USAID
ВІД АМЕРИКАНСЬКОГО НАРОДУ

Фонд Східна Європа

ЛАБОРАТОРІЯ
ЗАКОНОДАВЧИХ
ІНІЦІАТИВ
www.parlament.org.ua

Михайло Кольцов , Оксана Приходько, Єгор Аушев

Пропозиції до політики щодо реформування сфери кібербезпеки в Україні

ГРУДЕНЬ, 2017

Підготовка аналітичних матеріалів є частиною проекту, що реалізує ГО «Лабораторія законодавчих ініціатив» у рамках Програми USAID «РАДА: підзвітність, відповідальність, демократичне парламентське представництво». Програма USAID «РАДА», що виконується Фондом Східна Європа, сприяє становленню підзвітного, відповідального і демократичного парламентського органу.

Більше на www.radaprogram.org

Думки, викладені в цій публікації, є виключною відповідальністю авторів дослідження та не обов'язково відображають точку зору USAID, Фонду Східна Європа та Лабораторії законодавчих ініціатив.

Лабораторія законодавчих ініціатив

Пропозиції до політики щодо реформування сфери кібербезпеки в Україні

(Policy Paper)

Автор:

Михайло Кольцов, Оксана Приходько, Єгор Аушев

ГРУДЕНЬ, 2017

АНОТАЦІЯ

Робота присвячена аналізу проблем у сфері кібербезпеки України та пошукам шляхів їхнього вирішення. Увагу авторів було зосереджено на вдосконаленні нормативно-правової бази, створенні належної інфраструктури, розвитку індустрії кібербезпеки, забезпеченні умов для плідної співпраці всіх українських та міжнародних стейкголдерів, розвитком культури мережевої та інформаційної безпеки. На думку авторів, побудова ефективної державної політики у сфері кібербезпеки можлива лише за наявності єдиного центру управління, чіткої узгодженої програми дій та підвищенні рівня довіри між основними стейкголдерами.

ABSTRACT

The paper is devoted to the analysis of problems with cybersecurity in Ukraine and to the search for ways to solve them. The authors' attention was focused on improving the regulatory framework, creating the proper infrastructure, developing the cybersecurity industry, ensuring conditions for the fruitful cooperation of all Ukrainian and international stakeholders, and developing a culture of network and information security. According to the authors, the construction of effective state policy in the field of cybersecurity is possible only if there is a single control center, a clear agreed program of action and increased confidence among the main stakeholders.

Зміст

Скорочення:

ВРУ - Верховна Рада України

Держспецзв'язок - Державна служба спеціального зв'язку та захисту інформації України

Директива NIS - Директива ЄС щодо заходів для забезпечення високого загального рівня безпеки мережевих та інформаційних систем у всьому Союзі

ЄС - Європейський Союз (ЄвроСоюз)

МСЕ - Міжнародний Союз Електрозв'язку

РЄ - Рада Європи

РНБОУ - Рада національної безпеки та оборони України

УПА - Угода про Асоціацію

GDPR - Регламент ЄС про захист фізичних осіб стосовно обробки персональних даних та про вільне переміщення таких даних, а також про скасування Директиви 95/46/ЄС

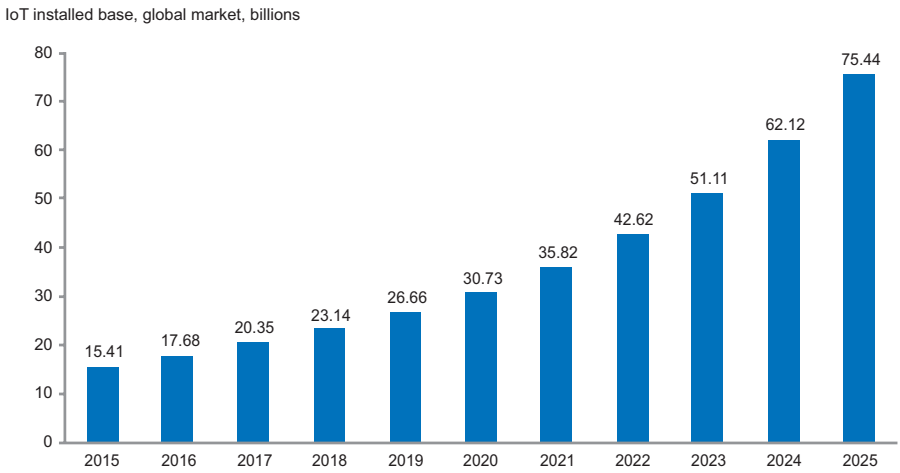
CSIRT/CERT - команда реагування на надзвичайні події в кіберпросторі (Computer Security Incident Response Team/Computer Emergency Response Team)

IoT - Інтернет речей (Internet of Things)

BSA - Business Software Allience

1. Ідентифікація та опис проблеми

Використання Інтернету, інтернету речей (IoT) та інформаційних технологій відкриває перед людством безмежні можливості, але й створює нові, дуже серйозні, загрози. Все більше інформації переміщується в онлайн і за останніми підрахунками у світі, вже понад 20 млрд пристроїв підключених, до інтернету, що у кілька разів більше ніж населення Землі. Також на серверах зберігаються мільярди гігібайтів різної інформації. Світ стає відкритим, та таке стрімке зростання потребує формування "правил гри".



Збереження кіберпростору відкритим, надійним та безпечним потребує комплексного та узгодженого підходу за участі усіх стейкголдерів. Україна зробила на цьому шляху три дуже важливих кроки:

- ратифіковано Конвенцію Ради Європи з кіберзлочинності,
- розроблено Стратегію кібербезпеки,
- створено команди реагування на надзвичайні події в кіберпросторі CSIRT (та кількість таких команд безумовно має збільшуватись).

Попереду робота над створенням відповідної нормативно-правової бази та інфраструктури, розвитком індустрії кібербезпеки, забезпеченням умов для плідної співпраці усіх українських та міжнародних стейкголдерів, розвитком культури мережевої та інформаційної безпеки. Кожен крок у цьому напрямку зустрічає відчайдушний спротив (як зсередини, так і з боку зовнішнього агресора). Подолання цього спротиву можливе лише за наявності єдиного "центру керування", чіткої узгодженої програми дій та підвищення рівня довіри між основними стейкголдерами.

Відсутність в Україні законодавчого забезпечення кібербезпеки в умовах гібридної війни значно підвищує ризики руйнування національної системи

кібербезпеки (якщо така взагалі існує), а також ставить під сумнів участь українських складових забезпечення кібербезпеки на європейському та світовому рівнях. Сьогодні в Україні відсутній єдиний центр координації роботи щодо законодавчого та нормативно-правового забезпечення ефективної системи кібербезпеки, яка би базувалась на комплексному аналізі наявного ста-ну в цій сфері, викликів, наявних та потенційних загроз, враховувала інтереси усіх стейкголдерів, інтегрувалась в європейську та глобальну міжнародну систему кібербезпеки, мала б достатнє фінансове, організаційне, технічне, кадрове забезпечення.

2. Регуляторні принципи сфери кібербезпеки (історія питання)

Правову основу кібернетичної безпеки України становлять Конституція України, закони України «Про основи національної безпеки», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», та інші закони, Конвенція Ради Європи про кіберзлочинність, інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, Стратегія кібербезпеки України, інші нормативно-правові акти. Найважливішими серед них є Конвенція Ради Європи про кіберзлочинність та Стратегія кібербезпеки України.

2.1. Конвенція Ради Європи про кіберзлочинність (Будапештська конвенція)

Конвенція Ради Європи про кіберзлочинність (Будапештська конвенція) є першим і найбільш визнаним міжнародно-правовим документом у сфері боротьби з міжнародною і національною кіберзлочинністю. Цей договір було вчинено 23.11.2001, і Україна була однією з перших його підписантів. Ратифікувала вона цю Конвенцію, щоправда, тільки 10.03.2006, та ще й не в повному обсязі (з заявами і застереженнями).

Загальна кількість країн, що ратифікували Конвенцію Ради Європи про кіберзлочинність, сягає 55, і, звісно, не обмежується країнами-членами РЄ (цю Конвенцію ратифікували також США, Канада, Японія, Мексика, Австралія та багато інших країн). Ще чотири країни підписали, але не ратифікували Конвенцію. Категорично проти її підписання виступають Росія та Китай.

Як зазначено у преамбулі, "Конвенція є необхідною для зупинення дій, спрямованих проти конфіденційності, цілісності і доступності комп'ютерних систем, мереж і комп'ютерних даних, а також зловживання такими системами, мережами і даними, шляхом встановлення кримінальної відповідальності за таку поведінку, як це описано в Конвенції, надання повноважень, достатніх для ефективної боротьби з такими кримінальними правопорушеннями шляхом сприяння їхньому виявленню, розслідуванню та переслідуванню, як на внутрішньодержавному, так і на міжнародному рівнях, і укладення домовленостей щодо швидкого і надійного міжнародного співробітництва". Водночас особлива увага звертається на необхідність забезпечити належний баланс між правоохоронними інтересами і повагою до основних прав людини, таких, як право кожного безперешкодно дотримуватись поглядів, а також право на свободу слова, включаючи право на пошук, отримання і передачу будь-якої інформації та ідей, незважаючи на кордони, права на повагу до приватного життя, а також права на захист особистої інформації.

Конвенція передбачає запровадження на національному рівні кримінальної відповідальності за наступні групи злочинів:

- Правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (Незаконний доступ, Нелегальне перехоплення, Втручання у дані, Втручання у систему, Зловживання

пристроями);

- Правопорушення, пов'язані з комп'ютерами (Підробка, пов'язана з комп'ютерами, Шахрайство, пов'язане з комп'ютерами);
- Правопорушення, пов'язані зі змістом (Правопорушення, пов'язані з дитячою порнографією);
- Правопорушення, пов'язані з порушенням авторських та суміжних прав.

Ця частина Конвенції більш-менш імплементована в українське законодавство, хоча є певні кримінальні порушення, що не є злочином за текстом Конвенції, але переслідуються за українським законодавством ("доросла" порнографія, наприклад), є певні порушення, що визначаються як злочини Конвенцією та не переслідуються чинним українським законодавством (наприклад, розсилка спаму). Звичайно, бажано було б гармонізувати і ці положення українського законодавства у відповідності до норм Конвенції, але ці питання не мають критичного впливу на рівень національної, європейської та світової кібербезпеки.

Проте такий вплив має ситуація з імплементацією наступного розділу Конвенції – Процедурне право. Багато положень з цього розділу не імплементовано в українське законодавство. Можливо, не в останню чергу це пояснюється низькою якістю офіційного українського перекладу Конвенції, розміщеного на сайті Верховної Ради України (http://zakon2.rada.gov.ua/laws/show/994_575). "Термінове збереження комп'ютерних даних, які зберігаються" (в оригіналі – Expedited preservation of stored computer data), "збирання комп'ютерних даних у реальному масштабі часу" (Real-time collection of traffic data) та інші перекладацькі хиби унеможливлюють адекватну імплементацію положень Конвенції в українське законодавство та ще більш ускладнюють пошук спільної мови між правоохоронцями та постачальниками послуг. Однак тільки поганою якістю перекладу проблеми з належною імплементацією Конвенції в українське законодавство не вичерпуються. Відсутність в українському законодавстві поняття "електронні докази" призводить до необхідності проведення обшуків та вилучення обладнання та носіїв інформації навіть у тих випадках, коли можна було б обмежитись отриманням електронних копій, і суттєво ускладнює міжнародне співробітництво.

Дуже важливим та контроверсійним є питання співпраці правоохоронних органів та постачальників послуг щодо порядку збереження інформації (про користувача послуг, про рух інформації), отримання до неї доступу (в тому числі і в електронному форматі), терміну збереження та порядку знищення інформації, розподіл повноважень між правоохоронними органами та СБУ тощо.

Слід зазначити, що, починаючи з 2011 року, Україна бере участь у реалізації проекту Ради Європи та Європейського Союзу "Кіберзлочинність@Східне партнерство", метою якого як раз і є ефективна імплементація Будапештської конвенції, удосконалення національного законодавства в сфері боротьби з кіберзлочинністю, налагодження державно-приватного партнерства в цій сфері. Однак ця робота ведеться за зачиненими дверима, за дуже обмеженої кількості учасників, і тому дуже легко нівелюється законопроектами, які вносяться тими, хто не є долученим до цієї роботи.

2.2. Стратегія кібербезпеки України

Стратегія кібербезпеки України була розроблена на виконання Стратегії національної безпеки України від 2015 року, затверджена рішенням Ради національної безпеки і оборони України та введена в дію Указом Президента України 27.01.2016.

Провідним розробником Стратегії кібербезпеки України виступила Державна служба спеціального зв'язку та захисту інформації (Держспецзв'язок). В роботі над документом брали активну участь представники Громадської Ради при Держспецзв'язку, представники приватного бізнесу, експерти НАТО, ОБСЄ, RAND corporation. Документ дуже ретельно узгоджувався з усіма іншими державними структурами, що мають стосунок до кібербезпеки, доопрацьовувався в Кабінеті Міністрів, в Раді національної безпеки і оборони.

Стратегія кібербезпеки базується на положеннях Конвенції Ради Європи про кіберзлочинність та має на меті створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави.

Для цього передбачається:

- 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 перебуває під юрисдикцією України, та порушення сталого функціонування якої матиме негативний вплив на стан національної безпеки і оборони України (критична інформаційна інфраструктура).

Головними перевагами цієї Стратегії є:

- дотримання європейського підходу до забезпечення кібербезпеки як до спільної відповідальності усіх ключових стейкхолдерів;
- орієнтація на стандарти ЄС та НАТО в сфері забезпечення кібербезпеки замість застосування пострадянських або виключно радянських стандартів;
- відмова від пріоритету "захисту національного сегменту Інтернету", який є притаманним російському та китайському підходам до кібербезпеки.

Ця Стратегія закладає загальну архітектуру національної системи кібербезпеки та розподіляє завдання та повноваження між основними суб'єктами забезпечення кібербезпеки (Радою національної безпеки і оборони, Міністерством оборони, Генеральним штабом Збройних Сил, Державною службою спеціального зв'язку та захисту інформації, Службою безпеки, Національною поліцією, Національним банком, розвідувальними органами України), передбачає створення умов 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, наукових установ, навчальних закладів, організацій, громадських об'єднань і громадян. Запланований розвиток мережі команд реагування на комп'ютерні надзвичайні події, створення та забезпечення функціонування національної телекомунікаційної мережі – єдиної платформи захищених електронних комунікацій органів державної влади; розбудова захищеної інтегрованої системи електронних державних реєстрів, баз даних, дата-центрів, зокрема єдиного дата-центру резервного збереження інформації і відомостей державних електронних інформаційних ресурсів.

Багато уваги Стратегія приділяє захисту критичної інфраструктури, який має передбачати, зокрема, комплексне вдосконалення правової основи кіберзахисту об'єктів критичної інфраструктури, визначення критеріїв віднесення інформаційних (автоматизованих), телекомунікаційних, інформаційно-телекомунікаційних систем до критичної інформаційної інфраструктури; формування та забезпечення функціонування державного реєстру об'єктів критичної інформаційної інфраструктури; розроблення та запровадження механізму обміну інформацією між державними органами, приватним сектором і громадянами стосовно загроз критичній інформаційній інфраструктурі, налагодженню співробітництва між суб'єктами забезпечення кіберзахисту критичної інфраструктури.

Передбачено також формування конкурентного середовища у сфері електронних комунікацій, надання послуг із захисту інформації та кіберзахисту; залучення експертного потенціалу наукових установ, професійних та громадських об'єднань до підготовки проектів концептуальних документів у цій сфері; підвищення цифрової грамотності громадян та культури безпекового поводження в кіберпросторі; розвиток міжнародного співробітництва та підтримка міжнародних ініціатив у сфері кібербезпеки, зокрема поглиблення співпраці України з ЄС та НАТО.

Паралельно з ухваленням Стратегії було створено Національний координаційний центр кібербезпеки як робочий орган РНБОУ.

Ухвалення Стратегії є дуже важливим кроком у розбудові системи національної кібербезпеки, вкрай необхідним, але недостатнім, адже Стратегія не пропонує відповідної термінології та не передбачає внесення змін до чинних нормативно-правових актів. Ці питання планувалось врегулювати під час написання Закону України про кібербезпеку, який мав розроблятись саме так, як розроблялась Стратегія кібербезпеки.

Замість цього до Верховної Ради України було внесено проект Закону про основні засади забезпечення кібербезпеки України (2126а). Цей законопроект почали розробляти ще до ухвалення Стратегії кібербезпеки України, і його перші версії суперечили багатьом положенням Стратегії. У результаті багаторазового переписування (з чисельними порушеннями Регламенту ВРУ) вдалось отримати таку редакцію цього законопроекту, яка не завдає суттєвої шкоди системі кібербезпеки України (здебільшого шляхом прямого запозичення окремих фрагментів з тексту Стратегії). Але законопроекту, який би підіймав систему національної кібербезпеки на якісно вищий рівень, поки що нема.

3. Реформа законодавства ЄС та її значення для кібербезпеки України

07.02.2013 Європейський Союз ухвалив Стратегію кібербезпеки, метою якої є відкритий, надійний і безпечний кіберпростір. Для цього передбачені заходи з наступних напрямків:

1. Досягнення кіберстійкості.
2. Суттєве скорочення кіберзлочинності.
3. Розробка політики кібероборони, пов'язаної зі Спільною політикою безпеки і оборони.
4. Розвиток виробничих і технологічних ресурсів для кібербезпеки.
5. Створення узгодженої міжнародної політики кіберпростору для ЄС і просування основних цінностей ЄС.

Одразу після оприлюднення Стратегії було розпочато роботу над відповідною директивою. Важливо наголосити, що цей документ розроблявся не окремо від інших напрямків, а як частина Стратегії Єдиного Цифрового Ринку (Digital Single Market Strategy), з одного боку, і частини Європейського Порядку Денного з питань безпеки (European Agenda on Security), з іншого.

http://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf

Стратегія та Порядок денний були оприлюднені навесні 2015 року, в липні 2016 року Європейська Комісія презентувала "Додаткові заходи зі сприяння розвитку індустрії кіберзахисту", а 06.07.2016 була ухвалена Директива ЄС щодо заходів із забезпечення високого загального рівня безпеки мережевих та інформаційних систем у всьому Союзі (DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union – NIS Directive).

3.1. Директива ЄС щодо заходів із забезпечення високого загального рівня безпеки мережевих та інформаційних систем у всьому Союзі (Директива NIS)

Ця Директива закладає єдині правила та вимоги в сфері кібербезпеки для всіх країн ЄС, але залишає за кожною країною-членом право вжити власних заходів щодо імплементації норм цієї Директиви в національне законодавство (це має бути зроблено до 9 травня 2018 року).

Для досягнення мети Директиви (забезпечення більш високого рівня мережевої та інформаційної безпеки в межах Європейського Союзу) необхідно вжити заходів у трьох основних напрямках:

- підвищити спроможність системи кібербезпеки на національному рівні;
- підвищити рівень пан-європейського співробітництва;
- запровадити управління ризиками та зобов'язати сповіщати про кіберінциденти операторів базових послуг та провайдерів цифрових

послуг.

Для підвищення спроможності кібербезпеки на національному рівні держави-члени ЄС повинні розробити національну стратегію мережевої та інформаційної безпеки (яка має містити стратегічні цілі, пріоритети та державне підґрунтя, заходи з підготовки до кіберінцидентів, реагування на них та відновлення після них, засади державно-приватного партнерства, програму освітніх, тренувальних заходів та заходів з підвищення обізнаності, план науково-дослідницьких робіт, план оцінки та управління ризиками, список стейкголдерів, відповідальних за реалізацію стратегії), визначити один чи більше державних органів, що будуть відповідати за виконання Директиви, створити одну чи більше команд реагування на комп'ютерні надзвичайні події.

Для підвищення рівня пан-європейського співробітництва створюються спеціальні мережі та Група співробітництва, яка буде забезпечувати планування, керування, обмін інформацією та підготовку звітів щодо стану кібербезпеки в усіх країнах ЄС.

Найбільш важливі законодавчі новели стосуються умов роботи операторів базових послуг та провайдерів цифрових послуг. Визначення операторів базових послуг кожна країна дає сама, але на підставі спільних для усього ЄС критеріїв:

1. Підприємство (незалежно від форми власності) надає послугу, яка є базовою для підтримки критичної соціально-економічної діяльності;
2. Надання такої послуги потребує використання мережевих або інформаційних систем;
3. Порушення безпеки буде мати значний руйнівний вплив на надання базової послуги.

У першу чергу це стосується наступних секторів:

- енергетика: електроенергія, нафта, газ;
- транспорт: повітряний, залізничний, водний, автодорожній;
- банки кредитні установи;
- інфраструктура фінансового ринку: біржі, центральні контрагенти;
- заклади охорони здоров'я;
- постачання питної води;
- цифрова інфраструктура: точки обміну Інтернет-трафіком, провайдери системи доменних імен, сервіс-провайдери, реєстратури доменних імен верхнього рівня

Під провайдерами цифрових послуг, які підпадають під дію цієї Директиви, маються на увазі онлайнові торговельні майданчики, постачальники хмарних послуг, пошукові системи.

Такі підприємства мають вжити необхідних (технічних та організаційних) заходів для того, аби попередити ризики кіберінцидентів, забезпечити мережеву та інформаційну безпеку (у відповідності до потенційних ризиків), належним чином відреагувати на кіберінциденти з метою мінімізації шкоди, повідомити компетентні органи про кіберінциденти. Директивою також передбачається дотримання міжнародних стандартів цими підприємствами, постійне проведення моніторингу, аудиту та тестування.

Очікується, що у вересні 2017 року Європейська комісія оприлюднить оновлену редакцію Стратегії кібербезпеки.

3.2. Реформа системи правового регулювання захисту персональних даних у Європейському Союзі

У січні 2012 року було ініційовано реформування законодавства Європейського Союзу в сфері захисту персональних даних з метою приведення його у відповідність до вимог "цифрової епохи" та на виконання Стратегії Єдиного Цифрового Ринку Європи (Digital Single Market Strategy). У зв'язку з цим були підготовлені два документи: Директива 2016/680 Європейського Парламенту та Ради ЄС від 27 квітня 2016 р. про захист фізичних осіб стосовно обробки персональних даних компетентними органами для цілей запобігання, розслідування, виявлення або переслідування кримінальних злочинів або виконання кримінальних покарань та про вільне переміщення таких даних, а також про скасування Рамкового Рішення Ради 2008/977 (Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/IHA)

http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG

та Регламент (Євросоюз) 2016/679 Європейського Парламенту та Ради від 27 квітня 2016 року про захист фізичних осіб стосовно обробки персональних даних та про вільне переміщення таких даних, а також про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних - REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR - General Data Protection Regulation).

http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001. 01.ENG&toc=OJ:L:2016:119:TOC

Директива набула чинності 24 травня 2016 року, але країни-члени мають транспонувати її в своє національне законодавство до 6 травня 2018 року. Регламент є нормативно-правовим актом прямої дії і автоматично стає частиною національного законодавства кожної країни-члена з 25 травня 2018 року.

Положення Регламенту спрямовані на гармонізацію захисту основних прав і свобод фізичних осіб щодо діяльності з опрацювання і на забезпечення вільного потоку персональних даних між державами-членами. Єдиний для всіх країн-членів Регламент має сприяти розбудові простору свободи, безпеки, справедливості і економічного союзу; економічного і соціального прогресу; зміцненню законності і зближенню економік в рамках внутрішнього ринку, а також загальному добробуту фізичних осіб держав-членів. Директива більш детально визначає умови співпраці з правоохоронними органами.

Головні новації, які вносяться в європейське право цими документами:

- "право бути забутим" (право вимагати знищення усіх персональних даних після закінчення терміну їх обробки);

- захист володільцями персональних даних "за конструкцією" (by design) та "за замовченням" (by default). Перше визначення означає, що володілець персональних даних як під час проголошення мети обробки, так і в процесі самої обробки має гарантувати відповідність усієї процедури Регламенту. Друге визначення має забезпечити, що володілець повинен імплементувати механізми гарантування того, що за замовченням обробляються лише ті персональні дані, які є необхідними для кожної детально визначеної мети обробки, і не зберігаються поза межами мінімальних строків, необхідних для досягнення таких цілей. Ці механізми повинні також забезпечити, щоб персональні дані не були доступними невизначеному колу осіб;
- передача персональних даних третій країні або міжнародній організації може мати місце лише за умови, якщо передача даних необхідна: для захисту життєво важливих інтересів суб'єкта даних або іншої особи; для захисту законних інтересів суб'єкта даних, якщо це передбачено законодавством держави-члена стосовно передачі персональних даних; для запобігання прямій і серйозній загрозі для громадської безпеки держави-члена або третьої країни;
- право знати про злами баз персональних даних (компанії та організації мають повідомляти свої національні контролюючи органи про будь-які загрози для персональних даних суб'єктів цих даних, а також вступати в комунікації з самим суб'єктами даних щодо цих ризиків);
- більш легкий доступ до своїх даних: фізичні особи будуть мати більше інформації про те, яким чином обробляються їхні персональні дані. Ця інформація має бути надана чітко та зрозуміло;
- право на перенесення персональних даних: фізичні особи зможуть переносити свої персональні дані під час зміни провайдерів послуг;
- необхідність призначати окремих фахівців або створювати окремі підрозділи для обробки персональних даних;
- більш жорстка відповідальність за порушення вимог до захисту персональних даних.

Наприклад, штраф у розмірі 10 мільйонів євро або 2 відсотків річного обігу (в залежності від того, що вище) буде стягнуто за порушення наступних положень Регламенту: ст. 8 (щодо умов отримання згоди неповнолітніх), ст. 11 (щодо обробки, яка не потребує ідентифікації), ст. 25-39 (що стосуються володільця та розпорядника, безпеки персональних даних, оцінки впливу обробки персональних даних та попередніх консультацій, призначення відповідального за безпеку персональних даних), 42 (правила сертифікації) та 43 (органи сертифікації), ст. 41 (4) обов'язків органу моніторингу.

Штрафом в розмірі 20 мільйонів Євро або 4 відсотків річного обігу (в залежності від того, що вище) буде каратись порушення положень Регламенту, що стосуються:

а) основних принципів обробки персональних даних, в першу чергу згоди (ст. 5), легітимності обробки (ст. 6), умов отримання згоди (ст. 7) та обробки особливих категорій персональних даних (ст. 9);
б) прав суб'єкта даних, що визначені ст. 12-22;

в) правил трансферу персональних даних у треті країни або міжнародним організаціям (ст. 44-49);
г) положень щодо специфічних ситуацій обробки (Глава IX);
д) невиконання наказів чи вимоги контролюючого органу щодо обмеження обробки або припинення переміщення даних (ст. 58(2)), або ненадання доступу (ст. 58(1)).

В усіх відповідних документах ЄС вказується, що реформа системи правового регулювання захисту персональних даних має безпосереднє відношення до врегулювання питань кіберзахисту та забезпечення мережевої та інформаційної безпеки. Саме тому ці питання не можна розглядати окремо одне від одного.

3.3. Що це означає для України?

16 вересня 2014 року Верховна Рада України ратифікувала Угоду про асо-ціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони. Ця Угода вимагає наближення українського законодавства до права Європейського Союзу.

http://zakon2.rada.gov.ua/laws/show/984_011

На час підписання Угоди ані Директива NIS, ані GDPR ще не були ухвалені, тому в Угоді нема чіткого припису щодо необхідності імплементувати ці норми в українське законодавство. Однак у Статті 3 Додатку XVII (Нормативно-правове наближення до набуття повного режиму внутрішнього ринку в конкретному секторі) зазначено:

1. Згідно зі статтями 114, 124, 133 та 139 Глави 6 «Заснування підприємницької діяльності, торгівля послугами та електронна торгівля» та Глави 7 «Поточні платежі і рух капіталу» Розділу IV цієї Угоди та статті 2(1) цього Додатка, Україна транспонує і на постійній основі впроваджує чинне законодавство ЄС, зазначене у Доповненнях, у свою національну правову систему відповідно до статті 2(2) цього Додатка.
2. З метою забезпечення правової визначеності Сторона ЄС інформуватиме Україну та Комітет з питань торгівлі на постійній основі у письмовій формі про всі нові законодавчі акти або зміни до законодавства ЄС у конкретному секторі.
3. Комітет з питань торгівлі вносить протягом трьох місяців будь-який новий або змінений законодавчий акт ЄС до Доповнень. Як тільки новий або змінений законодавчий акт ЄС буде додано до відповідного Доповнення, Україна транспонує законодавство до своєї національної правової системи відповідно до статті 2 (2) цього Додатка. Комітет з питань торгівлі також ухвалює рішення про орієнтовний період транспонування законодавчого акта.
4. У випадку, якщо Україна передбачає виникнення особливих складностей із транспонуванням законодавчого акта ЄС до свого національного законодавства, вона повинна невідкладно поінформувати Європейський Союз та Комітет з питань торгівлі. Комітет з питань торгівлі

може вирішити, чи може Україна у виняткових випадках бути частково або тимчасово звільнена від виконання своїх зобов'язань щодо транспонування відповідно до статті 3(3) цього Додатка.

5. У випадку, якщо Комітет з питань торгівлі надасть таке часткове звільнення від виконання своїх обов'язків на підставі статті 3(4) цього Додатка, Україна повинна на постійній основі звітувати про прогрес, досягнутий щодо транспонування відповідного правового акта ЄС.

Звичайно, зараз вкрай необхідно отримати інформацію про те, чи інформувала Сторона ЄС Україну та Комітет з питань торгівлі на постійній основі в письмовій формі про ці зміни в законодавстві ЄС (Директива NIS та GDPR). І, якщо так, то які з підрозділів української державної влади мають відповідати на ці повідомлення. Але навіть за відсутності такої інформації надзвичайно небезпечно вдавати, що відсутність цих пунктів в УПА має вберегти українську сторону від відповідальності за порушення європейського законодавства. І в Директиві NIS, і в GDPR наголошується на тому, що відповідальність за порушення цих нормативів нестимуть не тільки ті підприємства, що розташовані в межах Євросоюзу, але й ті, що розташовані поза цими межами, але мають стосунок до обробки персональних даних громадян ЄС або до забезпечення кібербезпеки громадян ЄС.

Відсутня офіційна інформація про плани розвитку питання кібербезпеки в Україні.

Сьогодні відсутня офіційна інформація про плани України вносити Директиву і Регламент в Додатки Угоди. Але Бісик Ірина Олександрівна, заступник керівника Управління з питань захисту персональних даних Уповноваженого Верховної Ради України з прав людини, під час телефонного спілкування повідомила, що апарат Уповноваженого зараз готує неофіційні переклади цих документів і буде створювати Робочу групу з наближення українського законодавства до європейських стандартів у сфері захисту персональних даних. Власне, така група вже була створена і навіть мала певні напрацювання, але, через зміну керівництва, цю роботу доведеться починати з нуля. Якщо зважити ще на переобрання Уповноваженого з прав людини, то завершення цієї роботи може відкластись на дуже довгий термін. Ситуація ускладнюється ще й тим, що за Угоду про Асоціацію відповідає Кабінет Міністрів України, який жодного стосунку до апарату Уповноваженого з прав людини не має. З іншого боку, важливість питання захисту персональних даних суттєво зросла після надання Україні безвізового режиму. Тому, можливо, це питання має бути піднято в рамках Платформи Громадянського Суспільства Україна – ЄС.

4. Як це питання вирішується в інших країнах (best practices)

BSA (Business Software Allience – міжнародна торговельна асоціація, створена 1988 року виробниками програмного забезпечення) розробила для країн-членів Євросоюзу матрицю кібербезпеки (EU Cybersecurity Dashboard)

http://cybersecurity.bsa.org/assets/PDFs/study_eucybersecurity_en.pdf

Надзвичайні події в кіберпросторі, що стають все частішими та масштабнішими, висувають питання кібернадійності та захисту критичної інфраструктури від кіберінцидентів на перший план. Для вирішення цих питань необхідно, аби і державні, і приватні стейкголдери були достатньо оснащені для того, щоб запобігати, мінімізувати та належним чином реагувати на кіберінциденти. Оцінити рівень цієї оснащеності можна за наступними критеріями:

- наявність та якість нормативно-правової бази;
- операційні можливості;
- державно-приватне партнерство;
- наявність окремих планів для окремих секторів;
- освіта.

Автори цієї матриці не виставляли окремим країнам-членам ЄС бали та не ранжували їх за місцями в рейтингу з кібербезпеки, лише зазначили, що поки що існує всього п'ять країн, в яких діють всі п'ять компонентів забезпечення кібербезпеки. Інформація щодо "гарячих ліній" взята з сайту inhope.org, що об'єднує "гарячі лінії" Європи та всього світу.

Австрія

Австрійська Стратегія кібербезпеки була ухвалена 2013 року. Вона є частиною більш загальної Національної стратегії з безпеки інформаційно-комунікаційних технологій. Стратегія являє собою деталізовану програму дій, в якій визначено завдання з кібербезпеки та безпеки інформаційно-комунікаційних технологій та заходи, що необхідні для їх досягнення. Національна команда реагування на надзвичайні комп'ютерні події CERT.at має широкі та дуже чітко прописані повноваження.

У країні існує декілька інституціалізованих (та багато неформальних) державно-приватних партнерських ініціатив (таких, наприклад, як Австрійський центр безпеки інформаційних технологій – Centre for Secure Information Technology Austria/A-SIT та Kuratorium Sicheres Österreich).

Окрім того, існує Austrian Trust Circles, метою якого є обмін інформації щодо захисту критичної інформаційної структури за окремими секторами економіки та розробки специфічних для окремих секторів планів з оцінки ризиків. Austrian Trust Circles є спільною ініціативою CERT.at та австрійського уряду. Існує також "гаряча лінія" stopline.at, куди можна поскаржитись на дитячу порнографію, онлайн пропаганду символіки націонал-соціалізму та інший небажаний контент.

Франція

Національна стратегія кібербезпеки з'явилась у Франції 2011 року. Особлива увага приділяється в цьому документі питанням захисту та національної безпеки.

Існує Національне агентство з безпеки інформаційних систем (ANSSI), яке тісно інтегроване з командою реагування на надзвичайні комп'ютерні події CERT-FR. В Стратегії кібербезпеки містяться рекомендації із забезпечення міцної співпраці з приватним сектором.

ANSSI регулярно оприлюднює перелік конкретних заходів із забезпечення кібербезпеки для окремих секторів економіки, що робить досвід цієї країни унікальним у межах Європейського Союзу.

На "гарячу лінію" pointdecontact.net можна поскаржитись на дитячу порнографію, пропагування самогубства, спонукання до насильства, дискримінації або ворожнечі, пропагування тероризму, виправдання злочинів проти людства.

Нідерланди

Нідерланди, за оцінками BSA, мають найрозвиненішу та "зрілу" систему кібербезпеки, як з точки зору правового забезпечення, так і з технічної та організаційної точки зори. Нідерланди кожні два роки переглядають свою Національну Стратегію кібербезпеки, а Національний Центр кібербезпеки, який являє собою національний CERT з додатковими повноваженнями, розробляє та впроваджує усі процедурні та технологічні питання, що стосуються до кібербезпеки. Цей же Центр активно співпрацює з Аналітичними та інформаційними центра-ми (ISACs), які відповідають за безпеку критичної інформаційної інфраструктури за секторами.

"Гаряча лінія" meldpunt-kinderporno.nl була ініційована голландськими Інтернет-провайдерами для боротьби з дитячою порнографією як приватна структура, але згодом отримала підтримку Міністерства юстиції Нідерландів. До речі, саме з Нідерландів почалась історія створення загальноєвропейської мережі "гарячих ліній" – InHope.

Іспанія

Іспанія ухвалила Національну Стратегію з кібербезпеки 2013 року. Це дуже якісний документ, який визначає конкретні цілі та засоби їх досягнення. Ця Стратегія є добре узгодженою як з Планом з національної безпеки, так і з чинним законодавством в галузі кібербезпеки – Стратегія, План та окремі законодавчі акти працюють разом в єдиному пакеті.

У Іспанії працюють два CERT-и – INTECO-CERT та CCN-CERT, створено Національний Центр із захисту критичної інфраструктури (CNPIC). Цей Центр є державною структурою, яка відповідає за інформаційну безпеку та кібербезпеку, тоді як роль CERT-ів зводиться до реагування на інциденти кібербезпеки. CNPIC відповідає також за поширення інформації щодо кіберзагроз та кіберінцидентів та забезпечує координацію та співпрацю між різними секторами економіки та між державними та приватними інституціями. Він створює також робочі групи, які розробляють секторальні плани з кібербезпеки.

У країні існує "гаряча лінія" для захисту дітей від шкідливого контенту, для підвищення обізнаності щодо ризиків кібербепеці, щодо налагодження співпраці між різними стейкголдерами щодо забезпечення кібербезпеки. Цікаво, що, аби потрапити на сайт цієї "гарячої лінії", потрібно зареєструватись (www.alia2.org/alerta2/english.php).

Велика Британія

Велика Британія розробила свою комплексну стратегію кібербезпеки 2011 року. Її виконання забезпечується ефективною правовою базою та наявністю двох CERT-ів: CERT-UK підтримує операторів, які захищають критичну інфраструктуру, а GovCertUK працює з державними установами. Окрім цього, існують Національна рада Безпеки та Офіс страхування з питань кібернетичної та інформаційної безпеки (Office of Cyber Security and Information Assurance).

У країні існує добре розвинена система державно-приватного партнерства, яке є частиною Стратегії з кібербезпеки. Наприклад, Центр захисту національної інфраструктури (CPNI), організує для компаній, що працюють в 14 секторах економіки, регулярні обміни інформацією та кращими практиками.

"Гаряча лінія" Internet Watch Foundation є однією з найстаріших у Європі. Саме у Великій Британії розташована штаб-квартира загальноєвропейської мережі "гарячих ліній" InHope.

Методологія, яку використовує BSA, досить добре корелює з тою, яка застосована Міжнародним Союзом Електрозв'язку в процесі розробки Global Cybersecurity Index

https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf

Правда, МСЕ, зафіксувавши наявність чи відсутність ключових компонентів (правові засади, технічні можливості, організаційні заходи, підвищення компетентності/нарощування потенціалу, партнерство) виставила усім країнам відповідні бали та створила відповідний рейтинг з кібербезпеки. Усі п'ять країн, що згадувалися в матриці BSA, потрапили до першої європейської десятки Global Cybersecurity Index, але на першому місці серед європейських країн опинилась Естонія (з точки зору BSA цій країні бракує інституціалізованого державно-приватного партнерства).

Естонія

Естонія однією з перших у світі (2008 року) ухвалила національну Стратегію кібербезпеки і переглянула її 2014 року. Ця Стратегія також підкріплена потужним пакетом законодавчих актів, що стосуються як кібербезпеки, так і інформаційної безпеки. В Естонії добре працює CERT Estonia, підпорядкований Адміністрації інформаційних систем. Значно сприяє підвищенню рівня кібербезпеки Естонії розташування в Таллінні Центру кібербезпеки НАТО.

"Гаряча лінія" vihjeliin.ee існує з 2011 року з метою боротьби з розповсюдженням дитячої порнографії, торгівлі дітьми та іншого нелегального контенту.

5. Альтернативні варіанти

5.1. Нічого не робити

Наразі правові засади кібернетичної безпеки України врегульовані перш за все Конвенцією Ради Європи з кіберзлочинності та Стратегією кібербезпеки.

Конвенція з кіберзлочинності ратифікована Україною не в повному обсязі, і це створює багато проблем (особливо з точки зору процедурного права). І українські, і європейські експерти наполягають на необхідності внесення змін до чинного українського законодавства з метою належної імплементації Конвенції.

Стратегія кібербезпеки України ухвалена Указом Президента України на підставі відповідного рішення Ради національної безпеки та оборони України. Правові акти Президента України є підзаконними, оскільки ухвалюються на основі та в межах Конституції і законів України.

Відсутність в українському законодавстві необхідної термінології, невизначеність питань щодо розподілу повноважень між різними державними та приватними установами в сфері кіберзахисту, відсутність законодавчо врегульованої та фінансово забезпеченої стратегії державно-приватного партнерства, невирішеність багатьох процедурних питань щодо дій правоохоронних та контролюючих органів, а також недостатня увага, що приділяється проблемам загальної освіти з кібербезпеки, підвищення обізнаності, нарощуванню потенціалу значно підвищують вразливість України перед кіберінцидентами та кібератаками. Необхідність законодавчого врегулювання перелічених питань вимагає прозорості законодавчого процесу, плідної співпраці українських та міжнародних стейкголдерів, сприяння підвищення довіри між ними.

5.2. Ухвалити Закон про засади кібербезпеки України (2126а)

Необхідність в ухваленні якісного Закону про кібербезпеку України є очевид-ною для всіх. Сьогодні такий закон (і навіть такий законопроект) в Україні відсутній. У Верховній Раді з 2015 року зареєстровано законопроект 2126а (Про засади кібербезпеки України). Попри багаторазове (непрозоре, з порушеннями Регламенту) його переписування він жодним чином не вирішує питання, які потребують законодавчого врегулювання. Цей законопроект не викликає спротиву лише в частині, де використовуються прямі запозичення з тексту Стратегії кібербезпеки. Проте не зважаючи на жорстку критику і негативні висновки українських та міжнародних експертів, цей законопроект очікує на повторне друге читання. Ухвалення законопроекту 2126а в чинній редакції (навіть без врахування загрози внесення правок з голосу) гальмує (або навіть повертає назад) роботу над створенням системи кібербезпеки України.

5.3. Ухвалити Закон про засади кібербезпеки України і розпочати роботу над підготовкою Закону про кібербезпеку України

Ухвалення законопроектів є результатом торгів між різними фракціями. Наразі голосування за законопроект 2126а є розмінною монетою задля вирішення інших стратегічних питань. Чи є сенс досягати такого результату і знов розпочинати цей процес (процес торгів) з нуля? Яким чином буде розвиватись ситуація в разі проведення довчасних виборів у Верховну Раду України? Чи будуть виконані домовленості, що досягнуті зараз, навіть у разі вчасного закінчення цієї каденції Верховної Ради?

5.4. Імплементувати Конвенцію РЄ про кіберзлочинность, провести через Верховну Раду України Стратегію кібербезпеки України, доповнити Угоду про асоціацію Директивою NIS та GDPR та розпочати роботу над їх імплементацією в українське законодавство

У рамках виконання проекту Ради Європи та Європейського Союзу "Кіберзлочинність@Східне партнерство" готується проект змін до Кримінально-процесуального кодексу України з метою належної імплементації Конвенції про кіберзлочинність. Прийняття цього законопроекту дозволить усунути одну з найбільших невідповідностей українського законодавства до європейського в сфері кібербезпеки, а саме – відсутності в українському законодавстві поняття "електронні докази". Очікується, що цей законопроект також врегулює взаємовідносини між правоохоронними органами та провайдерами, а також між правоохоронними органами та розвідкою та контррозвідкою. Поки що цей законопроект не було винесено на публічне обговорення, але європейські експерти, що залучені до його розробки, вже підтвердили свою участь у Восьмому Українському Форумі з управління Інтернетом (6 жовтня 2017 року).

Намагання законодавців переписати "Засади кібербезпеки" у відповідності з власними політичними та економічними інтересами можуть надовго загальмувати процес розбудови системи кібербезпеки в Україні. Аби цього не сталось, пропонується в наявний текст Стратегії кібербезпеки України додати розділи, яких потребує законодавче врегулювання питань становлення системи кібербезпеки на початковому періоді, а саме, термінологію та зміни до чинного законодавства України, без яких належна імплементація Стратегії неможлива. Робота над цими розділами є надзвичайно складною, і потребує залучення вітчизняних та міжнародних фахівців найвищого рівня.

Під час доопрацювання Стратегії необхідно орієнтуватись на вимоги до національних стратегій кібербезпеки, які прописані в ст. 7 Директиви NIS. Зокрема щодо:

- створення державного каркасу системи кібербезпеки з чітким розмежуванням ролей та відповідальностей державних установ та інших стейкголдерів у сфері кібербезпеки;

- ідентифікації заходів, що забезпечують попередження, належне реагування та відновлення щодо кіберінцидентів, на засадах державно-приватного партнерства;
- акценту на освіту, підвищення обізнаності, навчально-тренувальних програмах із забезпечення безпеки мережевих та інформаційних систем;
- розробки плану науково-дослідних робіт та впровадження наукових розробок із забезпечення безпеки мережевих та інформаційних систем;
- розробки плану оцінки ризиків;
- створення переліку стейкголдерів імплементації національної стратегії кібербезпеки.

Наступним кроком має стати переклад та експертне опрацювання відповідного законодавства ЄС – Директиви NIS (а також оновленого тексту Стратегії кібербезпеки ЄС) та GDPR.

У відповідності до механізму, розробленого в Угоді про асоціацію між Україною та ЄС, необхідно розробити Дорожню карту імплементації цих документів у законодавство України, скласти таблицю транспонування (щодо кожної зі статей документів), визначити назву того українського законопроекту, в який мають бути внесені зміни (або які мають бути створені заново). І тільки на підставі результатів такої роботи належить приступати до написання повноцінного Закону про кібербезпеку України (а краще навіть вже в назві Закону підкреслити його європейське спрямування – щодо мережевої та інформаційної безпеки).

Звичайно, виконати весь цей обсяг роботи (та ще й провести отримані законопроекти через Верховну Раду України) до травня 2018 року неможливо. Тому вже зараз українська сторона має розпочати переговори щодо запровадження пільгового періоду для України (на якийсь зрозумілий термін).

Паралельно з цим необхідно організувати закриті та відкриті дискусії з основними стейкголдерами щодо:

- визначення державної структури (або державних структур), які будуть відповідальні за впровадження в Україні стандартів безпеки мережевих та інформаційних систем, визначення єдиного контактного центру з питань безпеки мережевих та інформаційних систем, взаємовідносини та розподіл повноважень між такою державною установою (установами), контактним центром та CSIRT(s). Наявність кількох державних структур може бути пов'язана з секторальною приналежністю таких структур. У випадку єдиної державної структури, відповідальною за безпеку мережевих та інформаційних систем, саме вона і має бути єдиним контактним центром. Такий контактний центр та така державна установа мають співпрацювати (на визначених на законодавчому рівні засадах) з CSIRT, правоохоронними органами та установою, що опікується захистом персональних даних;
- визначення критеріїв, за якими буде складатись перелік операторів базових послуг та провайдерів цифрових послуг;
- створення переліку операторів базових послуг та провайдерів цифрових послуг (у країнах-членах ЄС цей процес має бути завершеним до

9 листопада 2018 року);

- визначення критеріїв "значної руйнівної дії" з урахуванням надання послуг у зазначених секторах економіки (див. 3.1), кількості користувачів сервісу конкретного оператора чи провайдера, залежності інших важливих секторів економіки від сервісу конкретного оператора чи провайдера, впливу (з урахуванням масштабу та тривалості) на соціально-економічну активність або громадську безпеку, ринкової частки оператора чи провайдера, географії поширення можливої руйнівної дії, ролі конкретного оператора в підтриманні конкретного сервісу на задовільному рівні з урахуванням альтернативних шляхів надання цієї послуги (усі ці критерії мають визначатись окремо для кожного з секторів економіки);
- стандартизації (від країн-членів ЄС вимагається дотримання мережевої нейтральності та міжнародних та європейських стандартів та забороняється введення окремих національних стандартів у сфері кібербезпеки, які не є сумісними з європейськими та міжнародними стандартами);
- механізмів запровадження системи мережевої та інформаційної безпеки та її аудиту (установа, що відповідає за імплементацію Директиви NIS, або незалежний сертифікований аудитор має отримати доступ до документації щодо оцінки ризиків та запровадження системи керування ризиками, а також оцінити ефективність такої системи. Водночас може вимагатись лише та інформація, яка є необхідною для проведення такого аудиту. В разі виявлення недоліків у цій системі оператора чи провайдера аудитор має вказати на них та зробити приписи щодо їх усунення. І тільки в разі невиконання цих приписів настає відповідальність за недотримання вимог мережевої та інформаційної безпеки);
- створення законодавчо-нормативної бази системи сповіщення про кіберінцидетни, системи аудиту та впровадження заходів мережевої та інформаційної безпеки.

Останній пункт потребує додаткового уточнення. У відповідності до вимог Директиви NIS передбачається два варіанти сповіщення про кіберінциденти – обов'язковий та добровільний. Обов'язковість сповіщення про кіберінциденти передбачається для тих операторів, що були внесені до офіційного переліку операторів базових послуг та операторів цифрових послуг, та відноситься до інцидентів, які підпадають під критерії "значної руйнівної дії". Інформація від таких провайдерів та щодо таких інцидентів має надсилатись до державної установи, що відповідає за імплементацію Директиви NIS, або до CSIRT. Якщо цей CSIRT створено при цій державній установі і вона ж сама є єдиним контактним центром, то проблем не має виникати. Якщо ж це окремі інституції, і CSIRT, і єдиний контактний центр повинні мати безперешкодний доступ до таких сповіщень. Після консультацій з операторами інформація про кіберінциденти може бути оприлюднена для громадськості, оскільки підвищення обізнаності про можливі ризики та запобіжні заходи є наріжним каменем розбудови системи кібербезпеки.

Окрім обов'язкового сповіщення передбачається також добровільне спові-

щення про кіберінциденти від тих операторів, що не входять до офіційного переліку операторів базових та провайдерів цифрових послуг, та щодо інцидентів, які не відповідають критеріям "значної руйнівної дії". На законодавчому рівні має бути закріплено, що інформація, що міститься в таких сповіщеннях (чи то обов'язкових, чи то добровільних) не має призводити до підвищеної відповідальності за наслідки кіберінцидентів.

Окремо необхідно зазначити вимоги щодо збереження конфіденційності. Найвищого рівню захист гарантований для персональних даних. Окремі вимоги передбачаються для захисту комерційних інтересів операторів та провайдерів. Директива NIS не стосується питання державних інтересів та національної безпеки, а також розслідування, викриття та переслідування кримінальних злочинів.

6. Перешкоди та шляхи подолання

6.1. Відсутність єдиного центру координації процесу розбудови національної системи кібербезпеки, непрозорість та незрозумілість цього процесу

Над законодавчим врегулюванням питань кібербезпеки України одночасно працюють декілька "центрів впливу":

- депутати Верховної Ради України (і це не тільки профільний комітет з питань інформатизації та зв'язку);
- Держспецзв'язку;
- інші державні установи;
- проект Ради Європи та Європейського Союзу "Кіберзлочинність@Східне партнерство";
- формальні та неформальні групи експертів.

Створення Національного координаційного центру кібербезпеки як робочого органу РНБОУ значно підвищує шанси на більш узгоджену співпрацю представників державних установ. Однак ані народні депутати, ані незалежні експерти до цього центру не входять, а результати його роботи не оприлюднюються.

Розширення Угоди про асоціацію між Україною та ЄС та створення в Урядовому офісі з питань європейської та євроатлантичної інтеграції спеціального підрозділу дозволило б систематизувати висновки українських та міжнародних експертів щодо різних проектів у галузі кібербезпеки, налагодити прямий контакт з експертами НАТО, ЄС, РЄ, ОБСЄ, інших організацій, зробити процес законотворчості більш прозорим, підзвітним та зрозумілим. Після проведення через Верховну Раду Стратегії з кібербезпеки та належної імплементації Конвенції з кіберзлочинності було б надзвичайно корисно ухвалити тимчасовий (щонайменше до травня 2018 року) мораторій на внесення законопроектів щодо кібербезпеки, аби забезпечити системне, методологічно обґрунтоване вирішення проблеми.

6.2. Відсутність загального розуміння наявного стану проблеми

Відсутність наявної достовірної статистики по Україні є дуже серйозним викликом для правильної діагностики і належного "лікування" проблем з кібербезпеки. Відсутність єдиного центру збору інформації щодо кіберінцидентів ускладнює правильну обробку результатів. Зрозуміло, що вся інформація з цього приводу не може бути відкритою. Але і ситуація, коли навіть рівень проникнення Інтернету в Україні за даними Міжнародного Союзу Електрозв'язку (44%) та Інтернет Асоціації України (66%) відрізняються між собою в півтора рази, не є нормальною.

http://www.internetlivestats.com/internet-users/ukraine/

http://osvita.mediasapiens.ua/mediaprosvita/research/dolya_regulyarnikh_internetkoristuvachiv_v_ukraini_zrosla_do_661/

6.3. Подолання недовіри між стейкголдерами

Забезпечення достатнього рівню кібербезпеки неможливе без плідної співпраці правоохоронних органів, постачальників послуг та користувачів. На жаль, довгий час в Україні існувала практика використання правоохоронних органів з метою знищення конкурентів. Нема впевненості і в тому, що такі випадки є неможливими зараз. У цих умовах сподіватись на ефективність саморегуляторних механізмів (хоча б на рівні "гарячих ліній" для скарг на кіберінциденти) і подальшої співпраці між постачальниками послуг та правоохоронними органами не доводиться.

Проведення належних розслідувань в правоохоронних органах з притягненням винних до відповідальності може допомогти у вирішенні цієї проблеми. З іншого боку, перші спроби справжньої саморегуляції з'явились під час консолідації постачальників послуг у їхній боротьбі з викрадачами телекомунікаційного обладнання. Якщо цей проект виявиться вдалим, він може закласти підвалини справжнього мультистейкголдеризму, без якого забезпечення кібербезпеки не є можливим. Дуже важливо, аби він також отримав відповідну підтримку з боку правоохоронних органів.

Не менш важливим є створення відповідних умов для розвитку індустрії кібербезпеки – як на фінансовому (пільги, проведення прозорих тендерів на бюджетне фінансування і таке інше) та організаційному рівні (затвердження прозорих та зрозумілих правил гри на цьому ринку). Корисним кроком у цьому напрямку може стати укладання відповідних меморандумів між гравцями ринку та державними установами, що відповідають за ці питання.

6.4. Просвітницька діяльність, підвищення обізнаності, нарощування потенціалу

Люди, процеси та технології є однаково важливими для забезпечення кібербезпеки. Навіть найкращі технології будуть неефективними, якщо будуть неправильно застосовуватись. Підвищення обізнаності, просвіта та навчання у відповідності до чітко визначених пріоритетів кібербезпеки, принципів, політики, процесів, програм є надзвичайно важливим компонентом забезпечення достатнього рівню кібербезпеки, і їм потрібно приділяти дуже багато уваги на усіх рівнях – політичному, законодавчому, регуляторному, бізнесовому, волонтерському. Найкращі світові практики показують, що культуру користування Інтернетом, інформаційну гігієну потрібно прищеплювати ще з дошкільного віку. Але роботою з дітьми обмежуватись не можна. Потрібно розробити окремі програми навчання та інформування для держслужбовців, правоохоронних органів, підприємців, представників громадських організацій, індивідуальних користувачів. Окремої уваги заслуговують люди похилого віку.

АНОТАЦІЯ

Робота присвячена аналізу проблем у сфері кібербезпеки України та пошукам шляхів їхнього вирішення. Увагу авторів було зосереджено на вдосконаленні нормативно-правової бази, створенні належної інфраструктури, розвитку індустрії кібербезпеки, забезпеченні умов для плідної співпраці всіх українських та міжнародних стейкголдерів, розвитком культури мережевої та інформаційної безпеки. На думку авторів, побудова ефективної державної політики у сфері кібербезпеки можлива лише за наявності єдиного «центру управління», чіткої узгодженої програми дій та підвищенні рівня довіри між основними стейкголдерами.

ABSTRACT

The paper is devoted to the analysis of problems with cybersecurity in Ukraine and to the search for ways to solve them. The authors' attention was focused on improving the regulatory framework, creating the proper infrastructure, developing the cybersecurity industry, ensuring conditions for the fruitful cooperation of all Ukrainian and international stakeholders, and developing a culture of network and information security. According to the authors, the construction of effective state policy in the field of cybersecurity is possible only if there is a single control center, a clear agreed program of action and increased confidence among the main stakeholders.

Михайло Кольцов – технічний консультант з питань відкритих даних та обробки інформаційних масивів, експерт Лабораторії законодавчих ініціатив

Оксана Приходько – директорка міжнародної громадської організації «Європейська Медіа Платформа»

Єгор Аушев – Керівник проекту Cyber Guard, співзасновник HACKEN