Проект

СТРАТЕГІЯ ЗАБЕЗПЕЧЕННЯ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ УКРАЇНИ

1. Визначення

Кібернетичний простір (кіберпростір) – сукупність інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем і мереж державних органів, органів місцевого самоврядування, військових формувань, органів військового управління, а також та фізичних осіб, які функціонують на території України або знаходяться підприємств, установ, організацій (незалежно від форми власності) під її юрисдикцією, інформаційних ресурсів, які в них наявні, програмне забезпечення, яке призначено для їх обробки;

кібернетична загроза (кіберзагроза) – наявні та потенційно можливі явища і чинники, що створюють небезпеку інтересам людини, суспільства та держави через порушення доступності, повноти, цілісності, достовірності, автентичності режиму доступу до інформації, яка циркулює в критичних об’єктах національної інформаційної інфраструктури;

кібернетична безпека (кібербезпека) – стан захищеності критичних об’єктів національної інформаційної інфраструктури та окремих її складових, за якого забезпечується їх стале функціонування і розвиток, своєчасне виявлення, запобігання і нейтралізація кібернетичних загроз в інтересах людини, суспільства, держави.

суб’єкти забезпечення кібернетичної безпеки - державні органи, (передусім інституції сектору безпеки і оборони України), органи місцевого самоврядування, підприємства, установи, організації незалежно від форми власності які здійснюють проектування, впровадження та експлуатацію складових критичних об’єктів національної інформаційної інфраструктури або забезпечують їх кіберзахист.

кібернетичний захист (кіберзахист) – сукупність заходів організаційного, нормативно-правового, воєнного, оперативного та технічного характеру, спрямованих на забезпечення кібернетичної безпеки;

кібернетичний злочин (кіберзлочин) – передбачене кримінальним законом суспільно небезпечне винне діяння, що полягає у протиправному використанні інформаційних та комунікаційних технологій, відповідальність за яке встановлена законодавством про кримінальну відповідальність;

кібернетичний тероризм (кібертероризм) – несанкціоновані дії з терористичною метою стосовно систем або мереж критичних об’єктів національної інформаційної інфраструктури, інформації, яка в них циркулює, та програмного забезпечення, призначеного для її обробки;

кібернетичне шпигунство (кібершпигунство) – передача або збирання з метою передачі іноземній державі, іноземній організації або їх представникам відомостей з обмеженим доступом, яке здійснюється в кіберпросторі.

кібернетична війна (кібервійна) – застосування іншою державою або групою держав збройної сили проти України в кібернетичному просторі.

критичні об’єкти національної інформаційної інфраструктури – складова кіберпростору, реалізація кібернетичних загроз щодо яких може призвести до настання таких наслідків:

- надзвичайна ситуація;
- блокування роботи або руйнування стратегічно важливих для економіки та безпеки держави підприємств, систем життєзабезпечення та об’єктів підвищеної небезпеки;
- блокування роботи державних органів, органів місцевого самоврядування;
- блокування діяльності військових формувань, органів військового управління, Збройних Сил України в цілому, або втручання в автоматизовані системи керування зброєю;
- порушення безпечного функціонування банківської та/або фінансової системи держави;
- розголошення державної таємниці;
- масові заворушення.

2. Загальні положення

Побудова інформаційного суспільства в різних країнах світу, глобалізація інформаційних процесів, суттєве зростання ролі інформаційної інфраструктури в різних сферах суспільного життя з одного боку створюють підґрунтя для ефективного соціально–економічного розвитку держав, задоволення конституційного права особи на інформацію, побудови ефективної системи державного управління. З іншого, – сучасні інформаційні технології, перетворює інформаційні системи урядового, оборонного, виробничого, кредитно – банківського, комунального та інших секторів на надзвичайно вразливі для реалізації кібернетичних загроз об’єкти.

Національна безпека України, її економічне процвітання та соціальне благополуччя все більше залежать від доступності, цілісності та конфіденційності інформаційних ресурсів, що забезпечуються інформаційними та комунікаційними технологіями, або в більш широкому розумінні - кіберпростором. Водночас, зростання залежності від інформаційно-комунікаційних технологій робить сучасне українське

суспільство більш уразливим перед можливими негативними наслідками протиправного використання кіберпростору. В цих умовах головним завданням держави є вжиття заходів, що дозволять принципово зменшити (а подекуди - унеможливити повністю) негативні наслідки від кібератак.

Джерелами кібернетичних загроз можуть бути міжнародні злочинні групи хакерів, окремі підготовлені у сфері інформаційних технологій злочинці, іноземні державні органи, терористичні та екстремістські угруповання, транснаціональні корпорації та фінансово-промислові групи тощо. Зростає загроза використання проти інтересів України кібернетичних засобів як з середини держави, так і з-за меж її кордонів. Такою ж реальною є загроза використання української інформаційної інфраструктури як "транзитного майданчику" для приховування атаки на інформаційну інфраструктуру третьої сторони.

Україна послідовно виходить з того, що кіберпростір є відкритим простором – відкритим до інновацій, вільного розповсюдження ідей, інформації та обміну думками.

Заходи із забезпечення кібербезпеки жодним чином не можуть суперечити принципу гарантування прав та свобод українських громадян, в тому числі права на недоторканість приватного життя та свободи спілкування.

Забезпечення кібербезпеки вимагає узгодженого, комплексного підходу – на чолі з державою, однак у тісному співробітництві з приватним сектором та громадянським суспільством, без якого неможливо вирішити дане завдання.

Забезпечення кібернетичної безпеки України відбувається із врахування положень Конституції, Закону України «Про основні засади внутрішньої та зовнішньої політики», Закону України «Про основи національно безпеки», Стратегії національної безпеки України та Доктрини інформаційної безпеки України.

Метою цієї Стратегії є визначення основних підходів до формування державної політики у сфері забезпечення кібернетичної безпеки України.

3. Загрози в сфері кібернетичної безпеки

Кіберзлочинність. Злочини із використанням сучасних інформаційно-телекомунікаційних технологій стають все звичнішою практикою в житті українських громадян. При чому новітні технології застосовуються не лише для скоєння традиційних видів злочинів, але й для скоєння нових видів злочинів, характерних передусім для розвинутого інформаційного суспільства. Найбільше увага злочинців зосереджена на спробах порушення роботи або несанкціонованого використання можливостей інформаційних систем державного, кредитно-банківського, комунального, оборонного, виробничого секторів. Все ще актуальною залишаються проблеми боротьби із дитячою порнографією та порушеннями авторських та суміжних прав.

Кібертероризм та кібершпигунство. Ціла низка вітчизняних підприємств, порушення роботи яких може становити загрозу життю та здоров'ю громадян, може стати потенційною ціллю для здійснення терористичних актів, в тому числі – із застосування сучасних інформаційних технологій. Не меншою загрозою є вчинення протиправних дій на шкоду третім країнам, що здійснюються із використанням вітчизняної інформаційної інфраструктури, що загрожують сталому та безпечному функціонуванню національних інформаційно-телекомунікаційних систем. Інформація з обмеженим доступом, що циркулює в національних інформаційних ресурсах є стійким об'єктом зацікавленості з боку інших держав, організацій та осіб. Крім того, все більшого поширення набуває політично вмотивована діяльність в кіберпросторі груп активістів (хактивістів), які здійснюють атаки на урядові та приватні сайти, що призводить до порушень роботи інформаційних ресурсів, а також репутаційних та матеріальних збитків.

Кібервійна. Воєнна сфера зазнає чи не найдраматичніших змін внаслідок розбудови глобального кіберпростору. Більшість країн світу активно трансформує свої потенціали у сфері оборони в напрямі посилення кібернетичних можливостей ведення бойових дій та захисту від аналогічних дій з боку супротивника, оскільки все актуальнішими стають нові типи загроз. З урахуванням широкої інформатизації сектору безпеки і оборони, зокрема, створення ЄАСУ ЗС України, оборонний потенціал нашої держави стає більш чутливим до кіберзагроз. Впровадження провідними країнами сучасних кіберозброєнь перетворює кіберпростір на окрему, поряд з традиційними «Земля», «Повітря», «Море», «Космос», сферу ведення бойових дій, а у найближчому майбутньому, рівень обороноздатності країни буде визначатись у т.ч. наявністю у неї ефективних підрозділів для ведення бойових дій в кіберпросторі та здатність протистояти кіберзагрозам в сфері оборони.

4. Основні принципи забезпечення кібернетичної безпеки України

Реалізація основних засад забезпечення кібернетичної безпеки України має здійснюватись при неухильному дотриманні таких принципів:

верховенства права, законності та пріоритету додержання прав і свобод людини і громадянина;

невідворотності відповідальності за вчинення кібернетичних злочинів;

пріоритетності запобіжних заходів;

комплексного здійснення правових, організаційних, технічних, криптографічних, інформаційних та інших заходів;

партнерства держави та приватного сектору з метою вироблення нових, більш оптимальних рішень;

пріоритетного розвитку та підтримки вітчизняної науково-інноваційної сфери;

відповідальності суб'єктів забезпечення кібернетичної безпеки за захист національної інформаційної інфраструктури;

дієвості, комплексності і постійності заходів забезпечення кібернетичної безпеки держави;

участі інституцій громадянського суспільства у забезпеченні кібернетичної безпеки держави;

співпраці на міжнародному рівні, з метою вироблення єдиних підходів та ефективної взаємодопомоги протидії кіберзагрозам.

5. Основні напрями забезпечення кібернетичної безпеки

Протидія реальним загрозам та мінімізація потенційних загроз потребує низки кроків держави в ключових сферах життєдіяльності, що мають особливе значення для забезпечення кібернетичної безпеки. З цією метою, держава, у партнерстві із суспільством, недержавним та приватним сектором, а також громадянами, з метою посилення кібербезпеки України, буде при формуванні власної політики кібербезпеки керуватись такими пріоритетами:

1) у зовнішньополітичній сфері:

підвищувати роль України як активного учасника формування стандартів світової політики по відношенню до кіберпростору;

підтримувати міжнародні ініціативи у сфері кібербезпеки з урахуванням національних інтересів України;

сприяти недопущенню мілітаризації кіберпростору;

неухильно дотримуватись взятих на себе міжнародних зобов'язань у сфері кібернетичної безпеки та боротьби з кібернетичною злочинністю;

підвищувати рівень міжнародного співробітництва у сфері забезпечення кібернетичної безпеки на загальнодержавному та відомчому рівнях;

сприяти створенню міжнародних правил поведінки держав у кіберпросторі та удосконаленню міжнародної нормативно-правової бази у відповідності до кібербезпекових викликів національній та міжнародній безпеці;

підтримувати як існуючі багатосторонні навчання із протидії кібернападам на державну та приватну інформаційну інфраструктуру, так і ініціювати нові види таких навчань.

2) у сфері державної та внутрішньополітичної безпеки:

створити Національну систему кібернетичної безпеки України;

встановити обов'язкові вимоги щодо кіберзахисту критичних об'єктів національної інформаційної інфраструктури в незалежності від форми власності, порядок захисту та контролю за його дотриманням;

здійснювати заходи реформування системи захисту інформації з обмеженим доступом з урахуванням реалій сьогодення задля уникнення витоків такої інформації;

посилювати технічні та технологічні можливості, науковий та людський потенціал Служби безпеки України, розвідувальних органів та Державної служби спеціального зв'язку і захисту інформації у кіберпросторі;

посилювати боротьбу з кібертероризмом та кібершпигунством, захист від їх проявів критичних об'єктів національної інформаційної інфраструктури;

забезпечити імплементацію положень Конвенції РЄ про кіберзлочинність у національне законодавство, зокрема, щодо:

- надання повноважень органам дізнання та слідства щодо видачі обов'язкових до виконання провайдерами приписів про термінове фіксування та подальше зберігання комп'ютерних даних, які потрібні для розкриття злочину;
- обов'язковості збереження провайдерами даних про трафік на строк до 90 днів із можливістю дальшого продовження терміну до 3 років;
- зобов'язання суб'єкта, який зберігає комп'ютерні данні, не розголошувати факт проведення оперативно-розшукових та процесуальних дій протягом визначеного законодавством періоду;
- надання провайдером органу дізнання або слідства інформації для ідентифікації постачальників послуг і маршруту, яким було передано інформацію;

удосконалювати кримінальне законодавство, виділити окремі склади злочинів де об'єктом протиправних посягань є елементи національної критичної інформаційної інфраструктури;

сприяти розвитку мережі команд реагування на комп'ютерні надзвичайні події (CERT);

3) у воєнній сфері:

здійснювати підготовку до застосування ЗС України в умовах «кібервійни»;

створювати можливості для відбиття військової агресії в кіберпросторі з урахуванням нових викликів та загроз;

захищати військову інформаційну інфраструктуру від реальних та потенційних кіберзагроз;

створити систему підготовки кадрів у сфері кібербезпеки для потреб ЗС та інших органів сектору безпеки і оборони України;

4) у соціальній, гуманітарній та науково-технологічній сферах:

розвивати та координувати науково-дослідні роботи у галузі кібербезпеки;

створювати сприятливі умови для молодих фахівців в ІТ-сфері, що має сприяти їх працевлаштуванню в Україні;

забезпечити внесення змін до навчальних планів та програм середньої та вищої школи, підготовки наукових та науково-педагогічних кадрів, що спрямовані на інформування основних цільових груп про кіберзагрози та методи протидії ним;

розробляти загальнодержавні програми підвищення рівня обізнаності населення щодо кіберзагроз (в тому числі через створення всеукраїнської системи змагань серед молоді, що присвячені проблемі кібербезпеці, запровадження «Національного тижню обізнаності з кібербезпекою»);

підтримувати зусилля громадянського суспільства та бізнесу щодо підвищення обізнаності населення з актуальних кіберзагроз;

стимулювати всі зацікавлені сторони до активної участі у щорічних Днях безпечного інтернету;

сприяти більш активній політиці державних безпекових інституцій щодо інформування населення про кіберзагрози;

забезпечити безперервне підвищення кваліфікації державних службовців та працівників, що задіяні на ключових об'єктах критичної інфраструктури;

сприяти розробці вітчизняної інноваційної продукції, що може бути використана з метою посилення кібернетичної безпеки держави.

6. Система забезпечення кібернетичної безпеки України

6.1. Одними з першочергових заходів на шляху побудови системи кібербезпеки держави є вдосконалення державного управління у даній сфері та впорядкування нормативно-правового поля.

6.2. З метою забезпечення кібернетичної безпеки України має бути створено цілісну Національну систему кібернетичної безпеки ключовими завданнями якої має бути:

формування та реалізація державної політики в сфері кібернетичної безпеки;

моніторинг кібернетичного простору з метою своєчасного виявлення, запобігання і нейтралізації кібернетичних загроз;

виявлення, попередження та припинення кібернетичних злочинів;

кібернетичний захист національної критичної інформаційної інфраструктури.

6.3. До складу Національної системи кібернетичної безпеки мають бути включені:

Служба безпеки України;

Міністерство внутрішніх справ України;

Міністерство оборони України;

Генеральний Штаб Збройних Сил України;

Державна служба спеціального зв'язку та захисту інформації України;

У разі необхідності до участі у здійсненні заходів, пов’язаних із виявленням, запобіганням і нейтралізацією кібернетичних загроз, залучаються інші суб’єкти забезпечення кібернетичної безпеки.

6.4. Вироблення пропозицій щодо визначення, коригування засад внутрішньої і зовнішньої політики у сфері забезпечення кібернетичної безпеки України має здійснювати Міжвідомча колегія з питань протидії кібернетичним загрозам при Президенті України, яка має статус консультативно-дорадчого органа. Очолює Колегію Президент України.

До складу Міжвідомчої колегії з питань протидії кібернетичним загрозам за посадою входять Прем’єр-міністр України, Голова Служби безпеки України, Міністр внутрішніх справ України, Міністр оборони України, начальник Генерального штабу Збройних Сил України, Голова Державної служби спеціального зв’язку та захисту інформації України, керівник Державного агентство з кіберзахисту.

6.5. З метою координації дій суб’єктів забезпечення кібернетичної безпеки, необхідним є створення Державного агентства з кіберзахисту - державного органу для забезпечення своєчасного виявлення, запобігання і нейтралізації кібернетичних загроз, управління Національною системою кібернетичної безпеки, забезпечення роботи Міжвідомчої колегії з питань протидії кібернетичним загрозам при Президенті України.

З метою виконання завдань Агентство:

організовує взаємодію суб’єктів забезпечення кібернетичної безпеки у т.ч. їх заходи щодо визначення можливих наслідків реалізації кібернетичних загроз, усунення передумов до їх настання та наслідків їх реалізації;

веде реєстр об’єктів національної критичної інформаційної інфраструктури, розробляє критерії визначення ступенів важливості, вразливості, захисту таких об’єктів, а також методику прогнозування наслідків, що можуть настати в результаті реалізації кібернетичних загроз щодо вказаних об’єктів;

надає методичну допомогу та рекомендації суб'єктам забезпечення кібернетичної безпеки щодо виявлення і усунення причин та умов, які сприяють вчиненню кібернетичних злочинів;

надає дозволи на впровадження в об’єктах національної критичної інформаційної інфраструктури програмного забезпечення та обладнання;

у межах компетенції контролює дотримання власниками об’єктів національної кібернетичні критичної інформаційної інфраструктури вимог чинного законодавства у сфері технічного захисту інформації;

спільно зі Службою безпеки України організовує спеціальну перевірку осіб, відповідальних за технічний захист інформації об’єктів критичної інформаційної інфраструктури;

аналізує внутрішні та зовнішні загрози;

готує пропозиції щодо вдосконалення законодавства України з питань кібернетичної безпеки;

організовує і проводить навчання та тренування в сфері кібернетичного захисту;

організовує та здійснює міжнародне співробітництво із спеціальними службами, правоохоронними органами іноземних держав та міжнародними організаціями з питань кібернетичного захисту та боротьби з кібернетичними злочинами.

6.2. З метою вдосконалення вітчизняного нормативно-правового поля та у зв’язку з створенням Національної системи кібернетичної безпеки, необхідно внесення наступних змін до Законів України:

- Про основи національної безпеки

щодо визначення кібернетичної безпеки самостійною сферою національної безпеки, загроз, основних напрямів державної політики;

- Про захист інформації в інформаційно-телекомунікаційних системах;

щодо розширення сфери дії закону на критичну інформаційну інфраструктуру;

- Про оборону України

щодо підготовки Збройних Сил України до відбиття агресії в кіберпросторі;

- Про інформацію

щодо статусу інформації яка циркулює в ІТС та АСУ критичної інформаційної інфраструктури;

- Про телекомунікації

щодо приведення Закону у відповідність до Конвенції РЄ про кіберзлочинність;

- Про боротьбу з тероризмом

щодо боротьби з кібернетичним тероризмом;

- Про ліцензування певних видів господарської діяльності

щодо ліцензування обладнання та програмного забезпечення для застосування в ІТС та АСУ об’єктів критичної інформаційної інфраструктури;

- Про захист населення і територій від надзвичайних ситуацій техногенного та природного характеру

щодо кіберзахисту об'єктів підвищеної небезпеки;

- Про оперативно-розшукову діяльність

щодо спецперевірки осіб, відповідальних за ТЗІ об’єктів критичної інформаційної інфраструктури

- Кримінальний кодекс
- Кримінальний процесуальний кодекс
- Кодекс про адміністративні правопорушення

щодо встановлення відповідальності за правопорушення у сфері кібернетичної безпеки (коли об'єктом протиправних посягань є державні інформаційні ресурси або критична інформаційна інфраструктура);

- Про Збройні Сили України
- Про Службу безпеки України
- Про Державну службу спеціального зв'язку та захисту інформації України

щодо уточнення компетенції та повноважень у зв'язку зі створенням Національної системи кібернетичної безпеки.

7. Етапи реалізації Стратегії

7.1. На першому етапі реалізації Стратегії (2014-2016 рр.) серед першочергових заходів передбачається вдосконалення нормативно-правової бази (в тому числі – за взятими на себе Україною міжнародними зобов'язаннями), створення ключових елементів Національної системи кібернетичної безпеки: сприяння створенню мережі CERTів в Україні, проведення заходів із підготовки ЗС України до ведення дій в умовах кібервійни, створення базису підготовки спеціалізованих кадрів для сектору безпеки та об'єктів критичної інфраструктури з протидії кіберзагрозам, формування відповідної нормативно-правової бази та практичних умов співробітництва між державним та недержавним сектором безпеки з питань протидії кіберзлочинності, збільшення уваги до заходів інформування громадян та бізнесу з питань кібербезпеки, має бути створено Державне агентство з кіберзахисту.

7.2. На другому етапі (2016-2017), передбачається вдосконалення міжнародних правил поведінки держав у кіберпросторі та вдосконалення міжнародної нормативно-правової бази у відповідності до кібербезпекових викликів національній та міжнародній безпеці, завершення розбудови Національної системи кібернетичної безпеки, впровадження програм підтримки вітчизняної інноваційної продукції, що може бути використана з метою посилення кібернетичної безпеки держави; сприяння розвитку мережі CERTів в Україні.

7.3. На третьому етапі (2017 і наступні роки), з огляду на динамічність сфери кібербезпеки та актуалізацію нових викликів та загроз, передбачається коригування Стратегії на основі оцінки ефективності її реалізації та нових викликів.