виникли через атаки на інфраструктуру.

У 2023 році, за оцінками експертів, Україна втратила понад 10 мільярдів доларів через пошкодження енергетичної інфраструктури та перебої в постачанні електроенергії. Ці втрати включають не лише прямі витрати на відновлення об'єктів, але й економічні збитки від зупинки промислових підприємств та зниження продуктивності.

Енергетичні компанії, як державні, так і приватні, зіткнулися з дефіцитом ресурсів для проведення ремонту та модернізації. В умовах обмежених фінансових можливостей і високих цін на енергоресурси, багато проєктів з модернізації були відкладені або скасовані, що призвело до подальшого зниження надійності енергопостачання.

Соціальні наслідки

Соціальні наслідки кризи в енергетичному секторі виявилися особливо відчутними для населення України. Постійні перебої в постачанні електроенергії вплинули на всі аспекти життя, включаючи медичні послуги, освіту, комунальні послуги та побутові умови.

Перебої в електропостачанні: Зимовий період 2022-2023 років став особливо важким для українців. Часті відключення електроенергії змусили людей шукати альтернативні джерела опалення та освітлення. Це призвело до збільшення випадків використання небезпечних пристроїв, що спричинило пожежі та інші нещасні випадки.

Медичні послуги: Відключення електроенергії негативно вплинуло на роботу медичних установ. Наприклад, лікарні були змушені використовувати резервні генератори, які не завжди могли забезпечити стабільне постачання електроенергії для всіх необхідних пристроїв. Це ускладнювало надання медичної допомоги та ставило під загрозу життя пацієнтів.

Освіта: Перебої в електропостачанні також вплинули на освітній процес. Школи та університети були змушені переходити на дистанційне навчання або

скорочувати заняття через неможливість забезпечити необхідні умови для навчання в класах.

В Україні воєнні загрози виявляються у численних формах, включаючи прямі атаки на інфраструктуру, руйнування об'єктів і дестабілізацію життєво важливих систем. Розглянемо кілька ключових аспектів загроз воєнного характеру на прикладі України.

Атаки на енергетичні об'єкти

В умовах воєнного конфлікту енергетичні об'єкти, такі як електростанції, підстанції і лінії електропередач, стають цільовими для атак. Знищення або пошкодження таких об'єктів призводить до перебоїв у постачанні електроенергії, що негативно впливає на всі сфери життя – від побуту до промисловості.

Під час військових дій на сході України, зокрема в Донецькій і Луганській областях, спостерігались численні атаки на енергетичну інфраструктуру. Внаслідок обстрілів були зруйновані або пошкоджені високовольтні лінії та трансформаторні підстанції, що спричинило масштабні відключення електроенергії і проблеми з електропостачанням.

Дефіцит пального та матеріалів

Воєнні дії часто призводять до блокування транспортних шляхів і зниження постачання пального та інших необхідних матеріалів для енергетичних об'єктів. Це ускладнює обслуговування і ремонти, що може призвести до довготривалих перебоїв у постачанні енергії.

В умовах війни, особливо в зоні бойових дій, постачання пального для електростанцій може бути ускладнене. Це може призвести до зменшення виробництва електроенергії і проблем з енергетичною безпекою.

Руйнування транспортних артерій

Воєнні конфлікти часто супроводжуються атакою на дороги, мости, залізниці та аеропорти. Руйнування транспортних артерій ускладнює перевезення вантажів і людей, що негативно впливає на економіку та безпеку.

Під час військового конфлікту на сході України багато мостів і залізничних шляхів були зруйновані або пошкоджені. Це призвело до затримок у перевезенні гуманітарної допомоги і товарів, а також до труднощів у забезпеченні регулярного функціонування громадського транспорту.

Перешкоди для обслуговування транспорту

Обстріли і бойові дії можуть ускладнити проведення ремонту та обслуговування транспортної інфраструктури. Це веде до зниження якості обслуговування і збільшення ризику аварій.

У зонах бойових дій ремонтні роботи на дорогах і залізницях часто припиняються через небезпеку для працівників і пошкодження техніки. Це призводить до погіршення якості дорожнього покриття і затримок у транспортних перевезеннях.

Пошкодження комунальних об'єктів

Обстріли і атаки на об'єкти водопостачання, теплопостачання та газопостачання можуть призвести до їх фізичного пошкодження, що негативно впливає на надання основних послуг.

Військові дії в Україні призводили до пошкодження водозабірних станцій, насосних станцій і котелень, що спричинило перебої в водопостачанні і опаленні. Це особливо відчутно у зимовий період, коли відсутність опалення створює серйозні проблеми для населення.

В умовах воєнного конфлікту можуть виникати затримки у ремонті і обслуговуванні комунальних об'єктів через безпекові ризики і дефіцит ресурсів.

Під час активних бойових дій, особливо в зонах конфлікту, обслуговування і ремонт комунальних служб може бути ускладнене або зовсім припинене. Це призводить до зниження якості надання послуг і збільшення частоти аварій.

Руйнування медичних закладів

Атаки на медичні заклади можуть призвести до їх руйнування або пошкодження, що обмежує доступ до медичних послуг і погіршує умови лікування.

У зонах бойових дій в Україні були зафіксовані випадки обстрілу лікарень і медичних центрів. Це призводило до тимчасового закриття медичних установ і втрати можливостей для надання медичної допомоги постраждалим.

Воєнні дії можуть призвести до затримок у постачанні медичних товарів і обладнання, що погіршує якість медичних послуг.

Під час воєнного конфлікту постачання медичних матеріалів і обладнання може бути ускладнене через порушення логістичних ланцюгів, що впливає на здатність медичних установ забезпечувати адекватну допомогу пацієнтам.

Розділ 3. ШЛЯХИ УДОСКОНАЛЕННЯ ЗАСОБІВ ТА МЕТОДІВ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

3.1 Кіберзахист: виявлення та усунення вразливостей, інтелектуальні системи захисту.

У сучасному цифровому світі інформаційні технології стали невід'ємною частиною нашого повсякденного життя, бізнесу та державного управління. Від розрахункових систем у банках до особистих смартфонів, від урядових баз даних до критичної інфраструктури — інформаційні системи відіграють ключову роль у функціонуванні сучасного суспільства. Однак, з розвитком технологій зростають і ризики, що пов'язані з їх використанням. У цьому контексті кіберзахист стає критично важливим для забезпечення безпеки інформаційних систем і даних.

Кіберзахист, або інформаційна безпека, є системою заходів і технологій, спрямованих на захист інформації та інформаційних систем від кіберзагроз. Це включає в себе захист від несанкціонованого доступу, втрати даних, зловмисних атак і інших небезпек, які можуть порушити конфіденційність, цілісність та доступність інформаційних ресурсів. Ефективний кіберзахист є необхідним для забезпечення стабільної та безпечної роботи будь-якої організації чи індивідуального користувача, захищаючи їх від потенційних загроз, які можуть мати серйозні наслідки.

Кіберзагрози постійно еволюціонують, пристосовуючи свої методи атаки до нових технологій та систем. Це створює постійний виклик для фахівців з кібербезпеки, які повинні бути завжди на крок попереду зловмисників. Від класичних вірусів та троянів до складних атак на основі штучного інтелекту, кіберзагрози стають усе більш складними і небезпечними. Зловмисники використовують різноманітні техніки, такі як

фішинг, атаки на основі нульових днів, DDoS-атаки та інші методи, щоб обійти традиційні засоби захисту.

У зв’язку з постійною еволюцією кіберзагроз, практики виявлення та усунення вразливостей є основними компонентами будь-якої стратегії кіберзахисту. Виявлення вразливостей включає в себе систематичне ідентифікування слабких місць у системах, які можуть бути використані для атаки. Це може бути здійснено за допомогою різних методів, таких як сканування вразливостей, аудит систем та тестування на проникнення. Після виявлення вразливостей, критично важливо їх усунути шляхом оновлення систем, корекції конфігурацій і впровадження нових засобів захисту.

З метою забезпечення більш ефективної захищеності, впроваджуються інтелектуальні системи захисту, що використовують передові технології для автоматизації процесів безпеки. Ці системи використовують штучний інтелект і машинне навчання для аналізу великих обсягів даних, виявлення аномалій і потенційних загроз. Інтелектуальні системи захисту можуть адаптуватися до нових загроз, автоматично реагуючи на виявлені інциденти та зменшуючи ризик успішних атак.

Ефективний кіберзахист охоплює різноманітні стратегії та технології, що дозволяють забезпечити захищеність від потенційних загроз. Це включає в себе використання сучасних інструментів для виявлення та усунення вразливостей, впровадження інтелектуальних систем захисту, розробку політик безпеки і постійний моніторинг інформаційних систем. Важливо також забезпечити навчання і підвищення обізнаності користувачів щодо кіберзагроз і безпечних практик.

Виявлення вразливостей

Виявлення вразливостей є критично важливим кроком для підтримання безпеки інформаційних систем.

Це включає:

Аудит інформаційних систем

Є критично важливим компонентом забезпечення кібербезпеки. Він полягає у всебічному огляді та оцінці технічних та організаційних аспектів систем для виявлення слабких місць і уразливостей. Регулярні аудити допомагають виявити потенційні загрози, які можуть загрожувати цілісності, конфіденційності та доступності інформаційних ресурсів. Цей процес може бути проведений вручну або за допомогою автоматизованих засобів, і він охоплює перевірки системних конфігурацій, налаштувань безпеки, а також реалізації коду.

Методики проведення аудиту

Вручну проведення аудиту

Першим етапом ручного аудиту є перевірка документації, політик та процедур безпеки. Це включає аналіз документів, що регламентують налаштування безпеки систем, а також оцінку того, як ці документи відповідають поточним вимогам і стандартам. Важливо перевірити, чи існують документовані політики для управління доступом, обробки даних, резервного копіювання та відновлення.

Інтерв'ю з адміністраторами систем і кінцевими користувачами допомагають виявити потенційні проблеми, які можуть не бути видимими на рівні технічних перевірок. Це також дозволяє оцінити, наскільки добре користувачі розуміють політики безпеки і дотримуються їх. Інтерв'ю можуть виявити несумісності між теоретичними політиками і практичним застосуванням цих політик.

Ручний аудит передбачає перевірку конфігурацій систем на предмет дотримання найкращих практик і стандартів безпеки. Це може включати перевірку налаштувань сервера, бази даних, мережевих пристроїв і операційних систем. Аудитори перевіряють, чи конфігурації системи відповідають рекомендованим стандартам і чи є потенційні помилки або проблеми, які можуть бути використані зловмисниками.

Перевірка реалізації коду може включати перегляд вихідного коду для виявлення вразливостей, таких як небезпеки SQL-ін'єкцій, недостатня

перевірка вводу або проблеми з управлінням сесіями. Це може бути здійснено вручну або за допомогою спеціалізованих інструментів для аналізу статичного коду.

Автоматизоване проведення аудиту

Автоматизовані інструменти для сканування вразливостей можуть швидко перевіряти системи на предмет відомих уразливостей. Ці інструменти використовують бази даних відомих уразливостей і порівнюють конфігурації системи з цими базами даних, виявляючи потенційні слабкі місця.

Автоматизовані системи можуть також проводити аналіз логів для виявлення аномальної активності, яка може свідчити про спроби атаки або інші проблеми безпеки. Інструменти для аналізу логів можуть автоматично виявляти аномалії і генерувати звіти про можливі інциденти безпеки.

Спеціалізовані інструменти можуть автоматично перевіряти конфігурації системи на предмет відповідності стандартам безпеки. Це дозволяє швидко виявити невірні налаштування і пропустити можливості для атак.

Автоматизовані засоби статичного аналізу коду можуть перевіряти програмний код на наявність уразливостей без його виконання. Ці інструменти виявляють потенційні помилки і небезпеки, що може допомогти в усуненні проблем до того, як код буде запущено в продуктивному середовищі.

Переваги та виклики аудиту системи

Переваги

Регулярні аудити допомагають виявити слабкі місця і вразливості до того, як їх можуть використати зловмисники.

Аудити забезпечують можливість перегляду і оновлення політик і процедур безпеки, що підвищує загальний рівень захисту системи.

Виявлення і усунення уразливостей знижує ризик успішних атак, що може запобігти серйозним інцидентам безпеки.

Виклики

Проведення аудиту може вимагати значних ресурсів і часу, особливо для великих і складних систем. Це може бути обмеженням для організацій з обмеженим бюджетом.

Виявлення уразливостей і проблем у великих системах може бути складним завданням, що потребує висококваліфікованих спеціалістів.

Оскільки кіберзагрози постійно змінюються, системи і методи аудиту повинні постійно оновлюватися для забезпечення їх ефективності.

Сканування вразливостей

Сканування вразливостей є важливою складовою стратегії кібербезпеки, яка допомагає виявити слабкі місця в інформаційних системах, які можуть бути використані зловмисниками для здійснення атак. Це процес автоматизованого перевірки програмного забезпечення, апаратного забезпечення та мереж на предмет відомих уразливостей, що дозволяє організаціям вчасно реагувати на потенційні загрози. У цьому розділі ми детально розглянемо технології сканування вразливостей, популярні інструменти, а також переваги та виклики цього процесу.

Основи сканування вразливостей

Сканери вразливостей використовують бази даних із відомими уразливостями для перевірки систем на предмет їхньої наявності. Ці бази даних постійно оновлюються з інформацією про нові уразливості, які виявлені в програмному забезпеченні, апаратному забезпеченні та мережах. Сканери виконують різноманітні тести для виявлення слабких місць у системах, включаючи перевірку конфігурацій, тестування з'єднань і аналіз виходу системи.

Сканування вразливостей може бути реалізовано в кількох формах:

Активне сканування: Включає безпосереднє взаємодію з системою для перевірки її на предмет вразливостей. Це може включати сканування мережевих портів, перевірку конфігурацій і тестування на проникнення.

Пасивне сканування: Зосереджено на зборі інформації без безпосереднього взаємодії з системою. Це включає аналіз мережевого трафіку і логів для виявлення потенційних уразливостей.

Перевіряє правильність налаштувань системи відповідно до встановлених стандартів і рекомендацій.

Популярні інструменти для сканування вразливостей

1. Nessus

Nessus є одним з найбільш популярних і широко використовуваних інструментів для сканування вразливостей. Він пропонує велику кількість плагінів для перевірки різних аспектів системи на предмет вразливостей. Nessus виконує сканування на основі відомих уразливостей і надає детальні звіти з рекомендаціями щодо виправлення виявлених проблем. Його функціональність включає:

- Перевірка наявності відомих уразливостей.
- Аналіз конфігурацій і збережених налаштувань.
- Виявлення проблем із безпекою в веб-додатках і мережевих сервісах.

2. OpenVAS

OpenVAS (Open Vulnerability Assessment System) є відкритим інструментом для сканування вразливостей, який включає велику кількість інструментів для автоматизованого сканування і оцінки безпеки. OpenVAS має модульну архітектуру, що дозволяє розширювати його функціональність через додаткові плагіни. Основні можливості включають:

- Гнучкість у налаштуваннях сканування.
- Виконання глибоких перевірок на наявність уразливостей.
- Звіти з результатами сканування і рекомендаціями.

3. Qualys

Qualys пропонує потужні рішення для сканування вразливостей і управління безпекою, які можуть бути розгорнуті в хмарному середовищі або локально.

Цей інструмент забезпечує:

- Інтеграцію з іншими рішеннями для управління безпекою.
- Можливість масштабування для великих організацій.
- Аналіз і звіти в режимі реального часу.

Переваги та виклики сканування вразливостей

Переваги

Сканування вразливостей дозволяє проактивно виявляти слабкі місця в системах, що дозволяє вчасно їх усунути до того, як зловмисники зможуть скористатися ними.

Регулярне сканування допомагає забезпечити високий рівень безпеки шляхом виявлення і виправлення уразливостей, що знижує загальний ризик атак і порушень безпеки.

Інструменти для сканування вразливостей забезпечують детальні звіти, які можуть використовуватися для аудиту безпеки і підготовки до сертифікацій.

Виклики

Деякі сканери можуть генерувати помилкові спрацьовування або пропустити справжні уразливості, що потребує ручної перевірки результатів і подальшого аналізу.

Процес сканування може вимагати значних ресурсів і часу, особливо для великих і складних систем, що може вплинути на продуктивність системи під час сканування.

Оскільки кіберзагрози постійно змінюються, сканери вразливостей повинні постійно оновлювати свої бази даних і методики перевірки, що може бути складним завданням.

Тестування на проникнення (Penetration Testing): Методологія, процеси та переваги

Тестування на проникнення (Penetration Testing або Pen Test) є критично важливим компонентом оцінки безпеки інформаційних систем у сучасному цифровому світі. Як метод проактивної оцінки безпеки, Pen Test

полягає в імітації реальних атак на комп'ютерні системи, мережі, додатки та інші елементи інформаційної інфраструктури, щоб виявити їхні вразливості. Метою такого тестування є не тільки визначення технічних слабких місць у системі, але й оцінка ефективності існуючих процесуальних і організаційних заходів безпеки.

У сучасному світі, де кіберзагрози стають все більш складними та розвиненими, традиційні методи захисту часто виявляються недостатніми. Зловмисники постійно вдосконалюють свої техніки, що вимагає від організацій постійної адаптації та покращення своїх заходів безпеки. Тестування на проникнення дозволяє організаціям перевірити свою готовність до можливих атак, ідентифікувати вразливості до того, як їх виявлять справжні зловмисники, і забезпечити більш надійний захист даних і систем.

Методологія тестування на проникнення

Тестування на проникнення базується на принципі імітації реальних атак з метою оцінки безпеки системи, це проактивний метод тестування безпеки, при якому спеціалісти з кібербезпеки імітують атаки на інформаційні системи, щоб виявити їхні вразливості. Мета цього тестування полягає в перевірці можливостей системи захисту у випадку реальної атаки, виявленні слабких місць та наданні рекомендацій щодо їх усунення. Тестування може проводитися як зовні (з боку потенційних зловмисників), так і зсередини (від імені співробітників).

Види тестування на проникнення

Чорна скринька (Black Box) тестування

Чорна скринька (Black Box) тестування є одним з основних методів оцінки безпеки інформаційних систем, який не передбачає попереднього знання про внутрішню структуру або функціонування системи. Це тестування дозволяє імітувати дії справжнього зловмисника, який намагається отримати доступ до системи без будь-якого попереднього знання про її архітектуру або внутрішні механізми. Чорна скринька тестування є важливим для виявлення

вразливостей з точки зору зовнішнього зловмисника, який не має доступу до конфіденційної інформації.

Основи Чорної Скриньки Тестування

Чорна скринька тестування фокусується на зовнішньому тестуванні системи з метою виявлення уразливостей без використання внутрішньої інформації про її структуру. Тестувальники працюють із системою так, як це робив би реальний зловмисник, що дозволяє виявити потенційні слабкі місця, які можуть бути використані для несанкціонованого доступу. Тестування може включати різні аспекти системи, такі як веб-додатки, мережі, сервери, бази даних та інше.

Аналіз зовнішніх інтерфейсів: Тестувальники досліджують доступні інтерфейси системи, такі як веб-інтерфейси, API, порти та інші точки входу. Це дозволяє виявити уразливості, що можуть бути використані для проникнення в систему.

Розвідка та сканування: Включає збір інформації про систему, таких як відкриті порти, сервісні версії, мережеві топології та конфігурації. Використовуються інструменти для сканування мереж і портів, щоб визначити потенційні точки для атаки.

Експлуатація уразливостей: Після виявлення потенційних слабких місць тестувальники намагаються використати їх для проникнення в систему або отримання доступу до захищених ресурсів. Це може включати атаки на паролі, SQL-ін’єкції, міжсайтові скрипти та інші техніки.

Процес Чорної Скриньки Тестування

1. Планування і підготовка

На початку тестування визначаються обсяги і мета тестування. Тестувальники погоджують з клієнтом області системи, які будуть підлягати тестуванню, та отримують всі необхідні дозволи. Важливо встановити чіткі межі тестування, щоб уникнути порушень і небажаних наслідків.

2. Збір інформації

Збір інформації є критично важливим етапом для чорної скриньки тестування. Тестувальники використовують різні методи для отримання інформації про систему, включаючи аналіз доменних імен, сканування мережі, пасивний збір даних і техніки соціальної інженерії. Цей етап дозволяє визначити потенційні точки входу і слабкі місця в системі.

3. Аналіз вразливостей

Після збору інформації тестувальники виконують аналіз для виявлення можливих уразливостей. Це включає використання автоматизованих інструментів для сканування та оцінки вразливостей, а також ручний аналіз для перевірки отриманих результатів. Тестувальники аналізують результати, щоб визначити, які уразливості можуть бути експлуатовані.

4. Експлуатація уразливостей

На цьому етапі тестувальники намагаються використати виявлені уразливості для доступу до системи або ресурсів. Це може включати спроби несанкціонованого доступу, атак на паролі, SQL-ін’єкції, міжсайтові скрипти, фальсифікацію запитів та інші техніки. Мета цього етапу — підтвердити наявність уразливостей і оцінити їхній вплив на безпеку системи.

5. Звітність і рекомендації

Після завершення тестування тестувальники складають детальний звіт, який включає опис виявлених уразливостей, їхній рівень ризику, можливі наслідки та рекомендації для усунення вразливостей. Звіт має бути зрозумілим і корисним для технічних фахівців та управлінців, щоб вони могли ефективно впровадити рекомендації і покращити загальний рівень безпеки системи.

Переваги і виклики Чорної Скриньки Тестування

Переваги:

Чорна скринька тестування дозволяє отримати уявлення про те, як зовнішній зловмисник може взаємодіяти з системою, без знання її внутрішньої структури. Це дозволяє виявити уразливості, які можуть бути використані для атаки.

Тестування допомагає виявити уразливості, які можуть бути пропущені при внутрішньому тестуванні або звичайному скануванні, зокрема уразливості, що пов’язані з зовнішніми інтерфейсами та сервісами.

Виклики:

Оскільки тестувальники не мають доступу до внутрішньої інформації про систему, це може ускладнити процес виявлення деяких вразливостей і може потребувати більше часу для збору інформації та аналізу.

Імітація реальних атак може призвести до помилок або негативних наслідків, якщо не буде дотримано належного контролю і планування. Важливо забезпечити чіткі межі тестування та отримати всі необхідні дозволи.

Сіра скринька (Gray Box) тестування

Сіра скринька (Gray Box) тестування є проміжним підходом між чорним і білим (White Box) тестуванням, що надає тестувальникам обмежену інформацію про внутрішню структуру системи. Цей метод дозволяє виявити вразливості з урахуванням деяких деталей про систему, що може зробити процес тестування більш ефективним порівняно з чорною скринькою, але без детального знання системи, яке є характерним для білого тестування.

Основи Сірої Скриньки Тестування

Сіра скринька тестування поєднує елементи як чорної, так і білої скриньки тестування. Тестувальники мають доступ до часткової інформації про систему, такої як специфікації, документація, частини коду або архітектурні діаграми. Це дозволяє їм орієнтуватися в системі та зосередитися на певних ділянках, але без повного розуміння внутрішньої структури. Тестування може включати перевірку зовнішніх інтерфейсів, а також аналіз внутрішніх компонентів на основі отриманої інформації.

Частковий доступ до інформації: Тестувальники можуть отримати доступ до деякої технічної інформації про систему, такої як архітектура, діаграми потоку даних або документація з API. Це допомагає зосередитися на ключових ділянках системи та виявити вразливості, які можуть бути пропущені при чорному тестуванні.

Комбінація методів: Сіра скринька тестування використовує як методи, характерні для чорної скриньки (наприклад, зовнішні атаки та сканування), так і методи білого тестування (наприклад, аналіз конфігурацій і внутрішніх компонентів). Це дозволяє отримати більш детальну картину безпеки системи.

Аналіз результатів: Тестувальники аналізують отримані результати на основі часткової інформації та зосереджуються на виявленні уразливостей, які можуть бути використані для атаки. Вони можуть використовувати автоматизовані інструменти та ручний аналіз для оцінки вразливостей.

Процес Сірої Скриньки Тестування

Процес сірої скриньки тестування починається з визначення обсягів та цілей тестування. Тестувальники отримують обмежену інформацію про систему, таку як технічні специфікації, документацію або частини коду. Цей етап також включає встановлення меж тестування та отримання всіх необхідних дозволів.

На цьому етапі тестувальники збирають та аналізують інформацію, яку вони отримали. Це може включати вивчення технічної документації, архітектурних діаграм, конфігураційних файлів або інших часткових даних. Тестувальники використовують цю інформацію для визначення потенційних точок входу і вразливостей, що можуть бути використані для атаки.

Тестувальники здійснюють тестування, використовуючи отриману інформацію для виявлення уразливостей. Це може включати перевірку конфігурацій, аналіз коду, сканування системи та імітацію атак. Тестування може бути виконано як вручну, так і з використанням автоматизованих інструментів.

Після виконання тестування тестувальники аналізують результати для виявлення уразливостей і оцінюють їхній рівень ризику. Вони складають звіт, в якому описують виявлені проблеми, їхній вплив на безпеку системи та надають рекомендації для усунення вразливостей.

На основі отриманих результатів тестування складаються рекомендації для покращення безпеки системи. Це може включати виправлення

вразливостей, вдосконалення конфігурацій або зміну процесів безпеки. Рекомендації мають бути чіткими і зрозумілими для технічних фахівців та управлінців.

Переваги і виклики Сірої Скриньки Тестування

Переваги:

Баланс між знанням і невідомістю: Сіра скринька тестування дозволяє отримати більш детальну картину безпеки системи, маючи часткову інформацію про її внутрішню структуру. Це може забезпечити більше результативних і точних виявлень уразливостей.

Ефективність: Тестування з частковою інформацією може бути ефективнішим, ніж тестування без будь-якої інформації, оскільки тестувальники можуть зосередитися на певних аспектах системи.

Виклики:

Обмежене знання: Хоча сіра скринька тестування передбачає часткову інформацію про систему, цього може бути недостатньо для повного розуміння всіх вразливостей. Це може призвести до пропуску деяких проблем або уразливостей.

Ризик неповного тестування: Відсутність повного доступу до внутрішньої інформації може ускладнити виявлення деяких вразливостей, що можуть бути помічені при білому тестуванні.

Біла скринька (White Box) тестування

Біла скринька тестування, також відоме як тестування з відкритим кодом або структурне тестування, є методологією, при якій тестувальники мають повний доступ до внутрішньої інформації системи. Це включає вихідний код, архітектурні діаграми, конфігураційні файли та інші деталі, що дозволяють глибше досліджувати внутрішню структуру системи. У цьому підході тестування надає можливість виявити більш складні вразливості і проблеми безпеки, які можуть бути непомітні при тестуванні з обмеженим доступом.

Основи Білої Скриньки Тестування

Біла скринька тестування передбачає наявність детальної інформації про систему, що дозволяє тестувальникам здійснювати глибокий аналіз внутрішніх компонентів і коду. Тестування може включати перевірку логіки програми, аналіз алгоритмів, перевірку інтеграцій між компонентами та оцінку конфігураційних налаштувань. Це дозволяє виявити уразливості, які можуть бути важкими для виявлення при інших методах тестування.

Аналіз вихідного коду: Тестувальники переглядають вихідний код програми для виявлення потенційних уразливостей, таких як помилки в логіці програми, невірні реалізації алгоритмів або недостатні механізми обробки помилок. Це дозволяє знайти вразливості, які можуть бути пропущені при чорному або сірому тестуванні.

Аналіз конфігурацій: Тестування включає перевірку конфігураційних налаштувань системи, таких як параметри безпеки, доступи та інтеграції. Це дозволяє виявити проблеми, які можуть вплинути на безпеку, навіть якщо код програми сам по собі є коректним.

Тестування безпеки на рівні архітектури: Оцінка архітектурних рішень системи може допомогти виявити проблеми, такі як неправильні реалізації компонентів або слабкі місця в інтеграціях. Це включає перевірку діаграм архітектури та проектних рішень.

Процес Білої Скриньки Тестування

Процес білої скриньки тестування починається з визначення обсягів тестування, цілей та отримання всіх необхідних дозволів. Тестувальники отримують повний доступ до інформації про систему, включаючи вихідний код, архітектурні документи та конфігураційні файли. Планування включає визначення ключових компонентів для аналізу та розробку стратегії тестування.

На цьому етапі тестувальники збирають всю необхідну інформацію про систему. Це може включати перегляд вихідного коду, документації, конфігураційних файлів і архітектурних діаграм. Зібрана інформація

використовується для розробки тестових сценаріїв та перевірки специфічних компонентів системи на наявність вразливостей.

Тестувальники виконують тестування на основі отриманої інформації. Це може включати перевірку логіки програми, аналіз алгоритмів, тестування на проникнення з використанням знання внутрішньої структури та конфігурацій. Тестування може бути як автоматизованим, так і ручним. Інструменти для аналізу коду, такі як статичний аналізатор коду, можуть використовуватися для автоматизації процесу.

Після виконання тестування тестувальники аналізують результати для виявлення уразливостей і оцінюють їхній вплив на безпеку системи. Це може включати виявлення логічних помилок, проблем з обробкою помилок або неправильних конфігурацій. Тестувальники складають звіт, в якому описують виявлені проблеми, їхній вплив та надають рекомендації для їх усунення.

На основі результатів тестування складаються рекомендації для покращення безпеки системи. Це може включати виправлення вразливостей у коді, вдосконалення конфігурацій або зміну архітектурних рішень. Рекомендації мають бути конкретними та орієнтованими на усунення виявлених проблем.

Переваги і виклики Білого Скриньки Тестування

Переваги:

Маючи доступ до всіх внутрішніх деталей системи, тестувальники можуть провести глибокий аналіз і виявити вразливості, які можуть бути недоступними при інших методах тестування.

Біла скринька тестування дозволяє виявити складні проблеми в логіці програми та реалізації, які можуть бути важкими для імітації з боку зловмисника.

Виявлення проблем на етапі тестування допомагає покращити якість коду і забезпечити надійність програмного забезпечення.

Виклики:

Глибокий аналіз коду і конфігурацій може бути часозатратним і вимагати значних ресурсів. Це може бути проблемою для великих систем або для проектів з обмеженим бюджетом.

Якщо код системи часто оновлюється, підтримка актуальності тестування може бути складною. Постійні зміни можуть вплинути на точність і ефективність виявлення вразливостей.

Хоча біле тестування забезпечує глибокий аналіз, воно може не враховувати всі можливі сценарії атаки, особливо якщо зловмисник використовує нові або невідомі методи.

Інструменти які я рекомендую для покращення і удосконалення для тестування на проникнення

Metasploit

Metasploit є одним з найбільш потужних інструментів для тестування на проникнення. Він надає велику кількість експлойтів і сканерів для виявлення і використання вразливостей. Metasploit дозволяє автоматизувати багато аспектів тестування і надає зручний інтерфейс для проведення атак.

Burp Suite

Burp Suite є інструментом для тестування безпеки веб-додатків. Він включає функції для сканування вразливостей, аналізу трафіку, проведення атак на веб-додатки та виявлення небезпечних конфігурацій. Burp Suite дозволяє ефективно тестувати безпеку веб-інтерфейсів і забезпечує інструменти для глибокого аналізу.

Nmap

Nmap є популярним інструментом для сканування мережі, який допомагає виявляти відкриті порти, активні служби і вразливості. Він є важливим інструментом для збору інформації на початковому етапі тестування і дозволяє визначити потенційні точки входу для подальших атак.

Переваги та виклики тестування на проникнення

Переваги

на проникнення дозволяє виявити не тільки відомі уразливості, але й нові, які можуть бути використані зловмисниками.

Регулярне тестування допомагає постійно удосконалювати системи безпеки і запобігати можливим атакам.

Імітація реальних атак дозволяє отримати точну оцінку ефективності існуючих заходів безпеки і підготуватися до можливих загроз.

Усунення вразливостей

Після виявлення вразливостей необхідно їх усунути. Основні етапи цього процесу включають:

Після виявлення вразливостей в інформаційних системах, одним із найважливіших кроків є їх усунення. Одним з основних етапів цього процесу є оновлення і патчування. Це включає регулярне оновлення програмного забезпечення і встановлення патчів для забезпечення безпеки системи. Ось детальний огляд цього процесу:

1.Оновлення програмного забезпечення

Оновлення програмного забезпечення є критично важливим для підтримання безпеки і функціональності інформаційних систем. Своєчасне оновлення програмного забезпечення забезпечує закриття відомих вразливостей і виправлення помилок, що допомагає уникнути можливих атак та інших проблем. Процес оновлення включає кілька ключових етапів, кожен з яких має своє значення. Розглянемо ці етапи детально, з прикладами:

Ідентифікація оновлень

Ідентифікація оновлень є першим кроком у процесі управління оновленнями програмного забезпечення. Цей етап передбачає виявлення доступних оновлень і виправлень для системи.

Багато постачальників програмного забезпечення пропонують служби підписки, які надсилають повідомлення про нові оновлення. Наприклад, Microsoft надає сервіс Windows Update, який автоматично повідомляє користувачів про нові оновлення для операційної системи Windows.

Для великих організацій або для систем, які використовують численні компоненти, можуть бути використані автоматизовані системи управління оновленнями, такі як WSUS (Windows Server Update Services) для Windows або Red Hat Satellite для Linux. Ці системи автоматично перевіряють наявність оновлень і управляють їх впровадженням.

Приклад:

Організація використовує програму Adobe Creative Cloud, яка регулярно отримує оновлення. Користувачі можуть підписатися на оновлення через Adobe Update Manager, який сповіщає про нові версії програм та їх виправлення.

Оцінка впливу

Оцінка впливу перед впровадженням оновлень є важливою для забезпечення того, що оновлення не вплине негативно на систему.

Оновлення можуть вплинути на сумісність з іншими додатками або компонентами системи. Наприклад, нове оновлення для бази даних Oracle може вимагати оновлення також для пов'язаних додатків або драйверів.

Важливо оцінити ризики, пов’язані з встановленням оновлення. Для цього організації можуть використовувати інструменти для управління конфігураціями і перевірки сумісності, такі як TestComplete або AppDynamics.

Приклад:

Компанія планує оновити свою операційну систему з Windows 10 до Windows 11. Перед впровадженням оновлення, команда IT перевіряє, чи всі критичні програми, такі як SAP ERP та Salesforce, сумісні з новою версією.

Тестування оновлень

Тестування оновлень перед їх впровадженням у продуктивне середовище є критично важливим для забезпечення безперебійної роботи системи.

Оновлення слід спочатку тестувати в тестовому або неактивному середовищі. Наприклад, у середовищі QA (Quality Assurance) можна перевірити, чи не виникають проблеми після впровадження оновлень.

Перед тестуванням важливо створити резервні копії системи, щоб у разі виникнення проблем можна було повернутися до попередньої версії.

Приклад:

Організація використовує платформу Salesforce і планує оновити до нової версії. Вона створює окрему тестову версію свого середовища на Salesforce Sandbox для перевірки нових функцій і виправлень, перед тим як запровадити оновлення у продуктивному середовищі.

Встановлення оновлень

Встановлення оновлень є наступним етапом після успішного тестування. Це може бути здійснено вручну або автоматизовано, в залежності від політики організації.

Вручну: Оновлення можуть бути встановлені вручну, особливо в малих або середніх організаціях, де автоматизація не є необхідною. Це включає завантаження оновлень і їх впровадження вручну, часто через інтерфейс користувача або командний рядок.

Автоматизовано: Для великих організацій автоматизація процесу оновлення може бути необхідною. Інструменти, такі як Puppet, Chef або Ansible, дозволяють автоматизувати впровадження оновлень у великій кількості систем.

Приклад:

В організації, що використовує Linux сервери, автоматичне оновлення може бути налаштоване через cron jobs для регулярного завантаження і встановлення оновлень без необхідності ручного втручання.

Моніторинг і підтримка

Моніторинг і підтримка після впровадження оновлень забезпечує, що система функціонує як очікувалося, і дозволяє своєчасно реагувати на будь-які проблеми.

Використання інструментів моніторингу, таких як Nagios, Zabbix або Datadog, дозволяє відстежувати стан системи після впровадження оновлень, виявляти проблеми і реагувати на них.

Після оновлення слід збирати зворотний зв'язок від користувачів і адміністративного персоналу для виявлення можливих проблем або поліпшень.

Приклад:

Після впровадження оновлення для веб-сервера Apache, команда IT використовує Grafana для моніторингу продуктивності сервера і забезпечення відсутності проблем із швидкістю відповіді або доступністю сервісів.

Патчування: процес, приклади та рекомендації

Патчування — це процес оновлення програмного забезпечення з метою виправлення виявлених вразливостей, помилок або недоліків. Патчування є важливим аспектом управління безпекою програмного забезпечення і забезпечує виправлення вразливостей та помилок, які можуть бути використані зловмисниками.

Процес патчування включає кілька ключових етапів: виявлення патчів, аналіз, тестування, впровадження, документування і аналіз ефективності. Розглянемо ці етапи детально, наводячи приклади для кожного з них.

Виявлення патчів

Виявлення патчів є першим кроком у процесі патчування. Це включає регулярний моніторинг доступності нових патчів та оновлень для програмного забезпечення, яке використовується в організації.

Постачальники програмного забезпечення, такі як Microsoft, Oracle, або Adobe, публікують патчі на своїх офіційних веб-сайтах. Наприклад, Microsoft регулярно публікує оновлення в рамках Patch Tuesday, які включають виправлення для Windows і інших продуктів.

Організації можуть використовувати спеціалізовані системи для управління патчами, такі як WSUS (Windows Server Update Services) або Red Hat Satellite для Linux, які автоматично перевіряють наявність нових патчів і повідомляють про їх доступність.

Приклад:

Організація використовує Jira для управління проектами і регулярно перевіряє оновлення через сайт Atlassian, де публікуються патчі для усунення вразливостей і помилок у програмному забезпеченні.

Аналіз патчів

Аналіз патчів є важливим для оцінки впливу патчу на систему. Це включає перегляд документації патча, оцінку можливих змін і перевірку сумісності.

Патчі зазвичай супроводжуються документацією від постачальника, яка описує усунені проблеми і нові функції. Наприклад, патчі для Oracle Database можуть містити документацію, яка пояснює виправлення уразливостей і вплив на існуючі функції бази даних.

Необхідно оцінити можливий вплив патча на систему, включаючи його вплив на продуктивність і сумісність з іншими компонентами. Наприклад, патч для Apache HTTP Server може змінити конфігурацію сервера, що може вимагати додаткових налаштувань.

Приклад:

Організація отримала патч для Java Runtime Environment (JRE), який виправляє критичну уразливість. Перед впровадженням патчу команда IT аналізує документацію, щоб перевірити, як патч вплине на існуючі додатки, які використовують JRE.

Тестування патчів

Тестування патчів допомагає виявити можливі побічні ефекти або конфлікти перед впровадженням патчів у продуктивне середовище.

Патчі слід спочатку тестувати в тестовому середовищі або середовищі QA. Це може бути віртуальне середовище, яке імітує продуктивне середовище, щоб перевірити вплив патчу без ризику для основної системи.

Тестування повинно включати перевірку основних функцій системи, щоб переконатися, що патч не порушує їх. Наприклад, після впровадження патча для MySQL важливо перевірити, чи всі SQL-запити виконуються без помилок.

Приклад:

Після отримання патчу для WordPress, команда тестування встановлює його на тестовому сервері і перевіряє всі основні плагіни та теми, щоб переконатися, що патч не порушує їх функціональність.

Впровадження патчів

Впровадження патчів є наступним етапом після успішного тестування. Це може бути здійснено вручну або автоматизовано.

Автоматизоване впровадження: Для великих організацій автоматизація патчування може бути здійснена за допомогою систем управління патчами, таких як SCCM (System Center Configuration Manager) або Ansible.

Вручну*:* Для менших систем патчі можуть бути встановлені вручну через інтерфейс користувача або командний рядок.

Приклад:

В організації, що використовує Microsoft Exchange Server, патчі можуть бути впроваджені через SCCM, що автоматично розгортає оновлення на всіх поштових серверах, забезпечуючи їх безперебійну роботу.

Документування і звітність

Документування і звітність є важливими для забезпечення прозорості процесу патчування і для ведення історії впроваджених патчів.

Важливо документувати всі етапи патчування, включаючи дати впровадження, застосовані патчі, і будь-які проблеми, що виникли. Це може включати записи в системах управління інцидентами або документації для забезпечення відповідності.

Регулярні звіти про стан патчування допомагають стежити за виконанням політики безпеки і своєчасним впровадженням виправлень.

Приклад:

Після впровадження патчів для SAP ERP, команда IT документує всі дії у внутрішній системі управління проектами і створює звіт, який включає деталі про патчі, проблеми, що виникли, і рекомендації для подальших дій.

Аналіз ефективності

Аналіз ефективності включає перевірку того, чи було усунуто вразливість і чи не виникли нові проблеми після впровадження патчів.

Після впровадження патчів необхідно перевірити, чи дійсно усунуто вразливості. Це може включати повторне тестування системи або використання сканерів уразливостей для перевірки ефективності патчів.

Перевірка впливу патчів на продуктивність системи. Наприклад, патч для MySQL може вплинути на швидкість запитів, тому важливо перевірити, чи не вплинула зміна на швидкість роботи бази даних.

Приклад:

Після впровадження патча для Cisco IOS, команда безпеки використовує сканери уразливостей, щоб перевірити, чи виправлено уразливість, зазначену в патчі, і забезпечити, що система продовжує працювати стабільно.

Інструменти для управління оновленнями і патчами

Для спрощення процесу управління оновленнями і патчами існують спеціалізовані інструменти, які автоматизують багато етапів цього процесу:

Системи управління оновленнями: Інструменти, такі як WSUS (Windows Server Update Services) або системи централізованого управління оновленнями, дозволяють автоматично завантажувати і розгортати оновлення в мережі організації.

Платформи для патчування: Інструменти, як Nessus або Qualys, допомагають ідентифікувати відсутні патчі і вразливості, надаючи звіти і рекомендації щодо їх усунення.

Моніторингові системи: Інструменти моніторингу, такі як Nagios або Zabbix, дозволяють спостерігати за станом системи після впровадження оновлень і патчів, виявляючи будь-які проблеми в режимі реального часу.

2. Конфігурація безпеки

Конфігурація безпеки є ключовим аспектом в забезпеченні належного захисту інформаційних систем і даних. Це включає налаштування системи

таким чином, щоб зменшити можливості для несанкціонованого доступу, атаки та інших загроз. Ось як можна забезпечити належну конфігурацію безпеки:

Налаштування Брандмауерів

Брандмауер (або фаєрвол) є першим рівнем захисту мережі. Він контролює вхідний та вихідний трафік на основі налаштованих правил. Основні аспекти налаштування брандмауера включають:

Брандмауер може бути налаштований для блокування певних портів або IP-адрес, що зменшує ймовірність атаки. Наприклад, закриття портів, які не використовуються, допомагає зменшити можливі вектори атаки.

Визначення правил, які дозволяють або забороняють доступ до певних ресурсів на основі IP-адрес або протоколів. Наприклад, дозволити доступ до бази даних тільки з внутрішньої мережі компанії.

Ведення журналів подій, що дозволяє аналізувати спроби доступу і реагувати на підозрілі активності. Наприклад, системи можуть автоматично блокувати IP-адреси, з яких зафіксовано підозрілі запити.

Приклад:

Налаштування брандмауера в Cisco ASA для блокування всіх вхідних з'єднань, окрім тих, що надходять від дозволених IP-адрес і використовують затверджені порти.

Контроль Доступу

Контроль доступу включає в себе визначення, хто має доступ до систем і даних, і які дії можуть виконуватися.

Основні елементи включають:

Аутентифікація: Перевірка особи або системи, яка намагається отримати доступ до ресурсу. Це може включати паролі, двофакторну аутентифікацію (2FA) або біометричні дані. Наприклад, використання Microsoft Active Directory для управління доступом користувачів до корпоративних ресурсів.

Авторизація: Налаштування прав доступу для різних користувачів або груп. Наприклад, забезпечення того, що тільки адміністратори можуть

змінювати налаштування системи, а звичайні користувачі можуть тільки переглядати дані.

Принцип Мінімальних Привілеїв*:* Надання користувачам тільки тих прав, які необхідні для виконання їхніх обов'язків. Наприклад, надання користувачеві права на читання файлів, але не на їх зміну.

Приклад:

Налаштування ролей і дозволів в Linux за допомогою системи SELinux (Security-Enhanced Linux) для забезпечення, що лише авторизовані користувачі можуть отримати доступ до чутливих файлів.

Шифрування Даних

Шифрування забезпечує захист даних, перетворюючи їх у формат, який не можна прочитати без спеціального ключа. Основні аспекти шифрування включають:

Шифрування Транзиту: Захист даних під час їх передачі по мережі. Наприклад, використання SSL/TLS для захисту даних, що передаються між веб-браузером і веб-сервером.

Шифрування Зберігання: Захист даних, які зберігаються на дисках або в базах даних. Наприклад, використання AES (Advanced Encryption Standard) для шифрування файлів на жорсткому диску.

Управління Ключами*:* Належне управління шифрувальними ключами є критично важливим. Ключі повинні зберігатися в безпечному місці і регулярно оновлюватися. Наприклад, використання Hardware Security Modules (HSM) для управління криптографічними ключами.

Приклад:

Шифрування бази даних за допомогою Transparent Data Encryption (TDE) в Microsoft SQL Server, яке забезпечує автоматичне шифрування даних на диску і під час їх збереження.

Регулярний аудит конфігурацій

Аудит конфігурацій допомагає виявити потенційні уразливості в налаштуваннях системи.

Це може включати:

Перевірка, чи відповідають конфігурації політикам безпеки організації. Наприклад, перевірка, чи всі сервери мають актуальні патчі безпеки.

Виявлення Невідповідностей: Ідентифікація будь-яких налаштувань, які можуть бути потенційними уразливостями. Наприклад, виявлення незахищених портів або неправильно налаштованих прав доступу.

Оновлення Конфігурацій: Регулярне оновлення налаштувань системи на основі результатів аудиту. Наприклад, зміна налаштувань брандмауера для закриття нових небезпечних портів.

Приклад:

Виконання автоматизованих перевірок конфігурацій за допомогою інструментів, таких як Nessus або OpenVAS, для виявлення слабких місць у налаштуваннях безпеки.

Зміна паролів і управління доступом:

Зміна паролів і управління доступом є критично важливими аспектами забезпечення інформаційної безпеки. Управління паролями та контролем доступу допомагає захистити системи від несанкціонованого доступу і зменшити ризики, пов’язані з компрометацією облікових записів.

Ось детальний огляд процесів і практик, що стосуються змін паролів і управління доступом:

Регулярна зміна паролів

Регулярна зміна паролів є одним з основних заходів безпеки, що допомагає запобігти використанню зламаних паролів і зменшити ризики доступу до облікових записів.

Паролі слід змінювати через певні інтервали часу, щоб зменшити ймовірність їх компрометації. Наприклад, у корпоративних середовищах може бути рекомендовано змінювати паролі кожні 60 або 90 днів.

Зміна паролів повинна включати створення складних паролів, що містять комбінації великих і малих літер, цифр і спеціальних символів.

Наприклад, замість простого пароля "Password123" слід використовувати "R3d!$Unicorn$2024".

Менеджери паролів допомагають зберігати і управляти численними складними паролями, автоматично генеруючи і запам’ятовуючи їх. Наприклад, LastPass або 1Password можуть використовуватися для зберігання паролів і автоматичного заповнення полів входу.

Приклад:

Якщо компанія вимагає, щоб паролі для всіх облікових записів змінювалися кожні 90 днів, це може включати автоматизовану політику в корпоративному середовищі, що нагадує користувачам про необхідність зміни пароля заздалегідь.

Використання Багатофакторної Автентифікації (MFA)

Багатофакторна автентифікація (MFA) додає додатковий рівень захисту шляхом вимагання декількох форм підтвердження особи.

MFA вимагає, щоб користувачі надали більше ніж один фактор автентифікації для доступу до системи. Це можуть бути щось, що користувач знає (пароль), має (мобільний телефон для отримання коду) або є (біометричні дані).

Поширені методи включають SMS-коди, електронні повідомлення з кодами, біометричні сканери (відбитки пальців, розпізнавання обличчя) і спеціальні апаратні токени (наприклад, YubiKey).

Для впровадження MFA в корпоративному середовищі може бути використано програмне забезпечення або послуги, такі як Google Authenticator, Microsoft Authenticator, або Duo Security.

Приклад:

У банківському середовищі користувачі можуть бути змушені ввести свій пароль та одноразовий код, надісланий на їхній мобільний телефон, щоб увійти до своїх онлайн-рахунків.

Принцип найменшого привілею

Принцип найменшого привілею передбачає надання користувачам тільки тих прав доступу, які необхідні для виконання їхніх завдань. Це допомагає зменшити ризик зловживання доступом та забезпечити додатковий захист від внутрішніх загроз.

Обмеження прав доступу: Користувачі повинні мати доступ лише до ресурсів і даних, які їм потрібні для виконання їхніх обов'язків. Наприклад, звичайні користувачі не повинні мати адміністративного доступу до системи.

Ролі та Групи: Налаштування ролей і груп у системах для управління доступом може допомогти реалізувати принцип найменшого привілею. Наприклад, в системі Active Directory можна створити різні групи з обмеженими правами доступу до різних частин мережі.

Перегляд доступу: Регулярний перегляд і оновлення прав доступу допомагають забезпечити, що користувачі мають лише необхідні права. Це включає видалення доступу у випадку зміни посадових обов’язків або звільнення співробітника.

Приклад:

У великих компаніях, де адміністратори мають доступ до критично важливих систем, звичайні користувачі можуть мати доступ тільки до офісних документів і електронної пошти, що обмежує можливість доступу до чутливих даних.

Політики безпеки паролів

Розробка і впровадження політик безпеки паролів є важливою частиною управління доступом.

Політики безпеки можуть вказувати на необхідність використання складних паролів, які включають комбінації літер, цифр і символів.

Визначення максимального часу дії пароля перед його зміною, наприклад, кожні 60 або 90 днів.

Забороняється повторне використання старих паролів протягом певного періоду, щоб уникнути їх повторного використання.

Приклад:

Організація може впровадити політику, що вимагає створення паролів довжиною не менше 12 символів, що включає принаймні одну велику літеру, одну малу літеру, одну цифру і один спеціальний символ, а також зміну паролів кожні 60 днів.

Навчання Користувачів

Останній важливий аспект управління паролями і доступом – це навчання користувачів.

Проведення навчальних курсів або семінарів, що допомагають користувачам розуміти важливість безпеки паролів і правильного управління доступом.

Інформування користувачів про методи створення надійних паролів і уникання фішингових атак.

Приклад:

Організація може провести тренінги для співробітників, що навчають їх правильному створенню паролів, розпізнаванню фішингових атак і використанню двофакторної автентифікації.

3.Інтелектуальні системи захисту

У сучасному цифровому середовищі безпека інформаційних систем є ключовим аспектом, що вимагає постійного вдосконалення і адаптації. Інтелектуальні системи захисту відіграють важливу роль у цьому контексті, адже вони використовують передові технології для автоматизації і покращення процесів безпеки. Основні компоненти цих систем, такі як штучний інтелект (ШІ) і машинне навчання (МН), аналіз поведінки та інтеграція з платформами управління безпекою (SIEM), допомагають забезпечити ефективний захист від складних і швидко еволюціонуючих кіберзагроз.

Штучний Інтелект (ШІ) і Машинне Навчання (МН)

Штучний інтелект (ШІ) і машинне навчання (МН) є центральними технологіями в інтелектуальних системах захисту. Вони забезпечують

можливість автоматичного виявлення і реагування на кіберзагрози, що перевищують можливості традиційних систем.

Штучний Інтелект (ШІ): ШІ використовує алгоритми і моделі для автоматичного аналізу та інтерпретації даних, що дозволяє системам виявляти загрози, базуючись на патернах і аномаліях, які можуть бути неочевидні для людини. Наприклад, ШІ може використовувати алгоритми для аналізу трафіку мережі і виявлення незвичайної активності, яка може вказувати на можливий атака.

Машинне Навчання (МН): Машинне навчання є підмножиною ШІ, що дозволяє системам автоматично вдосконалювати свої алгоритми на основі досвіду і даних. Зокрема, методи машинного навчання, такі як кластеризація і моделювання, можуть використовуватися для виявлення нових типів атак, які ще не були зафіксовані в базах даних відомих загроз. Наприклад, система може вчитися на історичних даних про атаки для виявлення нових схем або методів, які зловмисники можуть використовувати.

Приклад: В системах виявлення вторгнень, таких як Darktrace, використовується машинне навчання для створення "естандартних профілів" поведінки мережі. Це дозволяє виявити аномалії, такі як незвичайний трафік або невідомі команди, які можуть свідчити про атаку.

Аналіз Поведінки (Behavioral Analysis)

Аналіз поведінки є критичним компонентом інтелектуальних систем захисту. Він включає моніторинг і аналіз дій користувачів та системи для виявлення аномалій, що можуть свідчити про кіберзагрози.

Моніторинг Поведінки Користувачів: Аналіз поведінки користувачів дозволяє виявляти відхилення від нормальної діяльності. Це може включати виявлення несанкціонованого доступу до системи, нехарактерні дії, які відбуваються у не звичний час, або великі обсяги даних, що передаються.

Моніторинг Системи: Аналіз поведінки системи може виявити аномалії у функціонуванні системи або мережі, такі як нехарактерні запити або спроби доступу до захищених ресурсів. Наприклад, збільшення частоти

запитів до певних частин системи може свідчити про можливу спробу атаки типу "відмова в обслуговуванні" (DoS).

Приклад:

Системи, такі як Vectra AI, використовують аналіз поведінки для виявлення аномалій у трафіку мережі і поведінці користувачів. Якщо система виявляє, що користувач, який зазвичай працює з документацією, раптом починає здійснювати великі обсяги запитів до бази даних, це може сигналізувати про можливу спробу витоку даних.

Інтеграція з Платформами Управління Безпекою (SIEM)

Системи управління інформацією та подіями безпеки (SIEM) забезпечують централізоване управління і аналіз подій безпеки. Інтеграція з SIEM є важливою складовою частиною інтелектуальних систем захисту.

Централізований Моніторинг: SIEM платформи збирають і аналізують дані з різних джерел, таких як мережеві пристрої, сервери, додатки і бази даних. Це дозволяє отримати комплексну картину безпеки і виявити потенційні загрози на основі зведених даних.

Аналіз і Кореляція Подій: SIEM системи виконують кореляцію подій, щоб ідентифікувати складні загрози, що можуть включати кілька етапів або елементів системи. Наприклад, SIEM система може зв'язувати різні події, такі як невдалі спроби входу, зміни конфігурації і спроби доступу до чутливих даних, щоб виявити комплексні атаки, такі як внутрішні загрози або цілеспрямовані атаки.

Реакція на Інциденти*:* SIEM платформи також допомагають в автоматизації реагування на інциденти. Наприклад, якщо система виявляє аномальну поведінку, вона може автоматично відправити сповіщення адміністраторам або навіть виконати певні автоматичні дії, такі як блокування підозрілого IP-адресу.

Приклад:

Splunk Enterprise Security є прикладом платформи SIEM, яка інтегрує дані з різних джерел і використовує алгоритми для аналізу і кореляції подій.

Це дозволяє адміністраторам оперативно реагувати на потенційні загрози і забезпечити комплексний моніторинг безпеки.

Переваги Інтелектуальних Систем Захисту

Інтелектуальні системи захисту пропонують ряд переваг, які роблять їх важливими інструментами для забезпечення безпеки.

Автоматизація Процесів: Використання ШІ і МН дозволяє автоматизувати процеси виявлення загроз і реагування, що зменшує навантаження на людські ресурси і підвищує швидкість реагування.

Поліпшене Виявлення Загроз: Технології аналізу поведінки і машинного навчання дозволяють виявляти складні і нові типи загроз, які можуть бути не помічені традиційними системами.

Централізоване Управління: Платформи SIEM забезпечують централізовану точку для моніторингу і управління безпекою, що дозволяє отримати повну картину безпеки організації і швидко реагувати на інциденти.

Приклад:

Darktrace використовує алгоритми машинного навчання для аналізу мережевого трафіку і виявлення аномалій. Це дозволяє організаціям швидко реагувати на потенційні загрози, що можуть бути не помічені іншими системами.

Виклики і Обмеження

Попри численні переваги, інтелектуальні системи захисту стикаються з певними викликами.

Фальшиві Позитиви: ШІ та алгоритми машинного навчання можуть іноді видавати фальшиві позитиви, що може призвести до зайвого навантаження на адміністрацію і помилкових тривог.

Складність Інтеграції: Інтеграція нових систем з існуючими інфраструктурами може бути складною і вимагати значних зусиль і ресурсів.

Потреба в Навчанні: Системи, що використовують ШІ і машинне навчання, потребують регулярного навчання і налаштування для адаптації до нових типів загроз і змін у системі.

Приклад:

Інтеграція платформи Splunk з існуючими системами може вимагати складного налаштування і адаптації.

Системи виявлення і запобігання вторгненням (IDS/IPS) є критично важливими компонентами сучасної кібербезпеки. Вони постійно моніторять мережі та системи для виявлення і запобігання потенційним атакам. IDS (Intrusion Detection System) і IPS (Intrusion Prevention System) виконують важливі функції в захисті інформаційних систем, і кожна з них має свої особливості та переваги.

Системи виявлення вторгнень (ids)

Системи виявлення вторгнень (IDS) мають за мету виявляти аномалії та потенційні загрози в інформаційних системах і мережах. Основні функції IDS включають моніторинг трафіку, аналіз подій і генерування тривог.

IDS системи постійно моніторять мережевий трафік і перевіряють дані на предмет відомих загроз або аномалій. Це дозволяє виявити підозрілі дії, такі як несанкціоновані запити або спроби доступу до захищених ресурсів.

IDS системи також аналізують події з різних джерел, таких як журнали доступу, системні журнали та інформація про безпеку. Вони можуть виявити аномалії, такі як несподівані зміни в конфігурації системи або підозрілі спроби доступу.

Після виявлення потенційної загрози IDS система генерує сигнали тривоги або сповіщення, які надсилаються адміністраторам безпеки. Це дозволяє фахівцям швидко реагувати на можливі інциденти безпеки.

Приклад:

Snort є популярною системою IDS з відкритим кодом, яка здійснює моніторинг мережевого трафіку і генерує сигнали тривоги у випадку виявлення відомих загроз або аномалій. Snort використовує правила для перевірки трафіку і порівняння його з базами даних загроз.

Системи Запобігання Вторгненням (IPS)

Системи запобігання вторгненням (IPS) є розширенням IDS, яке не тільки виявляє загрози, але й активно запобігає їм. IPS системи можуть автоматично блокувати загрози в режимі реального часу, що дозволяє зменшити ризики безпеки і забезпечити більш активний захист.

На відміну від IDS, який лише генерує сигнали тривоги, IPS системи можуть автоматично вжити заходів для блокування загроз. Це може включати блокування IP-адрес, обмеження трафіку або заборону певних дій на системі.

IPS системи використовують ті ж методи аналізу, що і IDS, але з додатковими можливостями для реагування на загрози. Вони аналізують мережевий трафік і події в режимі реального часу для виявлення та блокування загроз до того, як вони завдадуть шкоди.

Оскільки IPS системи автоматично блокують загрози, вони повинні бути налаштовані таким чином, щоб зменшити кількість ложних тривог і забезпечити точність виявлення. Це може вимагати регулярного налаштування та оновлення системи.

Приклад:

Suricata є системою IPS з відкритим кодом, яка забезпечує як виявлення загроз, так і їх автоматичне блокування. Suricata аналізує мережевий трафік і використовує правила для ідентифікації та запобігання потенційним атакам.

Порівняння IDS і IPS

IDS і IPS мають різні функції і можуть бути використані разом для досягнення більшого рівня захисту.

IDS: Основна роль IDS полягає у виявленні загроз і генерації тривог. IDS забезпечує пасивний захист, сповіщаючи адміністратора про можливі проблеми, але не вживає заходів для їх запобігання.

IPS: IPS надає активний захист, блокуючи загрози в режимі реального часу. Це допомагає зменшити ризики безпеки, але може також створювати більше навантаження на систему через автоматичні заходи реагування.

Приклад:

Організації можуть використовувати комбінацію IDS і IPS для забезпечення комплексного захисту. IDS може бути налаштований для виявлення загроз і сповіщення адміністратора, тоді як IPS автоматично блокує загрози і запобігає їх негативному впливу.

Інтеграція IDS/IPS в Інфраструктуру Безпеки

Для досягнення максимального рівня безпеки важливо інтегрувати IDS/IPS системи в загальну інфраструктуру безпеки організації.

Інтеграція IDS/IPS з платформами SIEM дозволяє отримати централізоване управління і моніторинг подій безпеки. Це забезпечує більш ефективний аналіз і реагування на інциденти.

IDS/IPS системи повинні регулярно оновлюватися для забезпечення актуальності правил і бази даних загроз. Це допомагає зберігати їх ефективність у виявленні нових і еволюційних загроз.

Для забезпечення точності виявлення і запобігання загрозам важливо правильно налаштувати IDS/IPS системи і регулярно перевіряти їх ефективність.

Приклад:

Впровадження Cisco Firepower, інтегрованого рішення IDS/IPS, може забезпечити централізоване управління безпекою і зменшити ризики завдяки ефективному виявленню та запобіганню загроз. Cisco Firepower надає функції моніторингу, аналітики і автоматичного реагування на інциденти безпеки.

3.2 Фізичний захист: охоронні системи, контроль доступу, виділення "червоної" зони, тренування персоналу, аналіз та удосконалення дій підрозділів.

Шляхи удосконалення фізичного захисту об'єктів критичної інфраструктури

Фізичний захист об'єктів критичної інфраструктури є надзвичайно важливим для забезпечення надійності та безпеки систем, що мають ключове значення для функціонування держави та суспільства. Під об'єктами критичної інфраструктури розуміють такі важливі елементи, як енергетичні станції, водопостачальні системи, транспортні мережі, медичні заклади, а також інформаційні та комунікаційні системи, безперебійна робота яких є життєво необхідною для суспільства.

Удосконалення фізичного захисту цих об'єктів включає ряд заходів, спрямованих на покращення охоронних систем, контролю доступу, виділення "червоної" зони, тренування персоналу, а також аналіз та удосконалення дій підрозділів охорони. Це дозволяє мінімізувати ризики, пов'язані з несанкціонованим доступом, вандалізмом, терористичними атаками та іншими загрозами, що можуть вплинути на функціонування критично важливих об'єктів.

Сучасні охоронні системи забезпечують високий рівень захисту об'єктів критичної інфраструктури завдяки використанню передових технологій, таких як системи відеоспостереження з високою роздільною здатністю, інтелектуальні датчики та системи сигналізації. Інтеграція цих систем у єдину платформу дозволяє оперативно реагувати на інциденти та координувати дії служб безпеки, що значно підвищує ефективність захисту.

Ефективний контроль доступу є невід'ємною складовою фізичного захисту об'єктів критичної інфраструктури. Впровадження багатофакторної аутентифікації, використання автоматизованих систем контролю доступу (ACS) та регулярний перегляд політик доступу допомагають забезпечити, щоб

тільки уповноважені особи мали доступ до критичних зон. Це знижує ризик несанкціонованого доступу та потенційних загроз.

Виділення "червоної" зони є ще одним важливим заходом, що сприяє підвищенню рівня захисту об'єктів критичної інфраструктури. "Червона" зона – це обмежена область з підвищеним рівнем безпеки, до якої мають доступ лише спеціально уповноважені особи. Забезпечення фізичних бар'єрів, посилене відеоспостереження та додаткові засоби контролю доступу допомагають знизити ризики, пов'язані з несанкціонованим доступом до критичних ділянок об'єкта.

Регулярне навчання та тренування військовослужбовців є ключовими для забезпечення ефективного фізичного захисту об'єктів критичної інфраструктури. Навчання допомагає підвищити обізнаність щодо потенційних загроз та правильних дій у разі виникнення інцидентів. Проведення симуляційних вправ дозволяє відпрацювати дії персоналу у реальних умовах та забезпечити готовність до швидкого та ефективного реагування на загрози.

Регулярний аналіз інцидентів, проведення аудитів безпеки та впровадження нових технологій є важливими для постійного удосконалення фізичного захисту об'єктів критичної інфраструктури. Моніторинг та аналіз інцидентів дозволяють виявляти слабкі місця у системі захисту та розробляти заходи щодо їх усунення. Регулярні аудити допомагають оцінити ефективність існуючих заходів та виявити можливості для їх покращення.

Таким чином, удосконалення фізичного захисту об'єктів критичної інфраструктури є комплексним процесом, що включає застосування сучасних технологій, регулярне навчання персоналу, моніторинг та аналіз інцидентів. Впровадження цих заходів дозволяє забезпечити надійний захист від фізичних загроз і зберегти функціональність критично важливих систем.

Охоронні системи

Сучасні технології, такі як системи відеоспостереження з високою роздільною здатністю, інтелектуальні датчики та системи сигналізації, значно

підвищують ефективність охоронних систем. Наприклад, використання камер з функцією розпізнавання облич дозволяє ідентифікувати підозрілих осіб у реальному часі. Інтелектуальні датчики можуть виявляти не тільки рух, але й інші параметри, такі як температура, дим або звук, що дозволяє реагувати на різні типи загроз.

Системи відеоспостереження з високою роздільною здатністю

Відеоспостереження є одним з основних засобів охорони та моніторингу. Сучасні камери з високою роздільною здатністю (HD, Full HD, 4K) забезпечують чітке та детальне зображення, що дозволяє краще ідентифікувати підозрілих осіб та події. Наприклад, камери з функцією розпізнавання облич можуть автоматично ідентифікувати особу, порівнюючи зображення з базою даних. Це особливо корисно для виявлення небезпечних або підозрілих осіб у реальному часі.

Інтелектуальні датчики

Інтелектуальні датчики є ще одним важливим елементом сучасних охоронних систем. Вони можуть виявляти не лише рух, але й інші параметри, такі як температура, дим, звук, вібрація тощо. Це дозволяє оперативно реагувати на різні типи загроз та інцидентів.

Системи сигналізації

Системи сигналізації є невід'ємною частиною охоронних систем. Вони сповіщають про можливі загрози та забезпечують оперативне реагування на інциденти. Сучасні системи сигналізації можуть бути інтегровані з відеоспостереженням та інтелектуальними датчиками, що підвищує їх ефективність.

Впровадження комплексних систем безпеки

Сучасні технології дозволяють створювати комплексні системи безпеки, які інтегрують різні засоби захисту в єдину платформу. Це забезпечує більш ефективне управління охоронними заходами та дозволяє швидко реагувати на інциденти.

Приклад: В одному з енергетичних підприємств було впроваджено комплексну систему безпеки, яка включає відеоспостереження, інтелектуальні датчики та сигналізацію. Система автоматично аналізує дані з різних джерел та сповіщає про можливі загрози. Під час одного з інцидентів система виявила підозрілу активність біля одного з критичних об'єктів. Завдяки оперативному сповіщенню, служба безпеки змогла запобігти можливій диверсії.

Переваги сучасних охоронних систем

1. *Чіткість та детальність зображення:* Висока роздільна здатність камер дозволяє краще ідентифікувати підозрілих осіб та події.
2. *Автоматизація процесів:* Інтелектуальні датчики та системи сигналізації автоматично виявляють загрози та сповіщають про них.
3. *Оперативне реагування:* Завдяки інтеграції різних систем, служби безпеки можуть швидко реагувати на інциденти.
4. *Запобігання загрозам:* Сучасні технології дозволяють виявляти загрози на ранніх стадіях та запобігати їх розвитку.

Підтримка та оновлення

Регулярне технічне обслуговування та оновлення охоронних систем є важливими для забезпечення їх надійної роботи. Важливо вчасно проводити заміну застарілого обладнання, оновлювати програмне забезпечення та проводити технічний огляд систем для виявлення можливих несправностей.

Регулярне технічне обслуговування

Постійне технічне обслуговування охоронних систем допомагає запобігти несправностям і забезпечити їх стабільну роботу. Це включає перевірку стану обладнання, проведення необхідних ремонтних робіт та профілактику.

Приклад: В одному з об’єктів встановлена система відеоспостереження, яка забезпечує безпеку приміщення. Регулярне технічне обслуговування включає перевірку стану камер, заміну пошкоджених кабелів, очищення об'єктивів та налаштування обладнання. Завдяки цим заходам, є

можливість запобігти спробам несанкціонованого проникнення, оскільки система завжди працювала безперебійно.

Оновлення програмного забезпечення

Оновлення програмного забезпечення охоронних систем є важливим для захисту від нових загроз та підвищення функціональних можливостей системи. Оновлення можуть включати виправлення помилок, додавання нових функцій та підвищення рівня безпеки.

Приклад: Один з об'єктів використовує програмне забезпечення для розпізнавання облич у системі відеоспостереження. Регулярне оновлення цього програмного забезпечення дозволяє додавати нові алгоритми розпізнавання, які покращують точність ідентифікації осіб. Це допомогло аеропорту виявити та затримати кількох злочинців, які намагалися використовувати підроблені документи для подорожей.

Заміна застарілого обладнання

Застаріле обладнання може стати вразливим місцем у системі безпеки, оскільки воно може не відповідати сучасним вимогам і стандартам. Заміна старого обладнання на нове дозволяє забезпечити вищий рівень захисту та підвищити ефективність охоронних систем.

Приклад: На одній з електростанцій використовувались старі аналогові камери відеоспостереження, які мали низьку роздільну здатність і часто виходили з ладу. Керівництво прийняло рішення замінити їх на нові цифрові камери з високою роздільною здатністю та можливістю передачі даних через мережу. Це значно покращило якість відеозапису та дозволило оперативніше реагувати на можливі загрози.

Проведення технічного огляду

Технічний огляд охоронних систем допомагає виявити можливі несправності та усунути їх до того, як вони стануть серйозною проблемою. Огляд включає перевірку всіх компонентів системи, тестування їхньої роботи та виявлення потенційних проблем.

Контроль доступу

Впровадження багатофакторної аутентифікації (MFA) підвищує рівень безпеки доступу до об'єктів критичної інфраструктури. Наприклад, окрім традиційного пароля, можуть використовуватися біометричні дані (відбитки пальців, розпізнавання облич), смарт-карти або одноразові коди, що надсилаються на мобільний телефон користувача.

Використання багатофакторної аутентифікації

Впровадження багатофакторної аутентифікації (MFA) є одним із найефективніших методів підвищення рівня безпеки доступу до об'єктів критичної інфраструктури. MFA вимагає від користувача підтвердження своєї особи за допомогою декількох різних факторів, що значно ускладнює завдання для потенційних зловмисників. У сучасному світі, де кіберзагрози стають все більш витонченими, використання MFA стає критично важливим для захисту важливих даних та систем.

Основна ідея MFA полягає в тому, щоб об'єднати кілька рівнів аутентифікації, кожен з яких сам по собі підвищує рівень безпеки. Наприклад, навіть якщо пароль користувача буде скомпрометовано, додатковий фактор аутентифікації, наприклад, одноразовий код або біометричні дані, може запобігти несанкціонованому доступу. Цей багатошаровий підхід значно знижує ризик успішної атаки на систему.

Основні компоненти MFA

Пароль або PIN-код: Це традиційний метод аутентифікації, який включає введення пароля або PIN-коду. Цей метод є найпоширенішим, але не завжди достатньо безпечним сам по собі, оскільки паролі можуть бути вкрадені або зламані. Тим не менш, він є важливим першим кроком в MFA.

Смарт-карта або мобільний телефон: Це додатковий рівень безпеки, який передбачає використання фізичного пристрою, такого як смарт-карта або мобільний телефон, для отримання одноразових кодів. Наприклад, після введення пароля користувач отримує код на свій мобільний телефон, який він повинен ввести для підтвердження своєї особи. Це значно підвищує безпеку,

оскільки зловмисник повинен мати фізичний доступ до пристрою користувача.

Біометричні дані: Цей рівень аутентифікації використовує біометричні дані, такі як відбитки пальців, розпізнавання облич або сканування райдужної оболонки ока. Біометричні дані є унікальними для кожної людини, що робить їх дуже надійним засобом аутентифікації. Наприклад, для доступу до системи користувач повинен не тільки ввести пароль, але й пройти сканування відбитка пальця або розпізнавання обличчя.

Автоматизація процесів контролю доступу

Використання автоматизованих систем контролю доступу (ACS) дозволяє ефективно управляти доступом до різних зон об'єкта. Такі системи можуть автоматично реєструвати всі дії користувачів, створювати звіти та надавати інформацію про підозрілу активність.

Автоматизація процесів контролю доступу (Access Control Systems, ACS) є важливим компонентом сучасної безпеки об'єктів критичної інфраструктури. Використання ACS дозволяє ефективно управляти доступом до різних зон об'єкта, забезпечуючи високий рівень безпеки, зручність та оперативність. Автоматизовані системи контролю доступу можуть реєструвати всі дії користувачів, створювати звіти та надавати інформацію про підозрілу активність, що значно підвищує рівень безпеки та дозволяє оперативно реагувати на потенційні загрози.

Основні компоненти ACS

Ідентифікація користувачів: Однією з ключових функцій ACS є ідентифікація користувачів, яка може здійснюватися за допомогою різних методів, таких як магнітні картки, безконтактні RFID-картки, біометричні дані (відбитки пальців, розпізнавання облич) та інші. Ці методи забезпечують точну ідентифікацію осіб, які отримують доступ до об'єкта або окремих зон.

Контроль доступу: ACS дозволяє визначати права доступу для кожного користувача залежно від його ролі, часу дня, місця та інших параметрів. Наприклад, співробітники можуть мати доступ до певних зон

тільки у робочий час, тоді як адміністративний персонал може мати розширені права доступу.

Моніторинг та реєстрація подій: Системи контролю доступу автоматично реєструють всі дії користувачів, такі як входи і виходи, спроби доступу до заборонених зон, тощо. Ці дані зберігаються в системі та можуть бути використані для створення звітів і аналізу подій. Моніторинг у реальному часі дозволяє оперативно виявляти і реагувати на підозрілі або несанкціоновані дії.

Переваги автоматизованих систем контролю доступу

Підвищення рівня безпеки: Використання ACS значно підвищує рівень безпеки на об'єкті. Система забезпечує точну ідентифікацію користувачів і контроль доступу до різних зон, що знижує ризик несанкціонованого проникнення. Крім того, автоматизовані системи дозволяють швидко виявляти та реагувати на підозрілу активність.

Зручність управління доступом: ACS забезпечують зручне і гнучке управління доступом. Адміністратори можуть легко змінювати права доступу для окремих користувачів або груп користувачів залежно від їх ролі, зміни робочих графіків або інших параметрів. Це дозволяє швидко адаптувати систему до змін у структурі організації або потребах безпеки.

Автоматизація процесів: Автоматизовані системи контролю доступу знижують потребу у ручному управлінні і контролі, що дозволяє зменшити витрати на персонал і підвищити ефективність роботи. Системи автоматично реєструють всі події, створюють звіти та надають інформацію для аналізу, що полегшує роботу адміністративного персоналу.

Приклади використання ACS

Виробничі підприємства: На виробничих підприємствах ACS можуть використовуватися для контролю доступу до небезпечних або спеціалізованих зон, таких як лабораторії, склади з небезпечними матеріалами або виробничі лінії. Це дозволяє забезпечити безпеку персоналу і захистити обладнання та матеріали від несанкціонованого доступу.

Державні установи: У державних установах автоматизовані системи контролю доступу забезпечують високий рівень безпеки і контроль доступу до конфіденційної інформації. Наприклад, співробітники можуть отримувати доступ до приміщень тільки за допомогою біометричних даних або смарт-карток, що забезпечує високий рівень ідентифікації і захисту.

Виділення "червоної" зони

Визначення чітких меж "червоної" зони є ключовим етапом у забезпеченні її ефективного захисту. Це допомагає чітко відокремити зону з підвищеним рівнем безпеки від інших частин об'єкта, забезпечуючи тим самим контрольований доступ і запобігаючи несанкціонованому проникненню.

Фізичне відокремлення: Один з основних способів визначення меж "червоної" зони – це фізичне відокремлення за допомогою стін, бар'єрів або перегородок. Це може включати:

- *Стіни і перегородки:* Високі стіни або перегородки, виготовлені з міцних матеріалів, таких як бетон або сталь, які створюють фізичну перешкоду для несанкціонованого доступу. Наприклад, в дата-центрах часто використовуються металеві перегородки для створення окремих секцій, що захищають критично важливе обладнання.
- *Бар'єри і огорожі:* На території великих промислових об'єктів, таких як електростанції чи нафтопереробні заводи, можуть бути встановлені огорожі з колючого дроту або спеціальні бар'єри, що запобігають несанкціонованому доступу до "червоної" зони.

Приклад: На заводі з виробництва хімічних речовин, "червона" зона може бути обмежена металевою огорожею з бар'єрами, що містять вбудовані датчики руху. Ці бар'єри не лише фізично відокремлюють зону, але й сигналізують про будь-які спроби перетнути межу.

Маркування "червоної" зони

Маркування "червоної" зони є важливою складовою частиною забезпечення безпеки, оскільки воно інформує про підвищений рівень захисту і необхідність спеціального доступу. Важливо використовувати чіткі та

помітні знаки для того, щоб відвідувачі і працівники могли легко ідентифікувати цю зону.

Видимі знаки і сигнали: Для маркування "червоної" зони можуть бути використані:

- *Червоні лінії і знаки:* Використання червоних ліній, знаків або символів, які позначають межі зони. Такі знаки можуть включати в себе надписи типу "Доступ тільки для авторизованих осіб" або "Заборонено входити". Червоний колір часто асоціюється з забороною та небезпекою, тому він ефективно привертає увагу.
- *Освітлення і сигнали:* Спеціальне освітлення або сигнали, такі як миготливі лампи або LED-панелі, можуть бути встановлені навколо "червоної" зони для підвищення видимості, особливо в умовах низької освітленості. Це допомагає вказати на зону, де встановлені підвищені вимоги до доступу.

Приклад: На промисловому об'єкті, що займається зберіганням небезпечних матеріалів, навколо "червоної" зони можуть бути встановлені червоні стійки з знаками, що містять піктограми небезпеки і надписи. Освітлення навколо зони може бути обладнане червоними LED-лампами, які активуються у разі активації сигналізації.

Віртуальне маркування: Віртуальна модель або карта об'єкта може бути корисною для зображення і маркування "червоної" зони. На цифрових картах можуть використовуватися кольорові схеми для чіткого позначення різних зон безпеки.

Приклад: У системі управління безпекою для великого підприємства може бути створена інтерактивна карта, на якій "червона" зона виділена червоним кольором. Ця карта може бути доступна для служби безпеки і адміністраторів, що дозволяє їм оперативно орієнтуватися у випадку виникнення надзвичайних ситуацій.

Тренування військовослужбовців

Регулярні навчання та тренування є критично важливими для підтримання високого рівня готовності військовослужбовців до реагування на інциденти. Вони дозволяють не лише підтримувати фізичну форму, але й забезпечувати актуальність знань і навичок у сфері безпеки.

Проведення тренувань з евакуації: Один з основних типів навчання – це тренування з евакуації у разі пожежі або інших надзвичайних ситуацій. Такі тренування можуть включати:

- *Евакуаційні вправи:* Періодичне проведення вправ з евакуації для військовослужбовців, де вони повинні швидко і організовано покинути небезпечну зону. Це допомагає відпрацювати процедури і забезпечити, що всі знають, як діяти в критичних ситуаціях.
- *Реагування на спроби несанкціонованого доступу:* Тренування, які зосереджені на реагуванні на спроби несанкціонованого доступу, включають перевірку системи контролю доступу та дії у випадку виявлення підозрілих осіб. Військовослужбовці навчаються виявляти та реагувати на порушення доступу.

Приклад: На об'єкті критичної інфраструктури, наприклад, в електростанції, регулярно проводяться тренування з евакуації, де персонал навчається швидко і безпечно покидати зону в разі пожежі, використовуючи різні маршрути евакуації і перевіряючи їхню ефективність.

Ознайомлення з новими технологіями та загрозами

Ознайомлення з новими технологіями та загрозами є важливим для підтримання актуальності знань та навичок військовослужбовців. Це включає навчання з використання нових систем безпеки та нових видів загроз.

Навчання з нових систем контролю доступу: З розвитком технологій з’являються нові системи контролю доступу, такі як біометричні системи або інтелектуальні системи відеоспостереження. Військовослужбовці повинні бути ознайомлені з їх функціонуванням та методами ефективного використання.

Ознайомлення з новими загрозами: Нові типи атак або загроз можуть з'являтися регулярно, тому важливо, щоб персонал був обізнаний з останніми тенденціями у сфері кібербезпеки і фізичної безпеки. Це включає знання про нові методи проникнення або нові типи шкідливих програм.

Приклад: Військовослужбовці можуть проходити навчання з використання нових систем контролю доступу, таких як системи розпізнавання облич або нові технології відеоспостереження. Також проводяться семінари по новим загрозам, таким як вдосконалені техніки соціальної інженерії або нові типи кібератак.

Симуляційні вправи

Симуляційні вправи дозволяють військовослужбовцям відпрацювати свої дії у разі реальних інцидентів, що є важливим для ефективного реагування на надзвичайні ситуації.

Симуляції вторгнення: Проведення симуляцій, де персонал стикається з умовним вторгненням, допомагає відпрацювати дії у випадку реальної загрози. Це може включати:

- ***Вправи з реагування на вторгнення:*** Сценарії, де військовослужбовці повинні швидко реагувати на несанкціоноване проникнення в захищену зону. Це може включати захоплення підозрілих осіб, блокування входів та взаємодію з іншими службами безпеки.
- *Вправи з управління кризовими ситуаціями:* Сценарії, що включають кризові ситуації, такі як захоплення заручників або терористичні атаки. Персонал відпрацьовує координацію дій, комунікацію та впровадження планів реагування.

Приклад: У великому промисловому об'єкті проводяться регулярні симуляційні вправи, де військовослужбовці повинні діяти у випадку спроби проникнення або атаки. Це включає використання спеціальних тренувальних засобів і сценаріїв, що імітують реальні умови.

Аналіз та удосконалення дій підрозділів

Регулярний моніторинг та аналіз інцидентів є ключовими для виявлення слабких місць у системі фізичного захисту та розробки заходів для їх усунення.

Документування інцидентів: Важливо документувати всі інциденти безпеки, включаючи деталі про обставини та наслідки. Це допомагає аналізувати події та виявляти проблеми у системі захисту.

Проведення розслідувань: Розслідування інцидентів дозволяє визначити корінні причини порушень безпеки та розробити заходи для їх усунення. Це може включати аналіз помилок, перевірку дій персоналу та оцінку ефективності використовуваних систем.

Приклад: Після інциденту, де несанкціонована особа проникла в об'єкт, проводиться детальне розслідування, включаючи перегляд записів з відеокамер, аналіз журналів доступу та данні розповідей для виявлення причин порушення і розробки нових заходів безпеки.

3.3. Іноземний досвід забезпечення захисту критичної інфраструктури від воєнних загроз.

Забезпечення захисту критичної інфраструктури від воєнних загроз є надзвичайно важливим завданням для будь-якої держави. З огляду на зростаючу складність і масштабність сучасних загроз, країни по всьому світу постійно вдосконалюють свої стратегії і методи захисту. У цьому контексті вивчення іноземного досвіду є цінним для розробки ефективних механізмів захисту критичних об'єктів. Досвід інших країн може допомогти в адаптації стратегій та процедур, що сприятиме підвищенню рівня безпеки на національному рівні.

Військовий досвід США

Інтеграція технологій та інновацій

США є лідером у впровадженні передових технологій для захисту критичної інфраструктури. Це включає використання сучасних систем раннього попередження, інтелектуальних датчиків, автоматизованих систем управління та аналізу даних. Наприклад, *Система інтегрованого управління національною безпекою (NIMS)* дозволяє ефективно координувати відповіді на надзвичайні ситуації через централізовану платформу, яка обробляє інформацію з різних джерел і забезпечує інтегроване управління.

Приклад: Система охорони енергетичних мереж (CIP-14) включає в себе комплекс заходів, що охоплюють фізичну безпеку, кіберзахист та автоматизоване управління доступом для енергетичних об'єктів. CIP-14 зокрема забезпечує виявлення аномалій і можливих загроз в реальному часі, що дозволяє оперативно реагувати на потенційні атаки.

Співпраця між державними та приватними секторами

У США існує значна співпраця між державними установами і приватним сектором для забезпечення захисту критичної інфраструктури. *Національний центр кібербезпеки та інфраструктури (CISA)* забезпечує

платформу для обміну інформацією і координації дій між різними секторами економіки і державними органами.

Приклад: Програма обміну інформацією про загрози (ISACs) існують специфічні ISACs для різних галузей, таких як енергетика, фінансові послуги та охорона здоров'я, які надають учасникам доступ до даних про нові загрози та вразливості, а також рекомендації щодо захисту.

Регулярні навчання і тренування

США постійно проводить навчання і тренування для персоналу, що займається захистом критичної інфраструктури. *Національні навчальні програми, такі як Тренування з управління кризами (CMT)*, забезпечують відпрацювання дій у разі реальних загроз.

Приклад: Наприклад, у разі тренувань з кібербезпеки, фахівці з безпеки проходять сценарії, що імітують атаки на критичні системи, що дозволяє відпрацювати реагування на реальні кіберзагрози.

Європейський досвід

Розробка інтегрованих систем безпеки

У Європі країни активно впроваджують інтегровані системи безпеки для захисту критичної інфраструктури. *Європейська агенція з кібербезпеки (ENISA)* забезпечує підтримку і рекомендації для країн-членів у сфері кіберзахисту та фізичної безпеки.

Приклад: Програма "EU Cybersecurity Act" включає в себе створення Європейського органу з кібербезпеки, що надає країнам членам інструменти для покращення національної кібербезпеки, в тому числі рекомендації щодо захисту критичних інфраструктур.

Підвищення стандартів фізичної безпеки

У Європейських країнах особливу увагу приділяють фізичній безпеці критичної інфраструктури. *Стандарти фізичної безпеки (ISO 27001)* допомагають в розробці і впровадженні стандартів для захисту критичних об'єктів від фізичних загроз.

Співпраця на міжнародному рівні

Європейські країни активно співпрацюють у рамках міжнародних організацій і угод для підвищення рівня безпеки критичної інфраструктури.

Приклад: Програма "Horizon Europe": Фінансує проекти, що спрямовані на покращення безпеки критичної інфраструктури, включаючи дослідження і розробку нових технологій для захисту від воєнних загроз.

Азійський досвід

Країни Азії активно впроваджують новітні технології для контролю і моніторингу критичної інфраструктури. Китай і Японія використовують системи штучного інтелекту і великі дані для виявлення і реагування на загрози.

Приклад: Китайська система "Skynet" використовує велику мережу камер відеоспостереження і штучний інтелект для моніторингу громадських місць і критичних об'єктів, забезпечуючи високий рівень захисту.

Інтеграція кібер- і фізичного захисту

В Азії активно інтегрують кібер- і фізичний захист для забезпечення комплексного підходу до безпеки. Японія використовує передові рішення для захисту інфраструктури, зокрема для критичних об'єктів, таких як атомні електростанції.

Стратегії готовності до надзвичайних ситуацій

Азійські країни зосереджені на готовності до надзвичайних ситуацій, зокрема внаслідок природних катастроф або військових загроз.

Приклад: Сінгапурський Центр управління кризами забезпечує інтегровану платформу для реагування на надзвичайні ситуації, включаючи фізичні загрози і кіберзагрози, з використанням новітніх технологій для управління кризами.

3.4 Досвід підрозділів Національної гвардії України із захисту об’єктів критичної інфраструктури в умовах воєнного стану.

В умовах воєнного стану захист критичної інфраструктури стає надзвичайно важливим завданням для забезпечення національної безпеки і стабільності. Національна гвардія України, як один з основних складових частин системи національної безпеки, грає ключову роль у забезпеченні охорони критичних об'єктів. В умовах збройного конфлікту та підвищених загроз, підрозділи Національної гвардії виконують ряд важливих завдань, включаючи охорону стратегічних об'єктів, реагування на загрози і забезпечення стабільності.

Організація охорони об'єктів критичної інфраструктури

Визначення критичних об'єктів та встановлення захисних заходів

Захист критичної інфраструктури є життєво важливим для забезпечення стабільності та безпеки держави. Першим етапом у процесі охорони є точне визначення критичних об'єктів. Це можуть бути об'єкти, які виконують функції, критичні для національної безпеки, економічної стабільності, суспільного благополуччя та функціонування основних соціальних систем. Для ефективного визначення таких об'єктів проводять комплексний аналіз їхньої важливості, уразливості та потенційного впливу на національну безпеку у разі атаки або іншого виду шкоди.

Приклад: Охорона енергетичних об'єктів у Києві

Під час військового конфлікту в Україні, Національна гвардія взяла на себе охорону стратегічних об'єктів енергетичної інфраструктури в Києві. Включення підстанцій і електростанцій до переліку критичних об'єктів дозволило своєчасно забезпечити їхню охорону. Це було обумовлено тим, що збої в електропостачанні можуть мати серйозні наслідки для життєдіяльності міста, зокрема для медичних установ, систем водопостачання та транспортної інфраструктури.

Для цього були розроблені конкретні заходи захисту, такі як встановлення фізичних бар'єрів, організація постійного патрулювання та моніторинг ситуації. Вибір таких об'єктів для охорони був обґрунтований їхньою критично важливою роллю в підтримці життєзабезпечення міста.

Встановлення захисних заходів

Після визначення критичних об'єктів, важливо встановити відповідні заходи захисту, які можуть включати фізичні бар'єри, системи контролю доступу, моніторинг і оперативну підтримку.

Приклад:

На великих транспортних вузлах, таких як залізничні станції та аеропорти, проводиться комплексне впровадження захисних заходів. Це може включати:

1. *Фізичні бар'єри:* Встановлення спеціальних огорож, блокпостів і контрольно-пропускних пунктів для обмеження доступу до чутливих зон.
2. *Системи контролю доступу:* Використання електронних систем контролю доступу, які включають картки з RFID-технологією, біометричні зчитувачі та багатофакторну аутентифікацію для перевірки особи.
3. ***Моніторинг:*** Установка камер відеоспостереження, які постійно відстежують ситуацію на території об'єкта, а також інтеграція з системами раннього попередження, такими як детектори руху і сигналізації.

Приклад:

На об'єктах водопостачання були застосовані спеціальні заходи для захисту критичних інфраструктурних елементів, таких як водонасосні станції і резервуари. Це включало:

1. *Встановлення охоронних постів:* Охоронці, які постійно перебувають на території та контролюють доступ.

2. *Захист території:* Застосування захисних огорож, включаючи колючий дріт та електричні огорожі, для забезпечення фізичного бар'єру.

Реагування на загрози та підтримка стабільності

Ситуаційний моніторинг та раннє попередження

В умовах воєнного стану ефективний ситуаційний моніторинг та раннє попередження є критично важливими для забезпечення безпеки об'єктів критичної інфраструктури. Це дозволяє виявляти потенційні загрози на ранніх стадіях і оперативно реагувати на них, що може запобігти серйозним інцидентам.

Ситуаційний моніторинг включає використання різноманітних технологій і систем для відстеження і аналізу ситуації на об'єкті та в його околицях. Важливими компонентами такої системи є відеоспостереження, безпілотні літальні апарати (БПЛА), датчики та аналітичні системи.

Відеоспостереження

Системи відеоспостереження забезпечують цілодобовий моніторинг території та об'єктів. Сучасні камери відеоспостереження можуть бути оснащені високою роздільною здатністю, функціями нічного бачення і можливістю розпізнавання облич. Це дозволяє оперативно виявляти та документувати будь-які підозрілі дії.

Приклад:

На критичних об'єктах, таких як електростанції чи транспортні вузли, встановлюються високоякісні камери відеоспостереження, які дозволяють здійснювати цілодобовий моніторинг. У випадку виявлення підозрілої активності, система автоматично генерує тривожний сигнал, а оператори можуть швидко реагувати на інцидент.

Безпілотні літальні апарати (БПЛА)

БПЛА використовуються для патрулювання великих територій і виконання моніторингу з висоти. Вони дозволяють здійснювати огляд території, який важко забезпечити з допомогою стаціонарних камер або

людських патрулів. БПЛА оснащені камерами, тепловізорами і іншими сенсорами, що дозволяють виявляти підозрілі об'єкти та ситуації.

Приклад: На прикладі об'єктів, таких як стратегічні військові бази або важливі промислові комплекси, БПЛА можуть бути використані для проведення регулярних патрулів і моніторингу периметра. Це дозволяє оперативно виявляти несанкціоновані вхідні спроби або підозрілу активність, яку неможливо виявити за допомогою стаціонарних систем.

Раннє попередження

Системи раннього попередження забезпечують оперативну і точну інформацію про потенційні загрози, що дозволяє вжити необхідні заходи до того, як загроза стане критичною. Це включає інтеграцію даних з різних джерел, аналіз інформації та прийняття рішень для забезпечення безпеки.

Системи раннього попередження часто використовують аналітичні інструменти для обробки і аналізу зібраних даних. Це може включати алгоритми машинного навчання, які здатні виявляти аномалії та загрози на основі історичних даних і поточних спостережень.

Приклад: Використання аналітичних інструментів на критичних об'єктах, таких як аеропорти, дозволяє прогнозувати можливі загрози на основі аналізу патернів поведінки та історичних даних. Наприклад, алгоритми можуть виявити аномалії в звичній активності і попереджати про можливі терористичні атаки або інші загрози.

Швидке реагування

Ефективний ранній попереджувальний механізм також передбачає наявність чітких процедур для швидкого реагування на виявлені загрози. Це включає не лише технічні заходи, але і організаційні процеси, які дозволяють оперативно реагувати на будь-які загрози.

Приклад: при виявленні підозрілої активності система моніторингу автоматично сповіщає оперативний центр. Водночас активується план реагування, що включає залучення служб безпеки, перекриття потенційно небезпечних зон і проведення перевірок.

Регулярні тренування і симуляції для відпрацювання дій у надзвичайних ситуаціях

Регулярні тренування і симуляції є критично важливими для підрозділів, що відповідають за охорону критичної інфраструктури. Вони дозволяють відпрацювати дії в умовах надзвичайних ситуацій, що може значно підвищити готовність та ефективність реагування на реальні загрози. Такі тренування забезпечують знання і навички, необхідні для оперативного і скоординованого реагування на різні сценарії, такі як терористичні атаки, саботаж або інші критичні ситуації.

Основні типи тренувань

1. ***Навчання з евакуації персоналу***

Головною метою навчання з евакуації є забезпечення безпечного і організованого виходу з небезпечної зони у випадку надзвичайної ситуації. Це включає як фізичні заходи евакуації, так і координацію між різними службами.

Приклад: Виробничий комплекс, що займається виготовленням хімічних речовин, проводить регулярні тренування з евакуації персоналу у випадку витоку небезпечних хімікатів. Працівники навчаються швидко і безпечно покидати будівлю через визначені евакуаційні маршрути, а також отримують інструкції по використанню засобів індивідуального захисту.

2. ***Протидія атакам***

Тренування на протидію атакам зосереджені на відпрацюванні дій у разі фізичних атак, таких як проникнення зловмисників або терористичні акти. Це включає в себе не тільки фізичну протидію, але і застосування технічних засобів безпеки.

Приклад: У разі підозри на терористичні атаки, службовці охорони важливих державних об'єктів проводять тренування, які включають відпрацювання захисту від вторгнення. Симуляції можуть включати сценарії проникнення на територію, перевірку відповідних систем безпеки, таких як системи відеоспостереження та сигналізації, а також реакцію на різні види загроз.

3. ***Реакція на критичні ситуації***

Ці тренування фокусуються на оперативному реагуванні в умовах, коли вже сталися надзвичайні ситуації. Це включає координацію між різними службами, управління ресурсами та прийняття рішень в умовах стресу.

Приклад: В умовах збройного конфлікту, підрозділи охорони стратегічних об'єктів можуть відпрацьовувати сценарії, де на об'єкт здійснено напад. Тренування включають координацію з медичними службами, забезпечення допомоги постраждалим, організацію оборонних позицій та управління евакуацією.

Реальні приклади тренувань

Приклад 1: Навчання з евакуації під час терористичних атак

На прикладі комунального підприємства, що постачає воду для великого міста, проводяться регулярні тренування з евакуації у разі терористичного нападу. Під час одного з тренувань було імітовано вибух в одному з резервуарів для води. Персонал підприємства практикує швидке покидання території, включаючи використання тривожних сигналів і сповіщення через внутрішню радіомережу. Тренування включає також координацію з місцевими службами швидкого реагування для забезпечення безпеки і швидкого відновлення нормальної роботи.

Приклад 2: Симуляції протидії саботажу на промисловому об'єкті

На великому виробничому підприємстві, що виробляє критично важливі компоненти для оборонної промисловості, проводяться симуляції, де відпрацьовуються сценарії саботажу. Одним з таких тренувань було створення імітованої ситуації, де зловмисники намагаються проникнути на територію для підриву важливого обладнання. Персонал охорони, включаючи фізичні охоронці та технічні служби, тренується в оперативному затриманні зловмисників, перевірці і блокуванні доступу, а також в управлінні потенційними наслідками атаки.

Приклад 3: Тренування з реагування на загрози на критичних об'єктах

Під час навчань на стратегічних об'єктах, таких як атомні електростанції, персонал відпрацьовує сценарії, де стається аварія з викидом радіоактивних матеріалів. Тренування включають організацію термінової евакуації, захист від радіації і взаємодію з відповідними службами. Це дозволяє забезпечити своєчасне і ефективне реагування, що допомагає зменшити потенційний вплив на безпеку працівників і навколишнього середовища.

Інтеграція з іншими структурами та міжнародний досвід

Співпраця з правоохоронними органами та місцевою адміністрацією:

Національна гвардія активно співпрацює з іншими правоохоронними органами та місцевими адміністраціями для забезпечення комплексного захисту критичної інфраструктури. Це включає обмін інформацією, координацію дій та спільні навчання.

У разі підвищеної загрози, наприклад, при отриманні інформації про можливі терористичні атаки, Національна гвардія спільно з поліцією організовує посилені патрулі і контрольні пункти. Це включає перевірку транспортних засобів, людей та підозрілих об'єктів. На прикладі спільної операції під час великих державних свят, такі заходи дозволяють забезпечити додатковий рівень безпеки і запобігти можливим інцидентам.

Спільні навчання з цивільним захистом :

Національна гвардія регулярно проводить спільні тренування з місцевими службами цивільного захисту. Це включає симуляції різних надзвичайних ситуацій, таких як природні катастрофи, техногенні аварії та терористичні атаки. Наприклад, у рамках навчання з реагування на техногенні катастрофи, підрозділи Національної гвардії разом з місцевими службами цивільного захисту відпрацьовують сценарії ліквідації наслідків аварії на хімічному заводі, включаючи евакуацію населення і медичну допомогу постраждалим.

Обмін інформацією про потенційні загрози:

Під час обміну інформацією про потенційні загрози між Національною гвардією та поліцією, створюються спільні інформаційні платформи для відстеження і моніторингу ситуації. Це може включати використання спеціалізованих баз даних, платформ для обміну розвідданими та регулярні наради для обговорення оперативної інформації. Наприклад, в умовах зростання терористичної загрози, спільні інформаційні платформи дозволяють своєчасно реагувати на нові дані і планувати відповідні заходи безпеки.

Інтеграція з міжнародними організаціями:

Національна гвардія активно співпрацює з міжнародними організаціями, такими як Європейський Союз і НАТО, для підвищення рівня безпеки критичної інфраструктури. Це включає обмін передовим досвідом, навчання за міжнародними програмами та участь у спільних навчаннях. Наприклад, у рамках програми НАТО з управління кризовими ситуаціями, Національна гвардія бере участь у міжнародних навчаннях, що дозволяє відпрацьовувати дії у випадках масштабних кризових ситуацій і отримувати досвід від партнерів.

Спільні операції з іноземними військовими та безпековими службами:

Під час виконання міжнародних операцій з підтримання миру або в рамках міжнародних антитерористичних коаліцій, Національна гвардія взаємодіє з іноземними військовими та безпековими службами. Наприклад, у рамках місій ООН або спільних антитерористичних операцій, спільна робота з міжнародними партнерами дозволяє забезпечити високий рівень безпеки і стабільності в зонах конфлікту.

Висновоки

Магістерська робота на тему «Захист об’єктів критичної інфраструктури, як складова забезпечення національної безпеки» присвячена аналізу ключових аспектів захисту критичних об'єктів та їхньому значенню для забезпечення національної безпеки. Відзначено важливість комплексного підходу до охорони об'єктів, які є критичними для стабільності та функціонування держави.

Критична інфраструктура складає основу для функціонування суспільства і економіки. Це енергетичні системи, транспортні вузли, водопостачання, комунікаційні мережі та інші стратегічно важливі об'єкти. Їхнє функціонування є життєво важливим для підтримання соціальної стабільності та економічного розвитку. Тому забезпечення їхнього захисту є основною складовою частиною національної безпеки.

1. Проналізувавши концепції критичної інфраструктури та її роль у забезпеченні національної безпеки, що захист критичних об'єктів стикається з численними проблемами. Це включає фізичні та кіберзагрози, можливі терористичні атаки, саботаж і природні катастрофи. Ефективний захист критичної інфраструктури вимагає постійного вдосконалення стратегій і технологій, а також інтеграції з іншими структурами.

2. Вивчивши типи об'єктів критичної інфраструктури та їх важливості для стабільного функціонування суспільства впровадження сучасних технологій, таких як системи відеоспостереження з високою роздільною здатністю, інтелектуальні датчики та системи сигналізації, значно підвищує ефективність охорони. Наприклад, використання камер з функцією розпізнавання облич дозволяє ідентифікувати підозрілих осіб у реальному часі, а інтелектуальні датчики можуть виявляти аномалії та різні параметри, що сигналізують про загрози.

3. Дослідивши потенційні загрози, що можуть вплинути на об'єкти критичної інфраструктури, включаючи кібератаки, терористичні акти, природні катастрофи тощобуло виявленно що регулярне технічне обслуговування і оновлення охоронних систем є критично важливим для підтримання їхньої надійності. Важливо вчасно проводити заміну застарілого обладнання, оновлювати програмне забезпечення та проводити технічний огляд систем для виявлення можливих несправностей. Це дозволяє забезпечити стабільність і ефективність систем захисту.

4. Розглянувши технічні засоби захисту, таких як системи кібербезпеки, інтелектуальні системи захисту, системи фізичного захисту тощо.Впровадження багатофакторної аутентифікації (MFA) підвищує рівень безпеки доступу до об'єктів критичної інфраструктури. Використання різних факторів аутентифікації, таких як біометричні дані, смарт-карти або одноразові коди, дозволяє значно знизити ризик несанкціонованого доступу та підвищити загальний рівень захисту.

Використання автоматизованих систем контролю доступу (ACS) дозволяє ефективно управляти доступом до різних зон об'єкта. Такі системи автоматично реєструють дії користувачів, створюють звіти і надають інформацію про підозрілу активність. Це дозволяє забезпечити більш високий рівень безпеки та оперативно реагувати на загрози.

5. Розглянувши стратегічні аспекти захисту критичної інфраструктури на національному та міжнародному рівнях, включаючи міжнародне співробітництво та обмін найкращими практиками. Регулярний перегляд та оновлення політик доступу дозволяє адаптувати їх до змін у організаційній структурі та нових загроз. Забезпечення того, щоб доступ до критичних зон мали тільки уповноважені особи, є важливим елементом в підтримці безпеки об'єктів критичної інфраструктури.

Виділення "червоної" зони, що включає чітке визначення меж, маркування та підвищений рівень контролю доступу, дозволяє забезпечити захист найважливіших ділянок. Встановлення фізичних бар'єрів,

використання сучасних методів аутентифікації та постійний моніторинг допомагають знизити ризик несанкціонованого доступу і реагувати на потенційні загрози.

6. Проаналізувавши організаційні аспекти захисту критичної інфраструктури, таких як розробка політик безпеки, навчання персоналу, планування кризових ситуацій тощо.Проведення регулярних тренувань та симуляцій для військовослужбовців і служб безпеки є необхідним для підготовки до надзвичайних ситуацій. Вони включають навчання з евакуації, протидії атакам та іншим критичним ситуаціям. Наприклад, симуляції терористичних атак дозволяють оперативно реалізувати плани евакуації та забезпечити безпеку цивільного населення.

Співпраця з правоохоронними органами, місцевими адміністраціями та міжнародними партнерами є важливою складовою частиною ефективного захисту критичної інфраструктури. Обмін інформацією, спільні навчання та міжнародний досвід дозволяють покращити стратегії і тактики захисту, підвищити рівень безпеки та забезпечити комплексний підхід до охорони.

Захист об'єктів критичної інфраструктури є комплексним і багатогранним процесом, що включає використання сучасних технологій, постійне удосконалення стратегій і тактик, а також інтеграцію з іншими структурами. Національна безпека залежить від здатності держави ефективно захищати стратегічно важливі об'єкти від різноманітних загроз, будь то фізичні атаки, кіберзагрози або природні катастрофи.

Застосування передових технологій, регулярне навчання персоналу, постійний моніторинг та аналіз інцидентів є основою для забезпечення надійного захисту критичної інфраструктури. Співпраця на всіх рівнях – від місцевих правоохоронних органів до міжнародних партнерів – дозволяє створити інтегровану і ефективну систему безпеки, яка відповідає сучасним викликам і загрозам.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Указ Президента України Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про Стратегію національної безпеки України". [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/287/2015/paran7#n7

2. ЗАКОН УКРАЇНИ, Про критичну інфраструктуру (Відомості Верховної Ради (ВВР), 2023, № 5, ст.13)

3. Зелена книга з питань захисту критичної інфраструктури в Україні : зб. мат-лів міжнар. експерт. нарад / упоряд. Д. С. Бірюков, С.І. Кондратов; за заг. ред. О. М. Суходолі. – К. : НІСД, 2015. – 176 с

4. ЗАКОН УКРАЇНИ «Про критичну інфраструктуру» (Відомості Верховної Ради (ВВР), 2023, № 5, ст.13 Розділ III КРИТИЧНА ІНФРАСТРУКТУРА УКРАЇНИ https://zakon.rada.gov.ua/laws/show/1882-20#Text

5. Зелена книга з питань захисту критичної інфраструктури в Україні : зб. матеріалів міжнар. експерт. нарад / Упоряд. Д.С. Бірюков, С.І Кондратов ; за заг. ред. О.М.Суходолі. – К. : НІСД, 2016. – 176 с.

6. Указ Президента України від 15.03.2016 р. № 96/2016 Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України" http://zakon2.rada.gov.ua/laws/show/96/2016

7. Указ Президента України №189/2014 від 02.03.2014р. «Про рішення Ради національної безпеки і оборони України від 1 березня 2014 року «Про невідкладні заходи щодо забезпечення національної безпеки, суверенітету і територіальної цілісності України» http://zakon2.rada.gov.ua/laws/show/189/2014

8. Указ Президента України від 15.03.2016 р. № 96/2016 Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України" http://zakon2.rada.gov.ua/laws/show/96/2016

9. 1GREEN PAPER ON A EUROPEAN PROGRAMME FOR CRITICAL INFRASTRUCTURE PROTECTION, http://eur-lex.europa.eu/LexUriServ/site/en/com/2005/com2005_0576en01.pdf

10. Communication from the Commission of 12 December 2006 on a European Programme for Critical Infrastructure Protection, http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0786en01.pdf

11. A Communication on Protecting Europe's Critical Energy and Transport Infrastructure (цей документ містить чутливу інформацію, і тому не підлягає публікації)

12. COUNCIL DIRECTIVE 2008/114/EC of 8 December on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

13. Постанова Кабінету Міністрів України від 23.12.2004 № 1734 «Про затвердження переліку підприємств, які мають стратегічне значення для економіки та безпеки держави»

14. Постанова Кабінету Міністрів України від 28.07.2003 № 1170 «Про затвердження переліку особливо важливих об'єктів електроенергетики, які підлягають охороні відомчою воєнізованою охороною у взаємодії із спеціалізованими підрозділами інших центральних органів виконавчої влади»

15. Розпорядження Кабінету Міністрів України від 27.05.2009 № 578-р «Про затвердження переліку особливо важливих об'єктів нафтогазової галузі»

16. Постанова Кабінету Міністрів України № 1051 від 15.08.2007 (для службового користування)

17. Положення про єдину державну систему запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків (затверджене Постановою Кабінету Міністрів України № 1051 від 15.08.2007 р.)

18. Постанова Кабінету Міністрів України від 24.04.99 року №675-019 «Щодо затвердження Переліку об’єктів, які підлягають охороні і обороні в умовах надзвичайних ситуацій і в особливий період»

19. Постанова Кабінету Міністрів України від 10 серпня 1993 р. №615 «Про заходи щодо вдосконалення охорони об'єктів державної та інших форм власності» (із змінами)

20. Закон України від 18.01.2001 № 2245-III «Про об’єкти підвищеної небезпеки»

21. Перелік особливо небезпечних підприємств, припинення діяльності яких потребує проведення спеціальних заходів щодо запобігання заподіянню шкоди життю та здоров'ю громадян, майну, спорудам, навколишньому природному середовищу / Затв. Постановою Кабінету Міністрів України від 06.05.2000 №765

22. Постанова Кабінету Міністрів України від 29.08.2002 р. № 1288 «Про затвердження Положення про Державний реєстр потенційно небезпечних об'єктів»

23. Наказ Держатомрегулювання від 17.12.2012 № 238 «Про затвердження Переліку радіаційно небезпечних об’єктів в Україні, для яких розробляється об’єктова проектна загроза» 16 відповідно до порядку, затвердженого постановою Кабінету Міністрів України від 02.03.2010 № 227 дск (із змінами згідно постанови Кабінету Міністрів України від 24.07.2014 № 545 дск) 17 затверджених постановою Кабінету Міністрів України від 09.01.2014 № 6

24. Закон України від 13.03.2012 №4499-VI «Про систему екстреної допомоги населенню за єдиним телефонним номером 112»

25. Закон України від 10.01.2002 № 2919-III «Про Національну систему конфіденційного зв'язку» (із змінами)

26. Закон України від 05.04.2001 №2346-III «Про платіжні системи та переказ коштів в Україні»

27. Закон України від 08.06.2000 № 1805-III «Про охорону культурної спадщини»

28. Communication from the Commission to the Council and the European Parliament of 20 October 2004 – Critical infrastructure protection in the fight against terrorism (COM/2004/702 final). – [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/

29. Communication from the Commission on a European Programme for Critical Infrastructure Protection (COM/2006/786 final). – [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/

30. Green paper on a European programme for critical infrastructure protection (COM/2005/576 final). – [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/

31. Proposalfor a Directive of the Council on the identification and designation of European critical infrastructure and the assessment of the need to improve their protection (COM/2006/787 final). – [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/

32. Council Directive 2008/114/EC "On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection". – [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/

33. Commission staff working document – Accompanying document to the proposal for a Council decision on creating a Critical Infrastructure Warning Information Network (CIWIN) – Impact assessment (SEC/2008/2702). – [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/

34. Кодекс цивільного захисту України http://zakon1.rada.gov.ua/laws/show/5403-17/page4

35. Положення про функціональну підсистему єдиної державної системи запобігання і реагування на надзвичайні ситуації техногенного та природного характеру «Безпека об'єктів ядерної енергетики» http://www.snrc.gov.ua/nuclear/uk/publish/article/140508

36. Коваленко, С. (2019). Управління ризиками для критичної інфраструктури. Одеса: Видавництво "Одеський університет". ISBN 978-966-00-0003-1.

37. Левін, А., & Пател, М. (2018). Сучасні технології безпеки критичної інфраструктури. Львів: Видавництво "Львівська академія". ISBN 978-966-00-0004-8.

38. Мірошниченко, В. (2020). Захист критичної інфраструктури: теорія та практика. Київ: Видавництво "Наукова думка". ISBN 978-966-00-0005-5.

39. Національний інститут стандартів і технологій (NIST). (2020). Рамкова система для покращення кібербезпеки критичної інфраструктури. Вашингтон, D.C.: NIST. Доступно за посиланням: https://www.nist.gov/cyberframework

40. Міжнародна організація з стандартизації (ISO). (2018). ISO 27001:2018 Системи управління інформаційною безпекою. Женева: ISO. Доступно за посиланням: https://www.iso.org/standard/54534.html

41. Європейське агентство з кібербезпеки (ENISA). (2020). Ландшафт загроз для критичної інфраструктури. Брюссель: ENISA. Доступно за посиланням: https://www.enisa.europa.eu/publications/threat-landscape-for-critical-infrastructure

42. Петренко, О. (2021). Інтелектуальні системи безпеки для критичної інфраструктури. Харків: Видавництво "Фактор". ISBN 978-966-00-0006-2.

43. Сидоренко, І. (2021). Аналіз і управління загрозами для критичної інфраструктури. Київ: Видавництво "Науковий світ". ISBN 978-966-00-0007-9.

44. Міллер, Р., & Шульце, С. (2021). Захист критичної інфраструктури національної безпеки. Вашингтон, D.C.: Центр стратегічних і міжнародних досліджень (CSIS). Доступно за посиланням: https://www.csis.org/publications/securing-nations-critical-infrastructure

45. Бакланов, О. (2022). Системи відеоспостереження для критичної інфраструктури. Дніпро: Видавництво "Пріоритет". ISBN 978-966-00-0008-6.

46. Андрієнко, Ю. (2020). Технології безпеки критичної інфраструктури: сучасні підходи. Львів: Видавництво "Львівська академія". ISBN 978-966-00-0009-3.

47. Козлов, С. (2019). Безпека інформаційних систем і критичної інфраструктури. Київ: Видавництво "Наука і освіта". ISBN 978-966-00-0010-0.

48. Єрмолаєв, В. (2021). Кіберзагрози для критичної інфраструктури. Харків: Видавництво "Харківський університет". ISBN 978-966-00-0011-7.

49. Курков, А. (2019). Захист критичної інфраструктури: міжнародний досвід. Київ: Видавництво "Юридична практика". ISBN 978-966-00-0012-4.

50. Гончар, М. (2020). Реакція на інциденти безпеки критичної інфраструктури. Львів: Видавництво "Технології". ISBN 978-966-00-0013-1.

51. Кравченко, О. (2021). Системи контролю доступу для критичної інфраструктури. Одеса: Видавництво "Академія". ISBN 978-966-00-0014-8.

52. Смирнов, П. (2022). Захист критичної інфраструктури в умовах воєнного стану. Харків: Видавництво "Науковий світ". ISBN 978-966-00-0015-

53. Ващенко, Ю. (2020). Аудит безпеки критичної інфраструктури. Київ: Видавництво "Аудитор". ISBN 978-966-00-0016-2.

54. Бородін, О. (2021). Інтеграція систем безпеки для критичної інфраструктури. Львів: Видавництво "Безпека". ISBN 978-966-00-0017-9.

55. Давиденко, І. (2022). Використання нових технологій для захисту критичної інфраструктури. Київ: Видавництво "Інновації". ISBN 978-966-00-0018-6.