УДК 342.951

КРАСНІКОВ С.А., провідний науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0001-6548-5457

РОЗВИТОК НАЦІОНАЛЬНОЇ СИСТЕМИ КІБЕРБЕЗПЕКИ УКРАЇНИ

DOI: https://doi.org/10.37750/2616-6798.2025.4(55).346414

Анотація. *Стаття присвячена аналізу сучасного стану та перспектив розвитку національної системи кібербезпеки України в умовах стрімкого розвитку інформаційних технологій і зростання кіберзагроз. Розглянуто основні нормативно-правові акти, що регулюють сферу кібербезпеки. Проаналізовано ключові кібервиклики, пов'язані з мілітаризацією кіберпростору, розвитком кіберзброї та впливом глобальних технологічних трендів, таких як хмарні обчислення, штучний інтелект і 5G-мережі. Запропоновано напрями вдосконалення національної системи кібербезпеки, серед яких виділяються розвиток державно-приватного партнерства у сфері кібербезпеки, гармонізація вітчизняних інформаційних стандартів з міжнародними стандартами (ISO/IEC, NIST) та підвищення рівня кіберграмотності населення.*

Ключові слова: *кібербезпека, національна система кібербезпеки, кіберзагрози, інформаційна безпека, державна політика*.

Summary. *The article is devoted to the analysis of the current prospects for the development of the national cybersecurity system of Ukraine in the conditions of the rapid development of information technologies and the growth of cyber threats. The main regulatory and legal acts that regulate the field of cybersecurity are reviewed. Analyzed key cyber challenges associated with the militarization of cyberspace, the development of cybersecurity and the influx of global technological trends, such as cloud computing, artificial intelligence and 5G limits. It is directly supported by the development of a comprehensive national cybersecurity system, which includes the development of public-private partnerships in the field of cybersecurity, the harmonization of commercial information standards with international standards (ISO/IEC, NIST) and advancing the level of cyber literacy among the population.*

Keywords*: cybersecurity, national cybersecurity system, cyberthreats, information security, government policy.*

Постановка проблеми. Сучасний світ характеризується швидким розвитком інформаційно-комунікаційних технологій, які трансформують усі сфери суспільного життя. Водночас, для національної безпеки з'являються нові кіберзагрози, спричинені мілітаризацією кіберпростору, розвитком сучасної кіберзброї та широким використанням цифрових сервісів. Технологічний рівень реалізації кіберзагроз постійно підвищується, водночас удосконалюються та розробляються нові технології, інструменти і механізми кібератак [1].

Україна вже тривалий час є об'єктом кібератак з боку рф. Протягом останніх десяти років проти України було здійснено велику кількість атак на об'єкти критичної інфраструктури шляхом кібер- та кіберфізичного впливу на їх інформаційні ресурси [2, с.312].

У 2024 році кількість кібератак на Україну зросла на 69,8%, досягнувши 4315 інцидентів, у порівнянні з 2023 роком, коли було зафіксовано 2541 кіберінцидентів.

Наразі спостерігається стійка тенденція до зростання кібератак передусім на критично важливу інфраструктуру України [3]. Це зумовлює потребу удосконалення національної системи кіберзахисту критичної інфраструктури.

Забезпечення кібербезпеки залишається одним із пріоритетів у системі національної безпеки України, реалізація якого здійснюється шляхом посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам у сучасному безпековому середовищі. У Стратегії забезпечення кібербезпеки зазначається: "Швидко змінюваний цифровий світ потребує формування більш збалансованої та ефективної національної системи кібербезпеки, яка зможе гнучко адаптуватися до змін безпекового середовища, гарантуючи громадянам України безпечне функціонування національного сегмента кіберпростору, передбачивши нові можливості для цифровізації всіх сфер суспільного життя" [1]. Поширення кіберзагроз на всі сфери життєдіяльності, пов'язані з функціонуванням об'єктів критичної інфраструктури, та вдосконалення методів їх реалізації обумовлює необхідність переосмислення стратегій та тактик протидії цим загрозам в умовах триваючої гібридної війни російської федерації проти України [2, с.313].

Результати аналізу наукових публікацій.

Сучасний стан розвитку національної системи кібербезпеки (на прикладі СБ України та Держспецз'вязку України) досліджували А. Марущак і С. Петров [4]. Питання правового забезпечення національної системи кібербезпеки висвітлено у працях О. Алексеєвої [5], О. Скіцько, Р. Ширшова [2; 6] та ін. Ефективний механізм правового регулювання щодо протидії кіберзагрозам представлено Д. Дубовим [7], А. Печенюком [8]. Національну систему кібербезпеки як складову частину системи забезпечення національної безпеки України розглянуто В. Ліпканом[9], І. Діордіцею [10].

Водночас, аналіз сучасного розвитку національної системи кібербезпеки України в умовах воєнного стану та тривалої російсько-української кібервійни свідчить про потребу комплексного удосконалення цієї системи.

Метою статті є аналіз розвитку національної системи кібербезпеки України й обґрунтування рекомендацій з її удосконалення.

Виклад основного матеріалу.

Національна система кібербезпеки регулюється низкою нормативно-правових актів. Правову основу забезпечення кібербезпеки України становлять Конституція України, закони України щодо основ національної безпеки, засад внутрішньої і зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, цей та інші закони України, Конвенція про кіберзлочинність, інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, укази Президента України, акти Кабінету Міністрів України, а також інші нормативно-правові акти, що приймаються на виконання законів України (ст. 3 Закону України "Про основні засади забезпечення кібербезпеки України") [11].

За останні роки було докладено зусиль до становлення та розвитку національної системи кібербезпеки. Розглянемо найбільш важливі правові та організаційні компоненти цієї системи.

Основним правовим компонентом цієї системи є Закон України "Про основні засади забезпечення кібербезпеки України" (далі – Закон) від 05.10.2017 р. № 2163-VIII. Цей Закон визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних

інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки [11]. Попри деякі неоднозначні формулювання у тексті законодавчого акту і можливі питання з його практичним застосуванням, слід зазначити, що період формування національного законодавства у сфері кібербезпеки розпочатий, а основний акт спеціального законодавства, що започатковує відповідну систему законодавства, ухвалений [12, с. 99].

Ст. 8 цього Закону визначає зміст національної системи кібербезпеки як "сукупність суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури" [11]. Важливим компонентом цієї системи є система активної протидії агресії у кіберпросторі, під якою пропонується розуміти сукупність організаційних, правових, наукових та технічних заходів, спрямованих на підвищення рівня кіберзахисту держави шляхом здійснення впливу на інформаційні (автоматизовані), електронно-комунікаційні, інформаційно-комунікаційні системи держави-агресора, джерела походження кіберзагроз та кібератак (пункт 22 ст. 1 цього Закону) [11].

Відповідно до ч. 2 ст. 8 цього Закону основними суб'єктами національної системи кібербезпеки є Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи України, Національний банк України, Міністерство закордонних справ України [11]. Завдання з безпосередньої протидії кіберзагрозам покладені на Службу безпеки України, Державну службу спеціального зв'язку та захисту інформації України, CERT-UA та Міністерство оборони України. Ці органи та структури відповідно до своєї компетенції здійснюють, зокрема, заходи щодо: 1) запобігання використанню кіберпростору у воєнних, розвідувально-підривних, терористичних та інших протиправних цілях; 2) виявлення і реагування на кіберінциденти та кібератаки, усунення їх наслідків.

Координація діяльності у сфері кібербезпеки як складової національної безпеки України здійснюється Президентом України через очолювану ним Раду національної безпеки і оборони України (ч. 1 ст. 5 Закону). Загальну координацію функціонування суб'єктів національної системи реагування на кіберінциденти, кібератаки, кіберзагрози здійснює Національний координаційний центр кібербезпеки як робочий орган Ради національної безпеки і оборони України (п. 5 ч. 3 ст. 9 Закону) [11]. Не дивлячись на те, що Національний координаційний центр кібербезпеки грає ключову об'єднувальну та координаційну роль у цьому процесі[1], сьогодні залишається доволі низьким рівень координації та управління силами і засобами забезпечення її безпеки, включаючи створення національної системи управління кіберінцидентами [2, с.314-315].

Законодавство України передбачає чіткий механізм функціонування національної системи кібербезпеки, який забезпечується шляхом: 1) формування та оперативної адаптації державної політики у сфері кібербезпеки, кіберзахисту з урахуванням наявних або потенційних ризиків, впровадження кращих практик та досягнення сумісності з відповідними стандартами Європейського Союзу та НАТО; 2) запровадження нормативно-правового регулювання у сфері кібербезпеки, кіберзахисту з урахуванням ризик-орієнтованого підходу, чіткого розподілу ролей, завдань, функцій та

відповідальності публічного сектору, операторів критичної інфраструктури та власників або розпорядників об’єктів критичної інформаційної інфраструктури, а також галузевої специфіки, гармонізації практик та стандартів з Європейським Союзом та НАТО; 3) запровадження заходів стимулювання розвитку та конкурентоспроможності індустрії послуг та продуктів у сфері кібербезпеки в Україні; 4) залучення експертного потенціалу приватного сектору, наукових установ, професійних та громадських об’єднань до розроблення проектів щодо стратегічного планування, державної політики, проектів нормативно-правових актів, нормативних документів, стандартів та методичних рекомендацій у сфері кібербезпеки; 5) систематичного проведення навчань з питань кіберзахисту для осіб, які в межах своєї компетенції безпосередньо здійснюють заходи з кіберзахисту в органах державної влади, органах місцевого самоврядування, що є власниками або розпорядниками інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, об’єктів критичної інфраструктури, об’єктів критичної інформаційної інфраструктури; 6) функціонування системи оцінювання стану кіберзахисту в органах державної влади, державних органах, органах місцевого самоврядування, державних підприємствах, господарських товариствах; 7) розвитку мережі команд реагування на кіберінциденти, кіберзагрози на національному, галузевому та регіональному рівнях, у тому числі із залученням приватних команд реагування; 8) розвитку та вдосконалення системи технічного і криптографічного захисту інформації; 9) створення та забезпечення функціонування Національної електронної комунікаційної мережі; 10) функціонування національної системи реагування на кіберінциденти, кібератаки, кіберзагрози та національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози; 11) впровадження єдиної (універсальної) системи індикаторів кіберзагроз з урахуванням міжнародних стандартів з питань кібербезпеки та кіберзахисту; 12) впровадження організаційно-технічної моделі кіберзахисту національної системи кібербезпеки; 13) застосування інструментів та механізмів державно-приватної взаємодії для виконання завдань у сфері кібербезпеки, включаючи, але не обмежуючись, функціонування національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози, заходи кіберзахисту та захисту інформації; 14) запровадження загальної системи або індивідуальних програм моніторингу, аналізу, координації дій, у тому числі під час реагування на кіберінциденти; усунення наслідків, здійснення заходів з відновлення; 15) організації та здійснення заходів з підготовки кадрів, підвищення рівня знань і навичок, проведення навчань, розроблення та реалізації освітніх і просвітницьких програм; 16) здійснення досліджень та нових розробок; забезпечення функціонування центрів кібербезпеки та їхніх сервісів; 17) розроблення програмних документів та нормативно-правових актів у сфері кібербезпеки, а також для вирішення інших завдань у сфері кібербезпеки; 18) розвитку міжнародного співробітництва у сфері кібербезпеки, підтримки міжнародних ініціатив у сфері кібербезпеки; 19) здійснення оперативно-розшукових, розвідувальних, контррозвідувальних та інших заходів, спрямованих на запобігання, виявлення, припинення та розкриття кримінальних правопорушень проти миру і безпеки людства, які вчиняються з використанням кіберпростору, розслідування, переслідування, оперативного реагування та протидії кіберзлочинності, розвідувально-підривній, терористичній та іншій діяльності у кіберпросторі, що завдає шкоди інтересам України, використанню мережі Інтернет у воєнних цілях [11].

Важливим етапом інституалізації національної системи кібербезпеки стало затвердження Указом Президента України від 26.08.2021 р. №447 Стратегії кібербезпеки України, зміст якої враховує попередній досвід та інституціональні проблеми, стан кібербезпекового середовища на національному та міжнародному рівні.

Розділ 4 Стратегії забезпечення кібербезпеки, який має назву "Національна система кібербезпеки: засади розбудови", передбачає, що: "для подальшої розбудови національної системи кібербезпеки на засадах стримування, кіберстійкості, взаємодії необхідним є:

посилення спроможності національної системи кібербезпеки для унеможливлення збройної агресії проти України у кіберпросторі або з його використанням, нейтралізації розвідувально-підривної діяльності, мінімізації загроз кіберзлочинності та кібертероризму (стримування);

набуття здатності швидко адаптуватися до внутрішніх і зовнішніх загроз у кіберпросторі, підтримувати та відновлювати стале функціонування національної інформаційної інфраструктури, насамперед об'єктів критичної інформаційної інфраструктури (кіберстійкість);

забезпечення розвитку комунікації, координації та партнерства між суб'єктами забезпечення кібербезпеки на національному рівні, розвиток стратегічних відносин у сфері кібербезпеки із ключовими іноземними партнерами, передусім з Європейським Союзом, Сполученими Штатами Америки та іншими державами - членами НАТО, співробітництво у цій сфері з іншими державами та міжнародними організаціями на основі національних інтересів України (взаємодія)" [1].

У цій Стратегії проголошено засади розбудови національної системи кібербезпеки: "Україна розбудовуватиме національну систему кібербезпеки, ґрунтуючись на: всеохоплюючому розумінні та постійному аналізі глобальних трендів кібербезпекового середовища, неухильному захисті національних інтересів України у сфері кібербезпеки; перманентності заходів з перегляду та уточнення повноважень і відповідальності суб'єктів забезпечення кібербезпеки держави, удосконалення законодавства у сфері кібербезпеки та оперативності дій щодо його актуалізації відповідно до безпекових умов, що змінюються; пріоритетності економічного і соціального розвитку суспільства; збалансованому забезпеченні потреб держави і прав громадян, дотриманні законності, повазі до основоположних цінностей, прав людини і громадянина; чіткому визначенні ролей та механізмів взаємодії під час розв'язання завдань кібербезпеки, стимулюванні до обміну інформацією, знаннями і досвідом; ризик-орієнтованому підході до забезпечення кібербезпеки; співпраці та інклюзивному діалозі всіх суб'єктів забезпечення кібербезпеки, зміцненні довіри, зокрема в рамках державно-приватного партнерства; впровадженні сучасних принципів, методів, підходів та механізмів публічного управління у сфері кібербезпеки; збалансованому розподілі наявних матеріальних, фінансових та інших ресурсів; проактивному підході до нейтралізації кіберзагроз; забезпеченні демократичного цивільного контролю за функціонуванням національної системи кібербезпеки"[1].

Водночас, надзвичайно важливі для розвитку національної системи кібербезпеки завдання Стратегії кібербезпеки України не були виконані в повному обсязі, зокрема у частині: створення в системі Міноборони кібервійськ; запровадження ефективних механізмів взаємодії основних суб'єктів національної системи кібербезпеки та сил оборони в частині спільного виконання завдань кібероборони; забезпечення виконання плану кібероборони як складової частини плану оборони України; удосконалення системи розвідувального забезпечення кібербезпеки держави; розроблення дієвих

механізмів залучення фахівців приватного сектору з кібербезпеки до участі у стримуванні та протидії агресії проти України в кіберпросторі; застосовування всіх доступних інструментів дипломатії та міжнародного права для протидії зловмисній діяльності проти України в кіберпросторі; запровадження чіткої програми кібернавчання та розвиток цифрової грамотності.

Не зважаючи на те, що виконання цих заходів передбачено Планом заходів на 2025 рік з реалізації Стратегії кібербезпеки України, затвердженим розпорядженням Кабінету Міністрів України від 7 березня 2025 р. № 204-р [13], більша їх частина залишається не реалізованою.

Викладене свідчить про потребу оновлення Стратегії з урахуванням нових видів кіберзагроз. Про це також свідчить загострення протистояння у кіберпросторі, де триває кібервійна України з рф.

Серед ключових кібервикликів для національної системи кібербезпеки України слід виділити:

мілітаризацію кіберпростору, адже розвиток сучасної кіберзброї та її використання в гібридних війнах створює загрози для критичної інфраструктури, зокрема енергетичних, транспортних і фінансових систем;

технологічний прогрес – хмарні обчислення, 5G-мережі, Інтернет речей і штучний інтелект створюють нові вразливості, які потребують адаптації до національної системи кібербезпеки;

низький рівень цифрової грамотності громадян та культури безпекового поводження в кіберпросторі, що підвищує ризики фішингових атак і соціальної інженерії;

відсутність дієвої системи інформаційно-аналітичного забезпечення кібербезпеки;

недостатню координацію діяльності суб’єктів забезпечення кібербезпеки;

неналежну спільну роботу суб’єктів забезпечення кібербезпеки з приватним сектором та громадськістю, що ускладнює реагування на кіберзагрози;

загрози інформаційної безпеки в інформаційно-комунікаційних системах та внутрішніх мережах об'єктів критичної інформаційної інфраструктури.

Серед цих викликів можна виділити: існуючу модель глобалізації, що сприяє поширенню міжнародного тероризму та виникненню нових схем його фінансування у кіберпросторі[1]; продовження війни рф проти України з використанням систематичних кібератак і проведення спеціальних інформаційних операцій; зростання кіберзагроз для об’єктів критичної інфраструктури, пов’язаних із втручанням у їх функціонування[2, с. 113].

З метою належної протидії цим кібервикликам та підвищення ефективності національної системи кібербезпеки України вбачається доцільним:

- забезпечення розвитку державно-приватного партнерства, в першу чергу, шляхом активного залучення приватного сектору до розробки технологій кіберзахисту та обміну інформацією про кіберзагрози.

- підвищення кіберграмотності населення шляхом проведення освітніх кампаній для громадян, розроблення програм навчання фахівців у сфері кібербезпеки.

- забезпечення розвитку технологічної інфраструктури шляхом впровадження сучасних систем моніторингу, аналізу та реагування на кіберзагрози, зокрема з використанням штучного інтелекту;

- гармонізація вітчизняних інформаційних стандартів з міжнародними стандартами з питань кібербезпеки й кіберзахисту для забезпечення сумісності з системами ЄС і НАТО.

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 [2, с. 113].

Висновки. Національна система кібербезпеки – це сукупність взаємопов'язаних елементів (суб'єктів забезпечення кібербезпеки) та зв'язків між ними, які утворюють цілісний механізм виявлення, запобігання, нейтралізації та реагування на реальні і потенційні загрози національній безпеці України у кіберпросторі. Важливим компонентом цієї системи є активна протидія агресії у кіберпросторі.

Розвиток є критично важливим для забезпечення національної безпеки в умовах гібридних загроз і стрімкого технологічного прогресу. Сучасна правова база з питань забезпечення кібербезпеки створює належну основу для функціонування національної системи кібербезпеки, однак потребує вдосконалення шляхом оновлення Стратегії забезпечення кібербезпеки України. Формування нової якості національної системи кібербезпеки потребує чіткого та зрозумілого визначення стратегічних цілей, що мають бути досягнуті під час реалізації згаданої Стратегії. Серед таких цілей, в першу чергу, доцільно виділити: гармонізацію вітчизняних інформаційних стандартів з міжнародними стандартами у сфері кібербезпеки; посилення державно-приватного партнерства у цій сфері; підвищення кіберграмотності населення. Під час реалізації цих стратегічних цілей Україна, крім основних суб'єктів національної системи кібербезпеки, має залучити до вирішення завдань у сфері кібербезпеки більш широке коло учасників, у тому числі суб'єктів господарювання, громадські об'єднання та окремих громадян України.

Вкрай важливою для зміцнення національної системи кібербезпеки є: забезпечення Національним координаційним центром кібербезпеки скоординованої діяльності усіх заінтересованих сторін у процесі розбудови та функціонування національної системи кібербезпеки; підтримка міжнародних ініціатив у сфері кібербезпеки, що відповідають національним інтересам України; поглиблення співпраці України з Європейським Союзом та НАТО з метою посилення спроможності України у сфері кібербезпеки; участь у заходах із зміцнення довіри при використанні кіберпростору, що проводяться під егідою Організації з безпеки і співробітництва в Європі[1].

Реалізація запропонованих заходів сприятиме удосконаленню національної системи кібербезпеки, здатної ефективно протидіяти сучасним кібервикликам.

Використана література

1. Стратегія кібербезпеки України: затвердж. Указом Президента України від 26 серпня 2021 року №47. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text.

2. Скіцько О.І., Ширшов Р.А. Актуальні питання забезпечення кібербезпеки об'єктів критичної інфраструктури. *Юридичний науковий електронний журнал*. 2024. №10/2024. С. 312-315. URL:http://lsej.org.ua/10_2024/73.pdf.

3. CERT-UA минулого року опрацювала 4315 кіберінцидентів URL:https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv.

4. Марущак А.І., Петров С.Г. Сучасний стан розвитку національної системи кібербезпеки (на прикладі СБ України та Держспецз'вязку України). *Інформація і право.* 2020. № 2(33)/2020. С. 77-84.

5. Алексеєва О.А. Правове забезпечення кібербезпеки об'єктів критичної інфраструктури. *Інформація і право*. 2023. № 4(47). С. 168-176.

6. Скіцько О., Ширшов Р. Нормативно-правове забезпечення кібероборони України: сучасний стан. *Юридичний вісник*. 2024. №3. С. 244-245.

7. Дубов Д.В. Кіберпростір як новий вимір геополітичного суперництва: монографія. Київ: НІСД. 2014. 328 с.

8. Печенюк А.В. Інформаційна безпека України як складова національної безпеки.URL:https://scholar.google.com.ua/citations?view_op=view_citation&hl=uk&user=_Iwh2mAAAAAJ&citation_for_view=_Iwh2mAAAAAJ:M3NEmzRMIkIC

9. Ліпкан В., Діордіца І. Національна система кібербезпеки як складова частина системи забезпечення національної безпеки України. *Підприємництво, господарство і право*. 2017. № 5. С. 174-180.

10. Діордіца І.В. Поняття та зміст національної системи кібербезпеки. URL: https://goal-int.org.

11. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року №2163. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

12. Довгань О.Д., Доронін І.М. Розвиток законодавства у сфері кібербезпеки: інформаційно-правове дослідження. *Наукові часописи УДУ імені Махайла Драгоманова*. Серія 18. Право. 2017. Випуск №32. С. 91-100. https://enpuir.npu.edu.ua/bitstream/handle/123456789/24333/Dovgan_Doronin.pdf?sequence=1&isAllowed=y.

13. План заходів на 2025 роки з реалізації Стратегії кібербезпеки: затв. розпорядженням Кабінету Міністрів України від 7 березня 2025 р. № 204-р. URL: https://zakon.rada.gov.ua/laws/show/204-2025-%D1%80#Text.

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~