УДК 343.3
DOI https://doi.org/10.32782/2524-0374/2024-10/71

АКТУАЛЬНІ ПИТАННЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

CURRENT ISSUES OF ENSURING CYBER SECURITY OF CRITICAL INFRASTRUCTURE OBJECTS

Скіцько О.І., к.т.н., с.н.с.,
головний науковий співробітник
Національна академія Служби безпеки України

Ширшов Р.А., науковий співробітник
Національна академія Служби безпеки України

В статті розглянути сучасні виклики, пов'язані з кібербезпекою об'єктів критичної інфраструктури (далі – ОКІ) України в контексті агресивної кіберполітики російської федерації. Визначено, що кібербезпека є невід'ємною складовою національної безпеки, особливо в умовах ескалації гібридної війни та зростання кількості атак на державні інформаційні системи.

Ключовими елементами кіберзахисту зазначено підвищення технологічної стійкості інформаційних систем, впровадження оперативного моніторингу, координацію діяльності між державними структурами та приватними організаціями, а також застосування сучасних інструментів захисту, зокрема систем виявлення та запобігання вторгненням (IDS/IPS). Наголошено на важливості розробки інтегрованих механізмів реагування на кіберінциденти та створення національної платформи для обміну інформацією про кіберзагрози.

У статті акцентується увага на високу вразливість цифрової інфраструктури України перед державними та кримінальними кіберзловмисниками, особливо в енергетичному та фінансовому секторах. Підкреслено, що подібні атаки часто спрямовані на підрив стабільності державних інститутів і критично важливих економічних галузей, що може мати наслідки для національної безпеки. Обґрунтовано необхідність удосконалення правового регулювання кібербезпеки, зокрема щодо запровадження нових стандартів і норм, а також посилення координації між державними органами та приватним сектором для зміцнення захисту національної критичної інфраструктури.

Підкреслено важливість розробки національної стратегії кіберстійкості, яка включає співпрацю з міжнародними партнерами, обмін найкращими практиками та інтеграцію зусиль у сфері кіберзахисту. Висвітлено значення новітніх технологій, зокрема штучного інтелекту та машинного навчання, у виявленні та нейтралізації загроз. Наголошено на необхідності постійного підвищення кваліфікації фахівців з кібербезпеки, зокрема шляхом участі у міжнародних навчальних програмах і практичних тренінгах, для ефективного реагування на нові виклики.

Ключові слова: кібербезпека, критична інфраструктура, кібератаки, інформаційні системи, гібридна агресія, кіберзлочинність, штучний інтелект, кібертероризм, соціальна інженерія, моніторинг, кіберстійкість.

The article examines the contemporary challenges related to the cybersecurity of Ukraine's critical infrastructure (CI) in the context of the aggressive cyber policy of the Russian Federation. It is determined that cybersecurity is an integral part of national security, especially in the conditions of escalating hybrid warfare and the growing number of attacks on state information systems.

Key elements of cyber defense are identified as increasing the technological resilience of information systems, implementing operational monitoring, coordinating activities between state structures and private organizations, as well as utilizing modern protection tools, including intrusion detection and prevention systems . The importance of developing integrated mechanisms for responding to cyber incidents and creating a national platform for sharing information about cyber threats is emphasized.

The article highlights the high vulnerability of Ukraine's digital infrastructure to state and criminal cyber actors, particularly in the energy and financial sectors. It is noted that such attacks are often aimed at undermining the stability of state institutions and critically important economic sectors, which can have far-reaching consequences for national security. The necessity of improving legal regulation of cybersecurity is substantiated, including the introduction of new standards and norms, as well as strengthening coordination between state bodies and the private sector to enhance the protection of national critical infrastructure.

The importance of developing a national cyber resilience strategy is emphasized, which includes cooperation with international partners, sharing best practices, and integrating efforts in the field of cyber defense. The significance of new technologies, particularly artificial intelligence and machine learning, in detecting and neutralizing threats is highlighted. The need for continuous professional development of cybersecurity specialists is stressed, particularly through participation in international training programs and practical exercises, for effective response to emerging challenges.

Key words: cybersecurity, critical infrastructure, cyberattacks, information systems, hybrid aggression, cybercrime, artificial intelligence, cyberterrorism, social engineering, monitoring, cyber resilience.

Протягом останніх років кіберпростір перетворився на середовище ведення наступальних дій за участю провідних держав світу для досягнення переваги у вирішенні комплексних проблем і воєнних конфліктів. В сучасних умовах кібернетичні операції є невід'ємною складовою російської гібридної агресії, спрямованої як на Україну, так і на країни Європейського Союзу, Сполучені Штати Америки, Канаду, Туреччину тощо.

Протягом останніх десяти років проти України було здійснено велику кількість атак на об'єкти критичної інфраструкттури шляхом кібер- та кіберфізичного впливу на їх інформаційні ресурси. Реалізація зазначеного впливу мала негативний ефект насамперед на сили безпеки та оборони України, підприємства енергетичного сектору, державні та недержавні фінансові установи, підприємства різних форм власності. У порівнянні з 2022 роком на сьогодні кількість кібератак на об'єкти критичної інфраструктури України та її партнерів збільшилася щонайменше вчетверо [1].

У 2023–2024 роках ситуація в країні значно ускладнилася: за даними звіту Оперативного центру реагування на кіберінциденти Державного центру кіберзахисту Держспецзв'язку, кількість зареєстрованих кіберінцидентів збільшилася на 62,5% у порівнянні з 2022 роком [2]. На даний момент фахівці Департаменту контррозвідувального захисту інтересів держави у сфері інформаційної безпеки СБУ щомісяця реєструють понад тисячу деструктивних інформаційних атак російського походження, спрямованих на український державний сектор та суспільство [3].

Основна мета цих атак – вплив на суспільно-політичну ситуацію в країні через створення умов для провокування деструктивних дій населення.

Рівень складності російських кібератак проти України зростає, що вказує на значну вразливість цифрових

та взаємопов'язаних систем перед злочинними діями. Зазначені атаки демонструють потенціал для серйозного втручання в роботу об'єктів критичної інфраструктури, що є невід'ємною частиною сучасного суспільства.

Зловмисники активно нарощують розвиток гібридної війни, метою якої є завдання шкоди енергетичній інфраструктурі, що підтверджує зростаюча важливість захисту таких систем.

Кіберфахівці отримали можливість вчитися та досліджувати досвід України. Такий досвід став джерелом цінної інформації про новітні методи захисту і реагування на кібератаки.

Водночас, викликає занепокоєння співпраця окремих держав із хакерськими угрупованнями для поширення шкідливого програмного забезпечення з метою зараження інформаційних мереж ОКІ.

Сучасні виклики технічного прогресу вимагають поглибленого розуміння загроз у кібер середовищі, а також чіткого усвідомлення того, яка саме інформація є основною ціллю кіберзлочинців. Це вимагає розробки ефективних заходів для забезпечення захисту даних та безпечного використання інформаційних ресурсів. Серед основних категорій кіберзагроз фахівці з кібербезпеки виділяють наступні [4]:

зовнішні загрози – включають DDoS та DoS атаки, а також використання зловмисниками зовнішніх вразливостей інформаційних систем підприємств. Такі загрози можуть бути спрямовані на порушення роботи сервісів і підрив функціональності критично важливих інфраструктурних об'єктів;

внутрішні загрози – охоплюють як системні, так і людські фактори. Серед них виділяються інсайдери, витік конфіденційної інформації та недотримання правил поводження з чутливими даними, що створює значні ризики для цілісності інформаційних активів;

цільові загрози – ключовою вразливою ланкою захисту залишається людський фактор, що піддається цільовому впливу з боку кіберзлочинців через методи соціальної інженерії. До найбільш поширених методів належать фішингові розсилки, що містять шкідливі файли або посилання. Такі атаки призводять до компрометації мереж організації шляхом впровадження вірусів, троянських програм, програм-шифрувальників і іншого шкідливого програмного забезпечення (ШПЗ).

Необхідність захисту об'єктів критичної інфраструктури у сучасних умовах обумовлена загрозами національній безпеці, визначених у Стратегії національної безпеки України [5] та Стратегії забезпечення державної безпеки [6].

Серед цих загроз можна виділити існуючу модель глобалізації, що сприяє поширенню міжнародного тероризму та виникненню нових схем його фінансування у кіберпросторі; продовження війни рф проти України з використанням систематичних кібератак і проведення спеціальних інформаційних операцій, зростання кіберзагроз для ОКІ, пов'язаних із втручанням у їх функціонування.

Перелік загроз національній безпеці розширюється та оновлюється відповідно до положень Стратегії кібербезпеки України [7]. Основні загрози включають гібридну агресію рф проти України у кіберпросторі, що відображається у систематичних кібератаках, спрямованих на інформаційні системи органів державної влади України та об'єкти критичної інфраструктури, з метою їх дестабілізації, отримання несанкціонованого доступу та встановлення контролю.

Також спостерігається використання кіберпростору для здійснення актів кібертероризму, фінансування та підтримки терористичної діяльності, що призводить до масштабних матеріальних та репутаційних втрат. Серед інших загроз – кіберзлочинність, що завдає шкоди інформаційним ресурсам, використання кіберпростору для скоєння злочинів, пов'язаних із незаконним поводженням із засобами ураження, викрадення закритої інформації для військових цілей. Крім того, значну загрозу становить розвідувально-підривна діяльність у кіберпросторі, що включає складні комплексні багатоланцюгові кібератаки, організовані державними акторами або спеціальними службами.

Стратегія воєнної безпеки України [8] визначила основні аспекти воєнної безпеки на глобальному рівні, зосереджуючись на підвищенні рівня невизначеності та непередбачуваності безпекового середовища, що характеризується зростанням конкуренції за ресурси та міждержавного суперництва із використанням політико-дипломатичних, економічних, інформаційних, воєнних і гібридних засобів. Крім того, спостерігається посилення конкуренції між державами у сфері інформаційних, кібернетичних та інших передових технологій, а також розробка на їх основі систем озброєнь (кіберфізичних систем), які використовують робототехніку та інноваційні матеріали.

У Концепції забезпечення національної системи стійкості [9] зазначається, що сучасні методи створення конфліктів і кризових ситуацій потребують глибокого розуміння їхньої природи на основі всебічного аналізу та оцінки ризиків для ключових сфер життєдіяльності суспільства і держави. Основними проблемами які необхідно вирішити на етапі впровадження національної системи стійкості, концепція визначає недостатній рівень розвитку системи забезпечення кібербезпеки, що унеможливлює гарантування кіберстійкості національних інформаційних ресурсів.

Технологічний рівень реалізації кіберзагроз постійно підвищується, водночас удосконалюються та розробляються нові технології, інструменти і механізми кібератак. Політично вмотивована діяльність у формі кібератак на державні та приватні інформаційні ресурси набуває дедалі більшого поширення у кіберпросторі. Використання кіберпростору для здійснення атак і ведення бойових дій набуває глобального характеру.

При оцінці рівня кіберзагроз для України слід враховувати: недосконаліть національної системи захисту критичної інфраструктури, відсутність єдиного державного органу, що здійснює координацію дій у цій сфері.

На стан безпеки об'єктів критичної інфраструктури (ОКІ) та їх інформаційних ресурсів також впливають наступні чинники: високий професійний потенціал вітчизняних програмістів; здатність молодих спеціалістів швидко освоювати сучасні технології; а також зростання економіки, що сприяє інтенсифікації процесів цифровізації країни [10].

Такий стан справ значно знижує ефективність виконання завдань безпеки, ускладнюючи забезпечення належного захисту критичної інформаційної інфраструктури [11], що, своєю чергою, підвищує рівень загроз національній безпеці України. Необхідно враховувати, що кібератаки активно застосовуються в сучасному кіберпросторі з протиправною метою не лише приватними особами, але й спецслужбами іноземних держав, а також підконтрольними їм групами та організаціями.

Таким чином, комплексний характер загроз національній безпеці, пов'язаних з кіберзлочинністю та кібертероризмом, вимагає визначення інноваційних підходів до розбудови системи кібербезпеки та кіберзахисту критичної інфраструктури, а також подальшого розвитку кіберпростору в умовах глобалізації та вільного обігу інформації.

Сучасні кіберзлочинці та кібертерористи здебільшого здійснюють асиметричні атаки, спрямовані на досягнення стратегічних цілей без застосування високотехнологічних засобів збройного характеру.

Технічний потенціал кіберзловмисників постійно зростає завдяки розширенню доступності новітніх інформаційних технологій, супутникових комунікацій, сучасних методів фальсифікації документів та інших ресурсів. Вони активно використовують ці технології для зміцнення

своєї присутності в кіберпросторі, де здійснюють поширення дезінформації, пропаганду, вербування нових членів і підтримання комунікації з осередками, зокрема через Darknet.

Ця діяльність охоплює надання інструкцій щодо підготовки та проведення диверсій, терористичних атак, а також інших протиправних дій у кіберпросторі, таких як кібератаки, викрадення даних тощо.

Постійно зростаюча залежність національної критичної інфраструктури від автоматизованих систем управління об'єктами критичної інфраструктури (ОКІ) є однією з ключових передумов для існування та подальшого розвитку кіберзлочинності та кібертероризму. Сучасні інформаційно-комунікаційні технології активно використовуються кіберзлочинцями для дестабілізації функціонування автоматизованих систем управління технологічними процесами на ОКІ, паралельно із застосуванням традиційних методів здійснення диверсій та терористичних актів.

Кібертероризм представляє найбільш значну загрозу для безпеки, створюючи численні кіберзагрози для об'єктів критичної інфраструктури.

На відміну від традиційних форм тероризму, кібертероризм характеризується використанням новітніх науково-технічних досягнень у галузі електронних комунікацій, комп'ютерних та інформаційних технологій.

Прояви кібертероризму можна класифікувати наступним чином: реалізація терористичних актів у кіберпросторі, де елементи кіберпростору виступають інструментом здійснення протиправних дій; використання компонентів кіберпростору як об'єктів злочинних посягань; застосування кіберпростору для досягнення проміжних або суміжних цілей терористів [12].

Основною формою кібертероризму є здійснення кібератак на інформацію, електронні обчислювальні системи, апаратуру передачі даних та інші компоненти інформаційної інфраструктури. Такі атаки можуть призводити до несанкціонованого проникнення в інформаційно-комунікаційну мережу або інфраструктуру, блокування засобів мережевого інформаційного обміну, перехоплення управління, а також інших дестабілізуючих дій [13].

Кібератаки за сприяння держав, спрямовані на викрадення інформації з обмеженим доступом, знищення чи дестабілізацію інформаційних ресурсів, важливих для інших країн, або блокування доступу до таких ресурсів з метою отримання політичних, економічних чи військових переваг, є однією з сучасних форм розвідувально-підривної діяльності в мирний час і перетворюються на форму бойових дій у воєнний час. Таким чином, будь-які кібератаки, здійснені державними організаціями, фактично є проявом кібервійни [14].

З метою підвищення ефективності протидії кібертероризму, Служба безпеки України (СБУ) створила платформу для обміну індикаторами загроз, відому як MISP-UA. Починаючи з 2023 року, інтеграція ІТ-компаній та операторів об'єктів критичної інформаційної інфраструктури (ОКІІ) у цю платформу суттєво підвищила рівень безпеки української критичної інфраструктури та державних інформаційних ресурсів у порівнянні з 2022 роком. Такий прогрес свідчить про успішне залучення сучасних технологій у зміцнення національної кібербезпеки, що забезпечує більш ефективну координацію зусиль у виявленні та нейтралізації загроз.

Фахівці з кібербезпеки СБУ забезпечили інтеграцію низки критично важливих об'єктів до Єдиної системи управління інформаційною безпекою "SIEM" (Security Information and Event Management), яка здійснює моніторинг подій у режимі реального часу та забезпечує можливість глибокого аналізу стану інформаційної безпеки [15]. Потенційно критичні події, ідентифіковані системою, підлягають аналізу кваліфікованими аналітиками, що дає змогу своєчасно виявляти, реагувати та запобігати загрозам.

СБУ, відповідно до визначених законодавством повноважень, здійснює запобігання, виявлення, припинення та розслідування злочинів проти миру і безпеки людства, що вчиняються у кіберпросторі. До її завдань належать також контррозвідувальні та оперативно-розшукові заходи з протидії кібердиверсіям, кібертероризму і кібершпигунству, а також перевірка готовності об'єктів критичної інфраструктури до можливих кібератак і кіберінцидентів. СБУ протидіє кіберзлочинності, наслідки якої можуть створити загрозу життєво важливим інтересам держави, розслідує кіберінциденти та кібератаки на об'єкти критичної інформаційної інфраструктури (ОКІІ) і державні електронні інформаційні ресурси, забезпечуючи реагування на кіберінциденти у сфері державної безпеки [16].

Особливу увагу слід приділити проблемним аспектам протидії загрозам інформаційної безпеки в інформаційно-комунікаційних системах та внутрішніх мережах об'єктів критичної інформаційної інфраструктури (ОКІІ). Сучасні кібератаки на ОКІІ здатні спричиняти системні кризи як на локальному, так і на регіональному та глобальному рівнях. Зловмисники, використовуючи новітні інформаційні технології, створюють передумови для виникнення масштабних аварій на виробничих підприємствах, блокування транспортної інфраструктури, дезорганізації державного управління, фінансової системи, а також дестабілізації роботи наукових і медичних установ. У контексті зростання інтеграції інформаційних технологій у системи державного управління та керування критичними інфраструктурними процесами, ці системи стають дедалі більш вразливими.

Таким чином, поширення кіберзагроз на усі сфери життєдіяльності, пов’язані з функціонуванням ОКІ, та вдосконалення інструментарію їх реалізації зумовлює необхідність зміни стратегії і тактики протидії в умовах триваючої гібридної війни рф проти України. Потребують перегляду засади забезпечення безпеки критичної інформаційної інфраструктури України, адже безпека та захищеність ОКІ визначена в Україні одним із базових елементів національної системи стійкості, стабільне функціонування яких необхідно забезпечувати, у т.ч: кібербезпека; захищеність та безперебійне функціонування інформаційних та комунікаційних послуг; безперебійне енерго-, водо-, теплопостачання, постачання продовольства; стійке функціонування транспортних систем.

Отже, кібербезпека критичної інфраструктури є одним із пріоритетів національної безпеки України, що вимагає адекватної протидії загрозам.

На стан захисту об'єктів критичної інформаційної інфраструктури (ОКІІ) в Україні впливають не лише відсутність надійної ізоляції між операційно-технологічними та корпоративними мережами, недостатнє тестування на проникнення та цілодобовий моніторинг, а й, як вже зазначалося, недоліки у сфері державно-приватного партнерства.

Поширення кіберзагроз на всі сфери життєдіяльності, пов'язані з функціонуванням об'єктів критичної інфраструктури (ОКІ), та вдосконалення методів їх реалізації обумовлює необхідність переосмислення стратегій та тактик протидії цим загрозам в умовах триваючої гібридної війни Російської Федерації проти України. Необхідно переглянути основні підходи до забезпечення безпеки критичної інформаційної інфраструктури, оскільки безпека та захищеність ОКІ визначені як один із базових елементів національної системи стійкості.

Отже, забезпечення кібербезпеки критичної інфраструктури є одним із ключових пріоритетів національної безпеки України, що вимагає адекватної, систематичної та ефективної протидії зростаючим кіберзагрозам.

Враховуючи сучасний стан захисту об'єктів критичної інфраструктури (ОКІ), існуючі загрози та виклики у протидії цим загрозам, для підвищення рівня безпеки критичної інформаційної інфраструктури на державному рівні

доцільно реалізувати такі заходи [17]: законодавчі – унормування поняття кібертероризму (комп'ютерного тероризму); організаційні – створення ефективної загальнонаціональної системи захисту критичної інформаційної інфраструктури України, координація та управління силами і засобами забезпечення її безпеки, включаючи створення національної системи управління кіберінцидентами; технічні – встановлення обов'язкових вимог (стандартів) інформаційної безпеки ОКІІ з урахуванням міжнародних стандартів та специфіки галузі, до якої належать такі об'єкти; впровадження нових алгоритмів підвищення рівня кіберстійкості комунікаційних та технологічних систем ОКІ; режимні, розвідувальні, контррозвідувальні та оперативно-розшукові заходи, спрямовані на зниження рівня вразливості ОКІІ до кіберзагроз воєнного, кримінального, терористичного та іншого характеру.

ЛІТЕРАТУРА

1. Від початку року російські хакери активізували атаки проти України – Юрій Мироненко. URL: https://cip.gov.ua/ua/news/vid-pochatku-roku-rosiiski-khakeri-aktivizuvali-ataki-proti-ukrayini-yurii-mironenko.

2. Кількість зареєстрованих в Україні кіберінцидентів у 2023 році зросла на 62,5% – Держспецзв'язку. URL: https://ms.detector.media/internet/post/33956/2024-01-12-kilkist-zareiestrovanykh-v-ukraini-kiberintsydentiv-u-2023-rotsi-zrosla-na-625-derzhspetszvyazku/.

3. Кіберфахівці СБУ щомісяця фіксують понад тисячу інформаційних атак на Україну. URL: https://ms.detector.media/kiberbezpeka/post/33614/2023-11-30-kiberfakhivtsi-sbu-shchomisyatsya-fiksuyut-ponad-tysyachu-informatsiynykh-atak-na-ukrainu/.

4. Як українському бізнесу захиститися від атак хакерів. URL: https://uaspectr.com/2022/07/27/yak-ukrayinskomu-biznesu-zahystytysya-vid-atak-hakeriv.

5. Указ Президента України від 14.09.2020 № 392/2020 «Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України». URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text.

6. Указ Президента України від 16.02.2022 № 56/2022 «Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про Стратегію забезпечення державної безпеки». URL: https://www.rnbo.gov.ua/ua/Ukazy/5264.html.

7. Указ Президента України від 26.08.2021 № 447/2021 «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України». URL: https://www.rnbo.gov.ua/ua/Ukazy/4974.html.

8. Указ Президента України від 25.03.2021 № 121/2021 «Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року «Про Стратегію воєнної безпеки України». URL: https://www.president.gov.ua/documents/1212021-37661.

9. Указ Президента України від 27.09.2021 № 479/2021 «Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року «Про запровадження національної системи стійкості». URL: https://www.president.gov.ua/documents/4792021-40181.

10. Мельник Д.С. Щодо актуальних потреб захисту національної критичної інформаційної інфраструктури України. Актуальні проблеми управління інформаційною безпекою держави: зб. тез наук. доп. наук.-практ. конф. Київ: НА СБУ, 2018. С. 114.

11. Критична інформаційна інфраструктура – сукупність об'єктів критичної інформаційної інфраструктури – комунікаційних або технологічних систем об'єктів критичної інфраструктури, кібератака на які безпосередньо вплине на їх стале функціонування (ч. 1 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України»).

12. Гнатюк С. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи. Ukrainian Scientific Journal of Information Security. Київ: № 2 (19), 2013. С. 118–129. с. 122.

13. Брижко В.М., Швець М.Я. Е-боротьба в інформаційних війнах та інформаційне право: монографія; за ред. члена-кореспондента АПрН України, д.е.н., професора М. Швеця. К.: НДЦПІ АПрН України, 2007. 236 с. с. 163.

14. Тропіна Т.Л. Кіберзлочинність та кібертероризм.: Збірник наукових статей / Під ред. Голубева В.А., Ахтирської Н.Н. Запоріжжя: Центр досліджень компьютерної злочинності, 2004. Вип. 1. С. 76–81. с. 78.

15. СБУ 2022 рік: захист держави в умовах війни. Інформаційна та кібербезпека. Сайт СБУ: головна сторінка. URL: https://ssu.gov.ua/.

16. Організаційно-правові основи забезпечення кібербезпеки: підручник / за заг. ред. М.М. Присяжнюка. Київ: Вид-во «Ліра-К», 2023. С. 265.

17. Мельник Д.С. Захист національної критичної інформаційної інфраструктури: актуальні проблеми та шляхи вирішення. Адміністративне право і процес: науково-практичний журнал. Київ, 2022, № 3 (38) / 2022, С. 5–16.