КАБІНЕТ МІНІСТРІВ УКРАЇНИ

ПОСТАНОВА

від 29 грудня 2021 р. № 1426

Київ

Про затвердження Положення про організаційно-технічну модель кіберзахисту

Відповідно до частини третьої статті 8 Закону України “Про основні засади забезпечення кібербезпеки України” та з метою забезпечення функціонування національної системи кібербезпеки Кабінет Міністрів України **постановляє:**

Затвердити Положення про організаційно-технічну модель кіберзахисту, що додається.

Прем’єр-міністр України **Д. ШМИГАЛЬ**

Інд. 49

ЗАТВЕРДЖЕНО
постановою Кабінету Міністрів України
від 29 грудня 2021 р. № 1426

ПОЛОЖЕННЯ
про організаційно-технічну модель кіберзахисту

1. Це Положення визначає механізм функціонування організаційно-технічної моделі кіберзахисту.

Організаційно-технічна модель кіберзахисту є комплексом заходів, сил і засобів кіберзахисту, спрямованих на оперативне (кризове) реагування на кібератаки та кіберінциденти, впровадження контрзаходів, спрямованих на мінімізацію вразливості комунікаційних систем.

Організаційно-технічна модель кіберзахисту складається з організаційно-керуючої, технологічної та базисної інфраструктури кіберзахисту та впроваджується для забезпечення функціонування національної системи кібербезпеки.

2. У цьому Положенні терміни вживаються у такому значенні:

базисна інфраструктура кіберзахисту — організована сукупність об’єктів критичної інформаційної інфраструктури, комунікаційних і технологічних систем підприємств, установ та організацій, що належать до об’єктів критичної інфраструктури, а також суб’єктів господарювання, громадян та їх об’єднань, інших осіб, які провадять діяльність та/або надають послуги у сферах електронних комунікацій, електронної комерції, розвитку національних електронних ресурсів, захисту інформації та кібербезпеки;

кібергігієна — уміння, навички користування інформаційними технологіями, спрямовані на здійснення заходів щодо своєчасного виявлення, запобігання і нейтралізації реальних і потенційних кіберзагроз;

команди реагування на комп’ютерні надзвичайні події — групи фахівців з кібербезпеки, які утворюються з метою забезпечення кіберзахисту комунікаційних, інформаційних та/або технологічних систем;

організаційно-керуюча інфраструктура кіберзахисту — організована сукупність суб’єктів забезпечення кібербезпеки, що формують та/або реалізують державну політику у сфері кібербезпеки, визначають процедури та механізми кіберзахисту, організаційно-правові засади взаємодії між силами кіберзахисту та іншими суб’єктами забезпечення кібербезпеки;

технологічна інфраструктура кіберзахисту — організована сукупність сил та засобів кіберзахисту, інфраструктурних об’єктів, що забезпечують

функціонування сил кіберзахисту, інформаційно-телекомунікаційних мереж та їх ресурсів, що використовуються в інтересах сил кіберзахисту;

сили кіберзахисту — урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA, інші команди реагування на комп'ютерні надзвичайні події, підрозділи (групи, команди, служби) захисту інформації, підприємства, установи та організації незалежно від форми власності, які провадять діяльність та/або надають послуги, пов'язані з кіберзахистом.

Інші терміни вживаються у значенні, наведеному в Законах України "Про основні засади забезпечення кібербезпеки України", "Про національну безпеку України", "Про захист інформації в інформаційно-телекомунікаційних системах", "Про електронні довірчі послуги".

3. Функціонування організаційно-технічної моделі кіберзахисту забезпечується шляхом:

формування та реалізації державної політики у сфері кібербезпеки, зокрема з урахуванням досвіду держав — членів ЄС та НАТО;

координації суб'єктів кіберзахисту під час здійснення заходів щодо забезпечення кібербезпеки об'єктів критичної інформаційної інфраструктури та національних електронних інформаційних ресурсів;

кіберзахисту інформаційно-телекомунікаційних систем, що обробляють національні електронні інформаційні ресурси, комунікаційних систем та об'єктів критичної інформаційної інфраструктури, їх кіберстійкості, здійснення постійного контролю за станом їх кіберзахисту;

розвитку системи реагування на кіберзагрози;

розвитку сил кіберзахисту та системи їх координації;

створення систем управління ризиками інформаційної безпеки на об'єктах критичної інфраструктури;

формування та розвитку спроможностей суб'єктів забезпечення кібербезпеки;

створення умов для безпечного функціонування інформаційної інфраструктури державних органів, органів місцевого самоврядування, військових формувань, утворених відповідно до закону, підприємств, установ та організацій незалежно від форми власності;

створення умов для розвитку державно-приватної взаємодії в сфері кібербезпеки;

розвитку системи кадрового, матеріально-технічного та експертно-аналітичного забезпечення сил кіберзахисту;

розвитку та постійного вдосконалення систем кіберзахисту об'єктів критичної інфраструктури з урахуванням результатів оцінки повноти, адекватності, результативності та ефективності процесів, що виконуються

в рамках впровадження системи інформаційної безпеки на об’єктах критичної інфраструктури.

4. Засобами кіберзахисту, які використовуються для впровадження організаційно-технічної моделі кіберзахисту, є системи виявлення вразливостей і реагування на кіберінциденти та кібератаки, інформаційні технології, технічні і програмні засоби (пристрої, обладнання, комплекси), які використовуються в інтересах забезпечення кіберзахисту національних електронних інформаційних ресурсів, комунікаційних і технологічних систем, а також об’єктів критичної інформаційної інфраструктури.

5. Заходами з кіберзахисту, які здійснюються у процесі впровадження організаційно-технічної моделі кіберзахисту, є організаційні, правові, інженерно-технічні заходи, заходи з криптографічного та технічного захисту інформації, які проводяться силами кіберзахисту та базуються на принципах персональної відповідальності за власні дії та колективної відповідальності за безпеку кожного, забезпечення пропорційності та/або співрозмірності заходів реальним та потенційним ризикам.

6. Команди реагування на комп’ютерні надзвичайні події здійснюють ідентифікацію, проводять оцінку та аналіз кіберінцидентів (кібератак), координують та беруть участь в процесі реагування на них, налагоджують комунікації та інформаційний обмін щодо кіберінцидентів (кібератак), зокрема інформують інші команди реагування на комп’ютерні надзвичайні події про кіберінциденти (кібератаки), узагальнюють досвід за результатами реагування та розробляють рекомендації щодо покращення стану кіберзахисту комунікаційних, інформаційних та/або технологічних систем, здійснюють профілактичні і попереджувальні заходи щодо об’єктів кіберзахисту.

7. Організаційно-керуюча інфраструктура кіберзахисту складається з таких секторів:

загальнодержавний, до складу якого входять основні суб’єкти національної системи кібербезпеки, сили безпеки і оборони та Національний координаційний центр кібербезпеки як робочий орган Ради національної безпеки і оборони України;

галузевий, до складу якого входять центральні органи виконавчої влади, інші державні органи, які забезпечують формування та/або реалізацію державної політики в одній чи кількох сферах, або безпосередньо проводять відповідно до компетенції заходи із забезпечення кібербезпеки, об’єкти критичної інфраструктури незалежно від форми власності;

регіональний (місцевий), до складу якого входять місцеві органи виконавчої влади, органи місцевого самоврядування, підприємства, установи та організації незалежно від форми власності, що провадять діяльність у сфері захисту інформації та кіберзахисту;

освіти та науки, до складу якого входять науково-дослідні установи, заклади вищої освіти у сфері захисту інформації та кібербезпеки, що беруть участь у підготовці, підвищенні кваліфікації та перепідготовці професійних кадрів;

приватний, до складу якого входять підприємства недержавної форми власності, організації та установи, що провадять діяльність у сфері захисту інформації та кіберзахисту (крім об'єктів критичної інфраструктури);

громадський, до складу якого входять громадські організації, об'єднання, асоціації, спілки та фахівці у сфері кібербезпеки, а також міжнародні та міжурядові організації, що провадять свою діяльність у сфері кібербезпеки.

8. Під час функціонування організаційно-керуючої інфраструктури кіберзахисту суб'єкти забезпечення кібербезпеки:

здійснюють законодавче та нормативно-правове регулювання питань кіберзахисту об'єктів критичної інфраструктури, кібербезпеки та кіберзахисту комунікаційних і технологічних систем;

забезпечують гармонізацію законодавства у сфері захисту інформації, інформаційної безпеки та кібербезпеки з відповідним законодавством ЄС;

забезпечують розвиток сил кіберзахисту, системи кадрового, фінансового, матеріально-технічного та експертно-аналітичного забезпечення сил кіберзахисту;

проводять регулярні навчання щодо попередження і реагування на кіберзагрози та кіберінциденти, відновлення після кібератак;

залучають наукові установи, професійні та громадські об'єднання до підготовки проектів законодавчих та інших нормативно-правових актів у сфері кіберзахисту;

організовують і проводять огляд стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом;

створюють умови для розвитку спроможностей сил кіберзахисту, спрямованих на виявлення кібератак та захист від них, для ліквідації їх наслідків, відновлення сталості і надійності функціонування комунікаційних та технологічних систем;

забезпечують впровадження сучасних принципів, методів, підходів та механізмів публічного управління в сфері кібербезпеки;

здійснюють співробітництво з питань кібербезпеки з органами інших держав, міжнародними, міжурядовими організаціями відповідно до компетенції та законодавства і міжнародних договорів України;

координують дії з розроблення протоколів та регламентів взаємодії, карт технологічних процесів, регламентів робіт, планів реагування на

кіберінциденти, планів відновлення та інших документів, що регламентують взаємодію між силами кіберзахисту;

організовують та проводять кібернавчання, розробляють програми та методики їх проведення, сценарії реагування на кіберзагрози, проводять заходи щодо протидії кіберзагрозам, з кібергігієни.

9. Технологічна інфраструктура кіберзахисту складається з таких рівнів:

національного — на базі сил кіберзахисту основних суб'єктів національної системи кібербезпеки та Національного координаційного центру кібербезпеки як робочого органу Ради національної безпеки і оборони України;

галузевого (регіонального, місцевого) — на базі сил кіберзахисту суб'єктів забезпечення кібербезпеки галузевого (регіонального) рівня;

об'єктового — на базі сил кіберзахисту підприємств, установ та організацій незалежно від форми власності, насамперед тих, що належать до об'єктів критичної інфраструктури.

10. Суб'єкти, що діють у технологічній інфраструктурі кіберзахисту, забезпечують оперативне (кризове) реагування на кібератаки та кіберінциденти та здійснюють обмін інформацією про ризики у сфері кібербезпеки, а також про кіберінциденти, кібератаки на:

національному рівні — між собою та відповідними підрозділами інших суб'єктів забезпечення кібербезпеки;

галузевому (регіональному, місцевому) рівні — з відповідними суб'єктами національного та галузевого (регіонального, місцевого) рівня технологічної інфраструктури кіберзахисту;

об'єктовому рівні — з відповідними суб'єктами всіх рівнів технологічної інфраструктури кіберзахисту.

11. Під час функціонування технологічної інфраструктури кіберзахисту сили кіберзахисту:

здійснюють заходи з оперативного та ефективного захисту кіберпростору щодо зменшення ризиків у сфері кібербезпеки, протидії кібератакам, кіберзлочинам, кібертероризму, кібершпигунству, а також забезпечення кібероборони та кіберрозвідки шляхом збору, аналізу, оцінювання, узагальнення та поширення інформації про ризики у сфері кібербезпеки, кіберінциденти, кібератаки;

здійснюють заходи з оперативного (кризового) реагування на кібератаки та кіберінциденти, зокрема за допомогою системи інформаційного обміну щодо таких подій, контрзаходи, спрямовані на усунення вразливостей комунікаційних систем;

здійснюють заходи з кіберзахисту об’єктів критичної інформаційної інфраструктури, комунікаційних систем, в яких обробляються національні електронні інформаційні ресурси та/або які використовуються державними органами, органами місцевого самоврядування, військовими формуваннями, утвореними відповідно до закону;

забезпечують функціонування систем оцінювання ризиків у сфері кібербезпеки і реагування на кіберінциденти та кібератаки щодо об’єктів кіберзахисту;

розвивають об’єднання (мережі) команд реагування на комп’ютерні надзвичайні події, взаємодіють з командами реагування на комп’ютерні надзвичайні події, а також підприємствами, установами та організаціями незалежно від форми власності, які провадять діяльність, пов’язану із забезпеченням безпеки у кіберпросторі;

здійснюють взаємодію між собою відповідно до рішень суб’єктів забезпечення кібербезпеки;

інформують про кібератаки та потенційні кіберризики інших суб’єктів забезпечення кібербезпеки, опрацьовують отриману від них, зокрема від громадян, інформацію про кіберінциденти та щодо об’єктів кіберзахисту, надають консультативну та практичну допомогу з питань реагування на кібератаки;

сприяють державним органам, органам місцевого самоврядування, військовим формуванням, утвореним відповідно до закону, підприємствам, установам та організаціям незалежно від форми власності, а також громадянам у вирішенні питань щодо кіберзахисту та протидії кіберзагрозам;

створюють та забезпечують функціонування основних складових частин системи захищеного доступу державних органів до Інтернету, системи антивірусного захисту національних електронних інформаційних ресурсів;

беруть участь у проведенні кібернавчань, розробленні програм та методик їх проведення, сценаріїв реагування на кіберзагрози та проводять заходи щодо протидії кіберзагрозам, з кібергігієни.

12. Здійснення заходів з кіберзахисту системами кіберзахисту передбачає:

ідентифікацію — виявлення реальних і потенційних кіберзагроз для запобігання їм і їх нейтралізації;

захист — розроблення та впровадження методів, засобів, процедур кіберзахисту, спрямованих на забезпечення сталості і надійності функціонування інформаційних, телекомунікаційних, інформаційно-телекомунікаційних та технологічних систем;

виявлення — проведення моніторингу визначення, збору та обробки нетипових подій у кіберпросторі;

реагування — вжиття заходів, спрямованих на запобігання кіберінцидентам, кібератакам, мінімізації їх можливих наслідків (запобігання виникненню загроз життю або здоров'ю людей та заподіяння шкоди майну), удосконалення систем кіберзахисту, з урахуванням необхідності забезпечення пропорційності та/або співрозмірності можливостей таких систем реальним та потенційним ризикам;

відновлення — поновлення штатного режиму функціонування інформаційних, телекомунікаційних, інформаційно-телекомунікаційних, технологічних систем після кібератаки, відновлення інформації та відомостей у разі їх пошкодження або видалення, створення умов для проведення розслідування кібератаки.

13. Під час забезпечення функціонування базисної інфраструктури кіберзахисту забезпечується:

захист у кіберпросторі національних електронних інформаційних ресурсів, комунікаційних і технологічних систем, зокрема тих, що використовуються для задоволення суспільних потреб;

захист об'єктів критичної інформаційної інфраструктури;

захист інтересів громадянина та суспільства у кіберпросторі;

розроблення програм розвитку основ кібергігієни на національному, галузевому (регіональному, місцевому), об'єктовому рівні;

здійснення заходів з формування культури кібербезпеки в установах, на об'єктах критичної інфраструктури і підприємствах незалежно від форми власності;

інформування громадян про кіберінциденти.

14. Базисна інфраструктура кіберзахисту функціонує для забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів у кіберпросторі.

_____