УКАЗ ПРЕЗИДЕНТА УКРАЇНИ
№96/2016

Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України"

Відповідно до статті 107 Конституції України, частини другої статті 2 Закону України "Про основи національної безпеки України"

п о с т а н о в л я ю:

1. Увести в дію рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України" (додається).
2. Затвердити Стратегію кібербезпеки України (додається).
3. Секретареві Ради національної безпеки і оборони України подати у місячний строк на розгляд Президентові України проект Положення про Національний координаційний центр кібербезпеки.
4. Цей Указ набирає чинності з дня його опублікування.

Президент України Петро ПОРОШЕНКО
15 березня 2016 року

Введено в дію
Указом Президента України
від 15 березня 2016 року
№96/2016

РІШЕННЯ
РАДИ НАЦІОНАЛЬНОЇ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ
від 27 січня 2016 року
Про Стратегію кібербезпеки України

Розглянувши проект Стратегії кібербезпеки України, внесений Кабінетом Міністрів України, Рада національної безпеки і оборони України вирішила:

1. Схвалити проект Стратегії кібербезпеки України і запропонувати її Президентові України для затвердження.
2. Кабінету Міністрів України разом із Службою безпеки України, Службою зовнішньої розвідки України та за участю Національного інституту стратегічних досліджень:
1) затвердити у двомісячний строк план заходів на 2016 рік із реалізації Стратегії кібербезпеки України, надалі розробляти і затверджувати на період реалізації Стратегії такі плани щороку до початку відповідного планового року;
2) інформувати щопівроку про стан реалізації Стратегії кібербезпеки України.
3. Утворити відповідно до статті 14 Закону України "Про Раду національної безпеки і оборони України" Національний координаційний центр кібербезпеки як робочий орган Ради національної безпеки і оборони України.

Секретар Ради національної безпеки і оборони
України Олександр ТУРЧИНОВ

ЗАТВЕРДЖЕНО

Указом Президента України
Від 15 березня 2016 року

№96/2016

Стратегія кібербезпеки України
1. Загальні положення

Стрімкий розвиток інформаційних технологій поступово трансформує світ. Відкритий та вільний кіберпростір розширює свободу і можливості людей, збагачує суспільство, створює новий глобальний інтерактивний ринок ідей, досліджень та інновацій, стимулює відповідальну та ефективну роботу влади і активне залучення громадян до управління

державою та вирішення питань місцевого значення, забезпечує публічність та прозорість влади, сприяє запобіганню корупції.

Водночас переваги сучасного цифрового світу та розвиток інформаційних технологій обумовили виникнення нових загроз національній та міжнародній безпеці. Поряд із інцидентами природного (ненавмисного) походження зростає кількість та потужність кібератак, вмотивованих інтересами окремих держав, груп та осіб.

Поширюються випадки незаконного збирання, зберігання, використання, знищення, поширення, персональних даних, незаконних фінансових операцій, крадіжок та шахрайства у мережі Інтернет. Кіберзлочинність стає транснаціональною та здатна завдати значної шкоди інтересам особи, суспільства і держави.

Агресія Російської Федерації, що триває, інші докорінні зміни у зовнішньому та внутрішньому безпековому середовищі України вимагають невідкладного створення національної системи кібербезпеки як складової системи забезпечення національної безпеки України.

Метою Стратегії кібербезпеки України (далі – Стратегія) є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави.

Для досягнення цієї мети необхідними є:
створення національної системи кібербезпеки;
посилення спроможностей суб'єктів сектору безпеки та оборони для забезпечення ефективної боротьби із кіберзагрозами воєнного характеру, кібершпигунством, кібертероризмом та кіберзлочинністю, поглиблення міжнародного співробітництва у цій сфері;

забезпечення кіберзахисту державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, а також інформаційної інфраструктури, яка знаходиться під юрисдикцією України, та порушення сталого функціонування якої матиме негативний

вплив на стан національної безпеки і оборони України (критична інформаційна інфраструктура).

Забезпечення кібербезпеки України як стану захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі, що досягається комплексним застосуванням сукупності правових, організаційних, інформаційних заходів, має базуватися на принципах:

верховенства права і поваги до прав та свобод людини і громадянина;
забезпечення національних інтересів України;
відкритості, доступності, стабільності та захищеності кіберпростору;
державно-приватного партнерства, широкої співпраці з громадянським суспільством у сфері забезпечення кібербезпеки та кіберзахисту;
пропорційності та адекватності заходів кіберзахисту реальним та потенційним ризикам;
пріоритетності запобіжних заходів;
невідворотності покарання за вчинення кіберзлочинів;
пріоритетного розвитку та підтримки вітчизняного наукового, науково-технічного та виробничого потенціалу;
міжнародного співробітництва з метою зміцнення взаємної довіри у сфері кібербезпеки та вироблення спільних підходів у протидії кіберзагрозам, консолідації зусиль у розслідуванні та запобіганні кіберзлочинам, недопущення використання кіберпростору в протиправних та воєнних цілях;
забезпечення демократичного цивільного контролю над утвореними відповідно до законів України військовими формуваннями та правоохоронними органами держави, що діють у сфері кібербезпеки.
Розвиток та безпека кіберпростору, запровадження електронного урядування, гарантування безпеки й сталого функціонування електронних комунікацій та державних електронних інформаційних ресурсів мають бути складовими державної політики у сфері розвитку інформаційного простору та становлення інформаційного суспільства в Україні.
Ця Стратегія базується на положеннях Конвенції про кіберзлочинність, ратифікованої Законом України від 7 вересня 2005 року № 2824-IV,

законодавства України щодо основ національної безпеки, засад внутрішньої та зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом та спрямована на реалізацію до 2020 року Стратегії національної безпеки України, затвердженої Указом Президента України від 26 травня 2015 року № 287 "Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про Стратегію національної безпеки України".

2. Загрози кібербезпеці

Кіберпростір поступово перетворюється на окрему, поряд із традиційними "Земля", "Повітря", "Море" та "Космос", сферу ведення бойових дій, у якій все більш активно діють відповідні підрозділи збройних сил провідних держав світу. З урахуванням широкого застосування сучасних інформаційних технологій у секторі безпеки і оборони, створення єдиної автоматизованої системи управління Збройних Сил України оборона нашої держави стає більш уразливою до кіберзагроз.

Економічна, науково-технічна, інформаційна сфера, сфера державного управління, оборонно-промисловий і транспортний комплекси, інфраструктура електронних комунікацій, сектор безпеки і оборони України стають все більш уразливими для розвідувально-підривної діяльності іноземних спецслужб у кіберпросторі. Цьому сприяє широка, подекуди домінуюча, присутність в інформаційній інфраструктурі України організацій, груп, осіб, які прямо чи опосередковано пов'язані з Російською Федерацією.

Сучасні інформаційно-комунікаційні технології можуть використовуватися для здійснення терористичних актів, зокрема шляхом порушення штатних режимів роботи автоматизованих систем керування технологічними процесами на об'єктах критичної інфраструктури. Більшого поширення набуває політично вмотивована діяльність у кіберпросторі у вигляді атак на урядові та приватні веб-сайти в мережі Інтернет.

Дедалі частіше об'єктами кібератак та кіберзлочинів стають інформаційні ресурси фінансових установ, підприємств транспорту та енергозабезпечення, державних органів, які гарантують безпеку, оборону, захист від надзвичайних ситуацій. Новітні технології застосовуються не лише для скоєння традиційних видів злочинів, але і для скоєння принципово нових видів злочинів, притаманних суспільству з високим рівнем інформатизації.

Загрози кібербезпеці актуалізуються через дію таких чинників, зокрема, як:
невідповідність інфраструктури електронних комунікацій держави, рівня її розвитку та захищеності сучасним вимогам;
недостатній рівень захищеності критичної інформаційної інфраструктури, державних електронних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, від кіберзагроз;
безсистемність заходів кіберзахисту критичної інформаційної інфраструктури;
недостатній розвиток організаційно-технічної інфраструктури забезпечення кібербезпеки та кіберзахисту критичної інформаційної інфраструктури та державних електронних інформаційних ресурсів;
недостатня ефективність суб'єктів сектору безпеки і оборони України у протидії кіберзагрозам воєнного, кримінального, терористичного та іншого характеру;
недостатній рівень координації, взаємодії та інформаційного обміну між суб'єктами забезпечення кібербезпеки.

3. Національна система кібербезпеки, основні суб'єкти забезпечення кібербезпеки

Національна система кібербезпеки має насамперед забезпечити взаємодію з питань кібербезпеки державних органів, органів місцевого самоврядування, військових формувань, правоохоронних органів, наукових установ, навчальних закладів, громадських об'єднань, а також підприємств, установ та організацій незалежно від форми власності, які провадять діяльність у сфері електронних комунікацій, захисту інформації

та/або є власниками (розпорядниками) об'єктів критичної інформаційної інфраструктури.

Рада національної безпеки і оборони України відповідно до Конституції України та у встановленому законом порядку має здійснювати координацію та контроль діяльності суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку України.

Основу національної системи кібербезпеки становитимуть Міністерство оборони України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національна поліція України, Національний банк України, розвідувальні органи, на які мають бути покладені в установленому порядку такі основні завдання:

на Міністерство оборони України, Генеральний штаб Збройних Сил України відповідно до компетенції – здійснення заходів з підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони); здійснення військової співпраці з НАТО, пов’язаної з безпекою кіберпростору та сумісним захистом від кіберзагроз; забезпечення у взаємодії з Державною службою спеціального зв'язку та захисту інформації України і Службою безпеки України кіберзахисту власної інформаційної інфраструктури;

на Державну службу спеціального зв'язку та захисту інформації України – формування та реалізація державної політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту критичної інформаційної інфраструктури, державний контроль у цих сферах; координація діяльності інших суб'єктів кібербезпеки щодо кіберзахисту; здійснення організаційно-технічних заходів із запобігання, виявлення та реагування на кіберінциденти і кібератаки та усунення їх наслідків, інформування про кіберзагрози та відповідні методи захисту від них; забезпечення функціонування державного центру кіберзахисту; проведення аудиту захищеності об'єктів критичної інформаційної інфраструктури на вразливість;

на Службу безпеки України – попередження, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, які вчиняються у кіберпросторі; здійснення контррозвідувальних та оперативно-розшукових заходів, спрямованих на боротьбу з кібертероризмом та кібершпигунством, а також щодо готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів; протидія кіберзлочинності, можливі наслідки якої безпосередньо створюють загрозу життєво важливим інтересам України; розслідування кіберінцидентів та кібератак щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури; забезпечення реагування на комп'ютерні інциденти у сфері державної безпеки;

на Національну поліцію України – забезпечення захисту прав і свобод людини та громадянина, інтересів суспільства і держави від злочинних посягань у кіберпросторі; запобігання, виявлення, припинення та розкриття кіберзлочинів; підвищення поінформованості громадян про безпеку в кіберпросторі;

на Національний банк України – формування вимог щодо кіберзахисту критичної інформаційної інфраструктури у банківській сфері;

на розвідувальні органи України – здійснення розвідувальної діяльності щодо загроз національній безпеці України у кіберпросторі, інших подій і обставин, що стосуються сфери кібербезпеки.

Мають бути створені умови для залучення підприємств, установ та організацій незалежно від форми власності, які провадять діяльність у сфері електронних комунікацій, захисту інформації та/або є власниками (розпорядниками) об'єктів критичної інфраструктури, до забезпечення кібербезпеки України. Зокрема, мають бути врегульовані питання щодо обов'язковості вжиття ними заходів із забезпечення захисту інформації та кіберзахисту відповідно до вимог законодавства, а також щодо сприяння ними державним органам у виконанні завдань із забезпечення кібербезпеки та кіберзахисту.

Держава сприятиме залученню наукових установ, навчальних закладів, організацій, громадських об'єднань і громадян до розробки та реалізації заходів із кібербезпеки і кіберзахисту.

4. Пріоритети та напрями забезпечення кібербезпеки України

4.1. Розвиток безпечного, стабільного і надійного кіберпростору має полягати, насамперед, у:

виробленні і оперативній адаптації державної політики у сфері кібербезпеки, спрямованої на розвиток кіберпростору, досягненні сумісності з відповідними стандартами ЄС та НАТО;

створенні вітчизняної нормативно-правової та термінологічної бази у цій сфері, гармонізації нормативних документів у сфері електронних комунікацій, захисту інформації, інформаційної та кібербезпеки відповідно до міжнародних стандартів і стандартів ЄС та НАТО;

формуванні конкурентного середовища у сфері електронних комунікацій, наданні послуг із захисту інформації та кіберзахисту;

розвитку технологій кіберзахисту засобів рухомого зв'язку, забезпеченні апаратної, контентної безпеки, безпеки додатків та сервісів зв'язку;

залученні експертного потенціалу наукових установ, професійних та громадських об'єднань до підготовки проектів концептуальних документів у сфері кібербезпеки;

підвищенні цифрової грамотності громадян та культури безпекового поводження в кіберпросторі, комплексних знань, навичок і здібностей, необхідних для підтримки цілей кібербезпеки, впровадженні державних і громадських проектів підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту;

проведенні навчань щодо надзвичайних ситуацій та інцидентів у кіберпросторі;

розвитку та удосконаленні системи державного контролю за станом захисту інформації, а також системи незалежного аудиту інформаційної безпеки, запровадженні кращих світових практик і міжнародних стандартів з питань кібербезпеки та кіберзахисту;

розвитку інфраструктури електронних комунікацій, включаючи широкосмуговий доступ до мережі Інтернет, цифрове та інтерактивне телебачення;

розвитку мережі команд реагування на комп'ютерні надзвичайні події;

створенні системи своєчасного виявлення, запобігання та нейтралізації кіберзагроз, у тому числі із залученням волонтерських організацій;
розвитку та вдосконаленні системи технічного і криптографічного захисту інформації;
розвитку міжнародного співробітництва у сфері забезпечення кібербезпеки, підтримці міжнародних ініціатив у сфері кібербезпеки, які відповідають національним інтересам України, поглибленні співпраці України з ЄС та НАТО для посилення спроможностей України у сфері кібербезпеки, участі у заходах зі зміцнення довіри у кіберпросторі, які проводяться під егідою ОБСЄ;
створенні умов для впровадження в Україні сучасних технологій кіберзахисту.

4.2. Кіберзахист державних електронних інформаційних ресурсів та інформаційної інфраструктури, призначеної для обробки інформації, вимога щодо захисту якої встановлена законом, має полягати, насамперед, у:
створенні та забезпеченні функціонування національної телекомунікаційної мережі – єдиної платформи захищених електронних комунікацій органів державної влади;
упровадженні організаційно-технічної моделі національної системи кібербезпеки, оперативному реагуванні на кібератаки та кіберінциденти;
розгортанні (відповідно до компетенції) єдиної системи ситуаційних центрів профільних органів державної влади сектору безпеки і оборони на базі захищеної інформаційної інфраструктури;
розбудові захищеної інтегрованої системи електронних державних реєстрів, баз даних, дата-центрів, у тому числі єдиного дата-центру резервного збереження інформації і відомостей державних електронних інформаційних ресурсів;
удосконаленні системи зберігання, передачі та обробки даних державних реєстрів і баз даних із застосуванням сучасних інформаційно-комунікаційних технологій (включаючи технології онлайн-доступу);
розробленні нових методів запобігання кібератакам, кіберінцидентам та поширенню інформації про них;
розробленні вимог (правил, настанов) щодо безпечного використання мережі Інтернет та надання електронних послуг державними органами;

підвищенні обізнаності працівників державних органів у сфері інформаційної безпеки та кібербезпеки, проведенні відповідних тренінгів, навчань.

4.3. Кіберзахист критичної інфраструктури має полягати, насамперед, у:
комплексному вдосконаленні правової основи кіберзахисту об'єктів критичної інфраструктури, визначенні критеріїв віднесення інформаційних (автоматизованих), телекомунікаційних, інформаційно-телекомунікаційних систем до критичної інформаційної інфраструктури;
формуванні та забезпеченні функціонування державного реєстру об'єктів критичної інформаційної інфраструктури;
регламентації вимог до кіберзахисту об'єктів критичної інфраструктури;
створенні та забезпеченні функціонування власниками (розпорядниками) об'єктів критичної інфраструктури підрозділів кіберзахисту;
установленні кваліфікаційних вимог для окремих категорій працівників об'єктів критичної інфраструктури з урахуванням сучасних тенденцій кібербезпеки та актуальних кіберзагроз, упровадження для таких працівників обов'язкової періодичної атестації на предмет відповідності зазначеним вимогам;
налагодженні співробітництва між суб'єктами забезпечення кіберзахисту критичної інфраструктури, розвитку державно-приватного партнерства у запобіганні кіберзагрозам, реагуванні на кібератаки та кіберінциденти, усуненні їх наслідків, зокрема в умовах кризових ситуацій, надзвичайного і воєнного стану, в особливий період;
розробленні та запровадженні механізму обміну інформацією між державними органами, приватним сектором і громадянами стосовно загроз критичній інформаційній інфраструктурі.

4.4. Розвиток потенціалу сектору безпеки і оборони у сфері забезпечення кібербезпеки передбачатиме здійснення в установленому порядку, зокрема, таких заходів:
здійснення захисту технологічних процесів на об'єктах критичної інфраструктури, в яких управління або моніторинг здійснюється за допомогою інформаційно-комунікаційних технологій, від несанкціонованого втручання у їх роботу;

періодичне проведення огляду національної системи кібербезпеки, розроблення галузевих індикаторів стану кібербезпеки;
розроблення та впровадження протоколів спільних дій, зокрема інформаційного обміну у режимі реального часу, суб'єктів забезпечення кібербезпеки під час виявлення кібератак та кіберінцидентів;
проведення навчань суб'єктів сектору безпеки і оборони щодо реагування на кібератаки та кіберінциденти, зокрема, проведення кібернавчань Збройних Сил України, інших суб'єктів сектору безпеки і оборони України, участь у таких навчаннях у рамках заходів колективної оборони;
реалізація державного стратегічного планування та програмно- цільового забезпечення у сфері розвитку електронних комунікацій, інформаційних технологій, захисту інформації та кіберзахисту;
здійснення воєнно-політичних, військово-технічних та інших заходів для розширення можливостей Воєнної організації держави, сектору безпеки і оборони у кіберпросторі, створення, розвиток сил, засобів та інструментів можливої відповіді на агресію у кіберпросторі, яка може застосовуватись як засіб стримування військових конфліктів та загроз у кіберпросторі (активний кіберзахист);
створення єдиного підрозділу із забезпечення кібербезпеки та кіберзахисту Збройних Сил України на стратегічному, оперативному та тактичному рівнях;
розвиток підрозділів кібербезпеки та кіберзахисту Збройних Сил України, Державної служби спеціального зв'язку та захисту інформації України, Служби безпеки України, Національної поліції України, розвідувальних органів, досягнення сумісності із відповідними підрозділами кібербезпеки та кіберзахисту держав – членів НАТО;
сприяння розвитку системи оперативного реагування на комп'ютерні надзвичайні події;
удосконалення системи контррозвідувального та оперативно-розшукового забезпечення кібербезпеки держави;
розвиток та координація проведення наукових досліджень у галузі кібербезпеки та кіберзахисту для потреб національної безпеки і оборони;
підвищення спроможності суб'єктів боротьби з кібертероризмом щодо протидії кібератакам на державні електронні інформаційні ресурси, об'єкти критичної інфраструктури, а також розвідувально-підривної

діяльності іноземних спецслужб, організацій, груп та осіб проти України у кіберпросторі;
обмеження участі у заходах із забезпечення інформаційної та кібербезпеки будь-яких суб'єктів господарювання, які знаходяться під контролем держави-агресора, визнаної Верховною Радою України, або держав та осіб, стосовно яких діють спеціальні економічні та інші обмежувальні заходи (санкції), прийняті на національному або міжнародному рівні внаслідок агресії щодо України, а також обмеження використання продукції, технологій та послуг таких суб'єктів для забезпечення технічного та криптографічного захисту державних інформаційних ресурсів, посилення державного контролю у цій сфері;
розмежування кримінальної відповідальності за злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, вчинені щодо державних та інших інформаційних ресурсів, щодо об'єктів критичної інформаційної інфраструктури та інших об'єктів, а також відповідне розмежування підслідності;
розвиток системи підготовки кадрів для потреб органів сектору безпеки і оборони України та розвиток науково-виробничого потенціалу такої системи.

4.5. Боротьба з кіберзлочинністю передбачатиме здійснення в установленому порядку, серед іншого, таких заходів:
створення ефективного і зручного контакт-центру для повідомлень про випадки кіберзлочинів та шахрайства у кіберпросторі, підвищення оперативності реагування на кіберзлочини правоохоронних органів, зокрема їх регіональних підрозділів;
удосконалення процесуальних механізмів щодо збирання доказів в електронній формі, що стосуються злочину, удосконалення класифікації, методів, засобів і технологій ідентифікації та фіксації кіберзлочинів, проведення експертних досліджень;
запровадження блокування операторами та провайдерами телекомунікацій визначеного (ідентифікованого) інформаційного ресурсу (інформаційного сервісу) за рішенням суду;

унормування порядку внесення обов'язкових до виконання операторами та провайдерами телекомунікацій приписів про термінове фіксування та подальше зберігання комп'ютерних даних, збереження даних про трафік;
врегулювання питання можливості термінового здійснення процесуальних дій у режимі реального часу із застосуванням електронних документів та електронного цифрового підпису;
упровадження схеми (протоколу) координації правоохоронних органів щодо боротьби з кіберзлочинністю;
підготовка суддів (слідчих суддів), слідчих та прокурорів для роботи з доказами, що стосуються злочину, отриманими в електронній формі, з урахуванням особливостей кіберзлочинів;
запровадження особливого порядку зняття інформації з каналів телекомунікацій у випадку розслідування кіберзлочинів;
підвищення кваліфікації співробітників правоохоронних органів.

5. Прикінцеві положення

Положення Стратегії враховуються у розробленні інших документів стратегічного планування суб'єктів сектору безпеки і оборони України у сфері кібербезпеки.