Аналітична доповідь

АТАКИ ЧЕРЕЗ ЛАНЦЮЖКИ ПОСТАЧАНЬ: ФОРМУЮЧИ СТРАТЕГІЧНУ ВІДПОВІДЬ

(версія для експертного обговорення)

ВСТУП

Повномасштабна війна, розв'язана РФ проти України 24 лютого 2022 р., загострила для нашої держави ключове екзистенційне питання – виживання країни. Цілком очікувано це змістило фокус уваги на суто військовий складник бойових дій. Водночас кіберскладник не зникає і так само, як і до війни, є важливим елементом агресії Росії проти України та її союзників. Так, протягом січня – лютого 2022 р. численні російські кібератаки мали очевидну підготовчу мету – ослабити українські ІТ-системи, посіяти хаос, відвернути увагу фахівців та паралізувати державні послуги.

Ця ситуація не змінилася й після 24 лютого. Українські державні структури відзначають кратне зростання кількості кібератак проти України, майже щодня Держспецзв'язку повідомляє про нові виявлені кібератаки та кіберінциденти. Компанія Microsoft у своєму звіті вказала на очевидний зв'язок між російськими кібератаками та наземними операціями. Цей же звіт засвідчує: проводячи підготовчі кібероперації, російські хакери активно використовували так звані ***атаки через ланцюжки постачань*** (англ. – *supple chain attacks*, далі – АчЛП)*.

Для України та світу цей тип атаки не є новим, але від цього не стає менш загрозливим. Вірус *NotPetya*, атаки на компанії – американську *SolarWinds,* ізраїльську *Amital Data,* монгольські *Able Software, Kaseya, Codecov*, на в'єтнамський урядовий центр сертифікації та українські урядові сайти в січні 2022 р. – їх усі об'єднує саме цей спільний тип атак – АчЛП.

Проблема буде лише загострюватись у часі: кількість під'єднаних пристроїв (*IoT*) лише зростає, програмні продукти стають дедалі складнішими, нові швидкості передавання даних спрощують приховування зловмисного коду в легальному трафіку. Складність та багатовимірність виробничих процесів у сфері ІТ, необхідність взаємодіяти з численними підрядниками, які надають хоч і обмежені за обсягом, але важливі для функціонування організацій послуги, посилення взаємозалежності різних компаній – усе це радикально множить вектори кібератак. Для України парадоксальним фактором загострення цієї проблеми стає употужнення її кібербезпеки, зокрема через надання допомоги в цій сфері з боку партнерів. Адже тепер ворожі хакери будуть шукати менш захищені об'єкти для атак, які дадуть можливість виводити з ладу захищеніші цілі.

Побудова захисту від АчЛП – одне з найдискусійніших питань, зважаючи на комплексність загрози й на те, скільки елементів може зачепити цей процес. Вочевидь, пошук системного рішення захисту від АчЛП може поставити під сумнів чинну модель надзвичайної відкритості ІТ-систем, змінити юридичний статус деяких програмних продуктів, спонукати розвиток ринку кіберстрахування та сертифікації і багато іншого.

Ця доповідь має на меті розглянути поточний стан проблеми АчЛП, можливі напрями пошуку українського рішення та розпочати експертну

* Сучасний ланцюжок постачань – це певна екосистема ресурсів, необхідних для розроблення, виробництва та поширення продукту. В ІТ-сфері ланцюжок постачань містить апаратне та програмне забезпечення, хмарні або локальні механізми зберігання та розподілу. Суть ідеї АчПЛ якраз і полягає в компрометації (ураженні) добре захищеного об'єкта через менш захищених постачальників. Шкідливий контент «підсаджують» у замовлене об'єктом ПЗ постачальника, після чого він через т. зв. довірене з'єднання ланцюгами постачань потрапляє до системи жертви.

дискусію щодо випрацювання національного підходу до проблеми протидії АчЛП.

І. АТАКА ЧЕРЕЗ ЛАНЦЮЖОК ПОСТАЧАНЬ У ПРОСТОРІ КІБЕРЗАГРОЗ, ЯКІ ЗРОСТАЮТЬ

Сьогодні загрози кібербезпеці організацій стрімко зростають: атаки може бути здійснено значною кількістю способів, а деякі з атак мають особливу небезпеку через їхню прихованість, масштабність, мультиплікативність та спроможність завдавати довгострокової шкоди. Однією з таких атак є АчЛП. Значні збитки від них, а також складність атрибуції та нейтралізації звели їх у статус однієї з найнебезпечніших глобальних кіберзагроз. Це актуалізує проблему випрацювання системних політик та стратегій спільних дій на рівні урядів і міжнародних альянсів.

Суттю такого типу атак є проникнення в телекомунікаційні мережі атакованого об'єкта (переважно – добре захищеного) не шляхом зламу його захисних систем, а через допоміжні системи підрядників, які або вже були перевірені справжнім об'єктом атаки (і визначені як «довірені з'єднання»), або взагалі не проходять таку перевірку. Цим атакам складно запобігти не лише через дедалі більшу кількість підрядників та кількість сторонніх систем, які використовують навіть найзахищеніші суб'єкти, але й часто через відсутність особливих вимог до кібербезпеки таких підрядників. Життєвий цикл АчЛП багато в чому збігається з так званими APT-атаками (*Advanced Persistent Threats – APTs*) – складними, багатоетапними заходами, до яких вдаються хакерські угруповання, аби вести свої кібероперації (з метою вимагання викупу чи шпигунства) проти найзахищеніших цілей.

Бачимо чітку тенденцію сталого зростання складності та масштабності (за наслідками) таких атак протягом останніх років. У липні 2021 р. Агентство Європейського Союзу з кібербезпеки (*ENISA*) оприлюднило доповідь **«Ландшафт загроз від атак через ланцюжки постачань» (***Threat Landscape for Supply Chain Attacks*)[1]. У дослідженні заналізовано 24 атаки та зроблено загальний висновок, що навіть найдосконаліших систем кібербезпеки недостатньо для захисту організацій в умовах розгортання нинішньої хвилі АчЛП. У звіті прогнозують також, що **за підсумками 2021 р. кількість атак на ланцюги постачань зросте в 4 рази проти 2020 р.**[2] Про те, що зростає ризик збільшення кількості кібератак, свідчить і звіт *Microsoft* 2022 р. На їхню думку, продовження російсько-української війни та її кіберскладника буде призводити до «ймовірнішого використання резервних можливостей (*highly reserved capabilities*), як-от вразливості «нульового дня», атаки на ОКІ чи *supply-chain attacks*»[3].

Ключова загроза від таких атак – можливий т. зв. каскадний ефект, або «ефект доміно»: ланцюгова реакція, спричинена однією атакою на одного постачальника, може в перспективі поставити під загрозу цілу мережу постачальників, а з ними й відповідну кількість споживачів. Часто АчЛП – це складні багатоетапні операції, які можуть тривати місяцями. Вплив нападів на постачальників може мати **далекосяжні наслідки** через збільшення взаємозалежності та складності використовуваних методів. Окрім завдання величезних збитків і створення широкомасштабних сталих загроз, зловмисники можуть **отримати стратегічну секретну інформацію** (кібершпигунство) **– під загрозою опиняється національна безпека держав або й**

[1] Див.: URL: https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks
[2] Там само.
[3] Див.: URL: https://cutt.ly/nGKYY4s

міжнародна безпека. У доповіді міститься ретельний аналіз емпіричних та цифрових даних, запропоновано також низку конкретних рекомендацій для постачальників і споживачів щодо управління ризиками кібербезпеки ланцюга постачань[4].

Протягом 2020 – 2021 рр. сталося декілька значних АчЛП, які в поєднанні зі здирницьким програмним забезпеченням (ПЗ) (*ransomware*) створили низку важливих прецедентів, чим привернули до себе увагу політичного керівництва низки держав.

Найбільш успішною та масштабною АчЛП стала атака ***Sunburst***[5]**,** яку виявлено в грудні 2020 р. (за не повністю підтвердженими даними, атака розпочалась у березні 2020 р.). На початку грудня одна з найвідоміших у світі компаній з кібербезпеки *FireEye* заявила про те, що її системи зламали невідомі хакери (найімовірніше – спонсоровані державою). Можливою, серед інших, ціллю атаки на *FireEye* було викрадення так званих «інструментів червоної команди» (*red team*) – набору хакерських програм, що їх використовують для тестування компаній-замовників на уразливості. Як одна з провідних компаній (із тісними контактами з американськими безпековими органами) *FireEye* мала чи не найефективніші з таких інструментів.

Вже за тиждень стало відомо, що *FireEye* є лише однією з багатьох постраждалих сторін – так само атакованими виявилися Пентагон, Міністерство фінансів США, Міністерство торгівлі США, Міністерства національної безпеки та інші урядові структури (усього до 250 державних установ), а також такі приватні компанії, як *Cisco, SAP, Intel, Deloitte, Nvidia, Fujitsu, Amazon*. За даними *Microsoft*, зловмисники намагались отримати доступ до хмарних сховищ атакованих компаній і організацій (зокрема для отримання доступу до їхнього електронного листування).

Атака стала можливою завдяки тому, що хакери зламали техаську ІТ-компанію ***SolarWinds,*** що створила та продавала для понад 36 тис. своїх клієнтів програмне забезпечення *Orion*. Це ПЗ дає можливість ефективніше управляти інформаційними системами організації і мало доступ до всіх внутрішніх мереж клієнтів. Хакери, так само як і з *NotPetya*, модифікували регулярне оновлення цього ПЗ, що дало їм можливість упровадити шкідливе ПЗ до частини цих клієнтів (попередньо – близько 18 тис. компаній), оминаючи всі системи кібербезпеки[6]. Відзначмо: компанія, за деякими даними, не приділяла належної уваги своїй кібербезпеці. Наприклад, сервер оновлень ПЗ *Orion* мав пароль «*solarwinds123*», а рекомендації власного директора з кібербезпеки Яна Торнтона-Трампа (*Ian Thornton-Trump*) було проігноровано, через що він покинув компанію. Хоча деталі того, як саме було зламано *SolarWinds,* все ще не відомі, серед версій є така – впровадження вірусу відбулося під час доопрацювання ПЗ одним з аутсорсових підприємств компанії, що розташовані в Чехії, Польщі та Білорусі.

Ця атака має всі ознаки «спонсорованої державою», про що свідчить не лише відсутність навіть спроб вимагання викупу, але й специфіка діяльності самих хакерів: унаслідок атаки вони отримали доступ до 18 тис. компаній, проте їхня

---

[4] Там само.

[5] Таку назву шкідливому програмному забезпеченню хакерів дали в FireEye – тепер її використовують на означення всієї атаки.

[6] За даними видання “heise online”, компанія SolarWinds у своїх рекомендаціях для клієнтів додатково пропонувала їм під час оновлення ПЗ відмикати антивірусні засоби. Див.: URL: https://www.heise.de/news/l-f-SolarWinds-Backdoor-Hersteller-sorgte-fuer-Ausnahmen-von-AV-Ueberwachung-4990910.html

реальна активна діяльність зосередилася лише на 40 – 50 з них – переважно урядових, великих ІТ-компанії. До останніх належить і *Microsoft*. На початок 2021 р. відомо, що зловмисники змогли отримати доступ до частини вихідного коду *Microsoft Windows*.

Окрім цієї атаки, протягом кінця 2020 р. стало відомо про ще декілька аналогічних випадків (щоправда, жоден з них не мав такого самого масштабу, як *Sunburst*):

- атака на ізраїльську компанію – розробника програмного забезпечення *Amital Data*. Унаслідок зламу її сервера хакери отримали змогу атакувати близько 40 клієнтів *Amital Data* – ключових логістичних компаній Ізраїлю. Компанії заявили про крадіжку інформації, але жодних спроб вимагати викуп за неї не надходило;

- невідомі хакери атакували В'єтнамський урядовий центр сертифікації (*Vietnam Government Certification Authority – VGCA*), який видає цифрові сертифікати громадянам та представникам бізнесу для підпису електронних звернень на адресу державних структур. Хакери скомпрометували програму, яка давала змогу підписувати відповідні документи, а отже, громадяни, звантажуючи цю програму з довіреного ресурсу (урядового сайту), заражали свої комп'ютери вірусом-бекдором;

- хакери змогли отримати доступ до сервера монгольської ІТ-компанії *Able Software*, яка є розробником ПЗ *Able Desktop*. Це система миттєвого обміну повідомленнями, якою користується багато місцевих державних службовців та державних установ. Завдяки цьому зловмисники змогли вбудувати шкідливе ПЗ в оновлення програми та встановити його на пристрої клієнтів.

У двох останніх випадках експерти покладають провину на китайських хакерів.

Водночас ці атаки лише чіткіше окреслюють ситуацію зі зламом *SolarWinds* – їхній випадок не є винятковим з погляду загальних тенденцій і вирізняється лише масштабами атаки.

До цього часу достеменно не відомо, хто саме стоїть за зламом. Майже всі американські коментатори (як з приватного, так і з державного секторів) покладають провину за цю кібератаку на РФ (мало того, указують на конкретну хакерську групу *APT29*, або «*Cozy Bear*», яку пов'язують із ФСБ РФ), але доказів цього не наводять. Ще одна версія – діяльність китайських хакерів, адже атака має спільні риси з АчЛП 2017 р. проти популярного ПЗ *CCleaner* (продукт компанії *Piriform*, яку за місяць до атаки купила відома антивірусна компанія *Avast*). Тоді хакерам вдалося через оновлення програми ПЗ *CCleaner* установити шкідливе ПЗ на комп'ютери понад 2,2 млн користувачів програми. Як і в разі з *SolarWinds*, хакери не намагалися працювати зі всіма зараженими комп'ютерами, а шукали конкретні компанії (зі сфери телекомунікацій та новітніх технологій) та інформацію на них. Цю атаку приписують не російським хакерам, а китайському кіберугрупованню *APT17* («*Axiom*»).

2021 р. відбулося щонайменше декілька потужних АчЛП, що мали значний уплив на сприйняття цієї загрози з боку найвищого політичного керівництва одразу декількох країни (передусім США).

Найзначніший з таких нападів – кібератака в червні 2021 р. на *Kaseya*[7]. Компанія виробляє програму для віддаленого контролю за великими флотиліями комп'ютерів у гігантських територіально розподілених ІТ-інфраструктурах (*VSA*).

[7] Див.: URL: https://www.digitalshadows.com/blog-and-research/kaseya-ransomware-supply-chain-attack/

Користуються нею великі транснаціональні корпорації та *MSP* (*Managed Service Providers*) – компанії, які надають послуги IT-адміністрування меншим організаціям[8]. Успішна первинна атака на ланцюг постачання програми дав можливість хакерам захопити контроль над кількома сотнями організацій корпоративних користувачів *VSA*. Після цього кількість уражених комп'ютерів росла в геометричній прогресії та досягла десятків тисяч ще до закінчення довгих вихідних у США. Відповідальність за кібератаку взяло на себе угруповання *REvil*, яке систематично поширює програми-здирники (*ransomware*). Сума викупу за розшифровку даних – 70 млн дол. (достеменно не відомо, чи було їх виплачено). Водночас ця атака привела до діалогу на найвищому політичному рівні (між президентами США та РФ) і до поступової ліквідації угруповання (спочатку в липні 2021 р. стало відомо[9] про зникнення інфраструктури *REvil* з мережі Інтернет, а в січні 2022 р. російські ЗМІ повідомили про арешт членів угруповання, хоча є сумніви, що заарештовано саме керівників, а не людей, які займались фізичним отриманням коштів від такої діяльності[10]).

У квітні 2021 р. був ще один визначний інцидент – з компанією *Codecov*[11]. Зловмисники здійснили злам інструменту для розроблення ПЗ фірми *Codecov – Bash Uploader*. Через унесені модифікації в код цього ПЗ (та його оновлень) зловмисники отримали можливість просочитися в сотні мереж клієнтів *Codecov*. Масштаби вражень не з'ясовано, але деякі компанії – користувачі продукту заявили про ймовірний вплив на них цього зламу.

Хай би які саме хакерські угруповання (а подеколи – держави) стояли за цими атаками, вони оприявнили низку важливих тенденцій:

1. Досвід попередніх атак методом АчЛП досі здебільшого не вивчено. Усі атаки 2020 р. зреалізовано за схожим принципом, а отже, майже ніхто не зміг зробити належних висновків і перебудувати свої системи кіберзахисту для уникнення таких атак у майбутньому.

2. АчЛП стають важливим трендом у воєнно-політичному протиборстві в кіберпросторі (складність проведення таких нападів робить їх малопридатними для звичайних хакерських атак з метою отримання фінансового зиску).

3. Хоча метод АчЛП відомий давно, лише останнім часом він набув істотного поширення. Можна обґрунтовано припустити, що однією з причин стала саме вдала атака *NotPetya*, яка виконала роль контрольного відпрацювання для такого типу атак і довела їхню високу ефективність за відносно невеликих витрат.

4. АчЛП не нівелюють цілком класичні методи кібербезпеки, але ставлять питання про їхні межі. Наприклад, розроблена й розгорнута в США система кіберзахисту урядових структур ***Einstein*** (відповідальне відомство – *US-CERT*), яка базується переважно на впроваджені системи активних сенсорів, так і не змогла ані виявити цю атаку, ані зреагувати на неї. Це ставить питання і перед Україною, де готуються реалізувати схожу систему. У ширшому сенсі – це проблема принципової зміни концепції ***«периметр захисту»***, коли за одиницю кібербезпеки розглядають конкретний об'єкт захисту разом з його системами кібербезпеки, на ширшу та динамічнішу ***«екосистему кібербезпеки»***, за якої безпосередній об'єкт кіберзахисту

[8] Див.: URL: https://styran.com/kaseya-usa-notpetya/
[9] Див.: URL: https://edition.cnn.com/2021/07/13/tech/revil-ransomware-disappears/index.html
[10] Див.: URL: https://lenta.ru/news/2022/01/20/revil_not_dead/
[11] Див.: URL: https://blog.gitguardian.com/codecov-supply-chain-breach/

розглядають сукупно з його відносинами з іншими суб'єктами, прямо чи опосередковано пов'язаними (організаційно чи на рівні інформаційно-телекомунікаційних систем). Частково такий підхід уже запропонувала «Кібербезпекова комісія США Соларіум» на початку 2020 р., але його все ще не імплементували повною мірою.

ЄС усвідомлює, що **нова хвиля АчЛП вимагає термінових спільних дій** політичних кіл і спільнот кібербезпеки. **Упровадження найліпших практик (*good practices*) та участь у скоординованих діях на рівні ЄС** є важливими для підтримки всіх держав-членів у розвитку таких можливостей – для досягнення спільного рівня безпеки[12].

Варто наголосити, що в галузі кібербезпеки Євросоюз досить послідовно рухається в напрямі **чимдалі глибшої міжвідомчої і міждержавної кооперації та координації, що є критично важливим для відсічі нових комплексних загроз,** як-от нинішній сплеск АчЛП. Зокрема, на сьогодні вже триває **процес створення Спільного кіберпідрозділу ЄС (*Joint Cyber Unit – JCU*)**. Концепцію *JCU* два роки тому запропонувала Європейська Комісія. Передбачають, що Спільний кіберпідрозділ буде єдиною платформою «для сприяння співпраці та надання можливості реалізувати свій повний потенціал». У її межах працюватимуть не лише спільноти кібербезпеки, але й (у разі необхідності) непрофільні відомства та органи, громадські та інші організації, причому як на рівні ЄС, так і в державах-членах[13]. Основні завдання *JCU* такі:

- забезпечення координованої відповіді з боку ЄС на масштабні кіберзагрози, інциденти та кризи;
- підвищення рівня обізнаності широкої громадськості про поточну кіберситуацію, налагодження постійної комунікації з громадянами;
- гарантування колективної готовності (*joint preparedness*)[14].

Нині вже повністю розгорнуто роботу з формування *JCU*.

Значну увагу безпеці ланцюжків постачань ПЗ приділено в **Указі Президента США щодо вдосконалення національної кібербезпеки (*Executive Order on Improving the Nation's Cybersecurity*),** оприлюдненому в травні 2021 р.[15] Зокрема, документ містить однорічний покроковий план спільних дій профільних відомств виконавчої гілки влади щодо посилення контролю над змістом коду того ПЗ, яке потрапляє в урядові системи та громадську інфраструктуру через ланцюжки постачань. Загалом план спрямовано на **досягнення трьох основних цілей:**

1. Розроблення силами *NIST* розгорнутого **визначення нового терміна «критичне програмне забезпечення»** (*«critical software»*), яке має відбивати «рівень привілейованого доступу, необхідного для функціонування …, а також потенціал шкідливості такого ПЗ в разі його компрометації»[16], тобто фіксувати мінімальні критерії безпечності його використання в ланцюгах постачань.

---

[12] Див.: URL: https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks
[13] Див.: URL: https://digital-strategy.ec.europa.eu/en/library/factsheet-joint-cyber-unit
[14] Див.: URL: https://ec.europa.eu/newsroom/dae/redirection/document/77509; https://www.enisa.europa.eu/news/enisa-news/eu-boost-against-cyberattacks-eu-agency-for-cybersecurity-welcomes-proposal-for-the-joint-cyber-unit
[15] Див.: URL: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
[16] Там само.

2. Підготовка та надання федеральним відомствам переліку категорій ПЗ і програмних продуктів, що відповідають цьому визначенню, а також спеціальних інструкцій (*guidance*) щодо заходів безпеки для критичного ПЗ.

3. Визначення в межах чинного законодавства механізму, який зобов'язує відомства вивести з експлуатації програмні продукти, що не відповідають новим критеріям критичного ПЗ[17].

У червні 2021 р. *NIST* опублікував нове розгорнуте визначення критичного ПЗ[18]. У ньому охоплено як основний обчислювальний інструментарій (захист кінцевої точки (*endpoint protection*), резервне копіювання даних, управління ідентифікацією та обліковими даними, операційні системи та контейнерні середовища тощо), так і ПЗ різного мережного статусу – від локального до хмарного.

Також *NIST* з 2008 р. реалізує дослідницьку програму щодо управління кіберризиками ланцюжків постачань (*cyber supply chain risk management*). 2020 р. *NIST* оприлюднив новий звіт з найліпшими практиками зниження вірогідності реалізації такого типу атак. Упереджувальні заходи передбачають таке:

- увага до проблеми на найвищому рівні організації (до прикладу, створення спеціальних *рад* за участі керівників установи та керівників підрозділів для оцінювання ризиків у ланцюжках постачальників);

- заснування формалізованих заходів (як-от: випрацювання офіційних політик організацій щодо цієї проблеми, заснування спеціальних команд для відстежування вразливостей, затвердження списків постачальників тощо);

- знання та взаємодія з критично важливими постачальниками (чітко визначити постачальників, від яких залежить функціонування вашої організації, оцінити вразливості та встановлювати для таких постачальників додаткові вимоги безпеки протягом усього циклу відносин);

- розуміння своїх ланцюжків постачань (чітко визначити, який вигляд мають ланцюжки постачань організації, хто є їхніми учасниками та, за можливості, мати додаткову інформацію про постачальників);

- тісна співпраця з ключовими постачальниками (може виходити за межі суто формальних відносин і мати тісніші взаємозв'язки, як-от: програми двостороннього навчання, взаємні візити, обмін досвідом тощо);

- залучення ключових постачальників в діяльність із забезпечення стійкості організації (передбачає установлення протоколів обміну інформацією, спільне дослідження кіберінцидентів, протоколи комунікування щодо виявлених уразливостей, скоординовані процедури відновлення діяльності, спільне «вивчення уроків» після інцидентів);

- оцінка та моніторинг відносин з постачальниками (оскільки їхній статус і можливості з часом змінюються, має бути налагоджений процес постійного моніторингу таких змін, визначення їхньої критичності для діяльності організації, має проводитись оцінювання постачальників, зокрема стосовно дотримання ними вимог безпеки – у перспективі важливим є створення універсальних галузевих питань за найкритичнішими аспектами діяльності);

---

[17] Див.: URL: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[18] Див.: URL: https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/critical-software-definition-explanatory

- створення планів продовження діяльності (як забезпечити функціонування організації, коли критичний постачальник раптово не зможе надавати послуги).

15 грудня 2020 р. Рахункова палата США (*Government Accountability Office*) оприлюднила результати власного аудиту щодо впровадження цих рекомендацій (у їх попередніх редакціях) у практику 23 цивільних урядових структур США[19]. За результатами дослідження виявилося, що 14 організацій не впровадили жодну із 7 основних вимог *NIST*, 2 агентства впровадили п'ять із семи рекомендацій, а інші – від однієї до трьох.

Національний центр з кібербезпеки королівства (*NCSC*) у своїх щотижневих звітах також констатує стрімке збільшення кількості та рівня небезпек АчЛП в усьому світі. Зокрема, у випуску від 15 жовтня 2021 р.[20] з посиланням на доповідь *BlueVoyant,* базовану на даних від 1200 співробітників великих світових компаній[21], Центр серед іншого наводить такі цифри:

- понад 90 % фірм по всьому світу зазнали шкоди в результаті слабких місць ланцюжка постачань;
- у 2020 – 2021 рр. кількість АчЛП зросла на 37 %.

У зв'язку з цим *NCSC* пропонує активніше застосовувати розроблений ним ще 2018 р. документ «Керівні принципи щодо убезпечення ланцюгів постачань» (*Supply chain security guidance*), призначений для звичайних (не критично важливих для національної безпеки) організацій / об'єктів[22]. Основу посібника становлять 12 принципів безпеки ланцюгів постачань, розділені на чотири смислові блоки:

1. Розуміння ризиків (стосуються етапу збору інформації).
2. Забезпечення контролю над власними ланцюгами постачань.
3. Перевірка своїх домовленостей.
4. Постійне вдосконалення[23].

Задля забезпечення ліпшої орієнтації пересічних громадян (підприємців) **уряд регулярно видає актуальну довідкову та просвітницьку літературу, написану неодмінно простою зрозумілою мовою** (*plain language*)[24].

Понад це, у Королівстві діє Урядова система забезпечення постачальників (*Government supplier assurance framework*), яка повинна надавати їм підтримку не лише у фізичному, але й у кібернетичному просторі[25].

---

[19] Дослідження охопило: Держдепартамент, міністерства сільського господарства, фінансів, освіти, енергетики, здоров'я, внутрішньої безпеки (*Homeland Security*), внутрішніх справ (*Interior*), міського розвитку, юстиції, праці, транспорту, економіки та у справах ветеранів; а також федеральні організації: Агентство захисту природного середовища, Управління загальних служб, *NASA*, Національний науковий фонд, Комісію з ядерного регулювання, Офіс управління персоналом, Адміністрацію малого бізнесу, Адміністрацію соціальної безпеки та *USAID*. Дослідження тривало з 2018 до 2020 рр. Повний звіт див.: URL: https://www.gao.gov/assets/720/711266.pdf

[20] Див.: URL: https://www.ncsc.gov.uk/report/weekly-threat-report-15th-october-2021#section_1

[21] Див.: URL: https://www.bluevoyant.com/resources/managing-cyber-risk-across-the-extended-vendor-ecosystem/

[22] Див.: URL: https://www.ncsc.gov.uk/collection/supply-chain-security/principles-supply-chain-security

[23] Див.: URL: https://www.ncsc.gov.uk/collection/supply-chain-security/principles-supply-chain-security/continuous-improvement

[24] Там само.

[25] Див.: URL: https://www.gov.uk/government/publications/government-supplier-assurance-framework

ІІ. ОСНОВНІ ЗАХОДИ ПРОТИДІЇ АчЛП: МЕНШЕ ДОВІРИ, БІЛЬШЕ РЕГУЛЮВАННЯ?

2.1. Підхід «нульової довіри» vs АчЛП: шукаючи нові стратегії захисту

Zero Trust (з англ. – **нульова довіра**) як модель захисту в кіберпросторі розробив колишній аналітик *Forrester* Джон Кіндерваг (*John Kindervag*) ще 2010 р. Нині *Zero Trust* є цілісною, ретельно опрацьованою концепцією, підходи якої широко застосовують у програмно-апаратних платформах, а також у регламентах, рекомендаціях та фреймворках з кібербезпеки, забезпечуючи ефективний захист від сучасних кіберзагроз, зокрема й АчЛП.

Як і в більшості сучасних кібербезпекових рішень, розроблених в умовах стрімкої «делокалізації» кіберпростору (коли він чимдалі більше переміщується в площину безпровідних мереж та мобільних пристроїв), архітектура *Zero Trust* фокусується на захисті об'єктів (або активів – обладнання, ПЗ, даних, мережних процесів тощо), а не традиційних «периметрів» (локацій). Понад це, як видно із самої назви цього підходу, основним його принципом є «ніколи не довіряти, завжди перевіряти» замість традиційного «довіряй, але перевіряй».

Наприклад, для **всіх** користувачів під час **кожного** входу в систему та/або мережу обов'язковою є багатофакторна автентифікація (*FIDO2* і т. ін.), а для пристроїв – автентифікація через апаратне забезпечення первинної перевірки (*hardware root of trust*)[26], приміром, за допомогою апаратного довіреного модуля (*Trusted Platform Module – TPM*).

Застосовуючи таку стратегію, можна значно підвищити рівень безпеки передусім завдяки: 1) т. зв. ефекту **мікросегментації**, коли враження одного з об'єктів не призводить до враження всієї системи (принцип ізольованих відсіків на кораблі); 2) **повному інформаційному контролю** щодо того, хто саме, коли й до яких активів отримував доступ.

Побудова сучасної та ефективної архітектури кіберзахисту за моделлю *Zero Trust (Zero Trust Architecture – ZTA)* передбачає зосередження уваги та зусиль на таких основних напрямах[27].

Дані. Найбільш важливий і цінний актив, а тому пріоритетний для захисту. Саме викрадення даних цікавить зловмисників найчастіше. Безпека корпоративних даних передбачає їх адекватний аналіз, класифікацію, збереження, контроль доступу та переміщення.

Мережі. Будь-які несанкціоновані присутність/переміщення в корпоративних мережах мають бути максимально ускладненими. Найефективнішою для цього є тактика розділення мережі на фрагменти та їх адміністративна ізоляція під контролем, наприклад, брандмауерів нового покоління. Ідеться про мікросегментацію, тобто налаштування окремих сегментів у мережі з власними унікальними обліковими даними доступу до нього. Користувачеві або пристрою, які можуть отримати доступ до одного сегмента, не дозволено отримати доступ до іншого сегмента без окремої перевірки.

---

[26] Більше див.: URL: https://bit.ly/2YxgdVU; https://habr.com/ru/post/499662/

[27] Див.: URL: https://blog.1gb.ua/perevod-chto-takoe-zero-trust-model-bezopasnosty/; https://docs.google.com/presentation/d/13wiv0xXXMEmoUX0H8XgIUSH2gsLnvUTxA8_PaYPJxFw/edit#slide=id.gedba26a291_0_121; https://www.upguard.com/blog/prevent-supply-chain-attacks-with-zero-trust-architecture; What is Zero Trust Security? Principles of the Zero Trust Model (crowdstrike.com)

Користувачі. Людина (співробітник, оператор, звичайний юзер та ін.) зазвичай є найслабшою ланкою в будь-якій автоматизованій системі (разом із системами кібербезпеки, а також практиками їх застосування). Тому рекомендують мінімізувати привілейований доступ, застосовувати багатофакторну автентифікацію, чіткі правила доступу до активів й користування ними, *VPN, CASB* (брокери безпечного доступу в хмару) та інші засоби контролю, що відповідають концепції *ZTA*. Особистість користувачів і права їхнього доступу треба постійно перевіряти. Ба більше, якщо вже зареєстрований користувач намагається отримати доступ до іншого ресурсу в мережі, його треба повторно перевірити.

Навантаження. Цей термін використовують системні адміністратори для позначення всього стека (комплексу) додатків і бекенду ПЗ (тобто службового, такого, що не відбито в користувацьких інтерфейсах), які функціонують у системі, зокрема й для забезпечення комунікації в ланцюгах постачань. Не встановлені вчасно оновлення чи патч (латка, виправлення програмних помилок і вразливостей) створюють для зловмисників численні додаткові вектори атаки. Водночас важливо виходити з тієї презумпції, що кожне оновлення є небезпечним, тож інсталювати його потрібно тільки після перевірки.

Пристрої. Надлишок під'єднаних мобільних пристроїв та периферії інтернету речей (від смартфона чи смартгодинника до «розумної» кавоварки), що інтегровані в локальні інфраструктури, також створює додаткові вектори атак. Доцільно мінімізувати наявність у мережах таких девайсів, інакше їх, поряд з рештою активів, треба піддавати сегментації, ізоляції та моніторингу (див. вище – «мікросегментація»).

Найприроднішим напрямом оборони від АчЛП видається саме захист мереж і точок входу. Однак розгалуженість і багатошаровість сучасних вебінфраструктур у поєднанні з досконалістю новітніх кіберзагроз у цьому разі роблять інші напрями не менш важливими для захисту від таких атак. З урахуванням специфіки АчЛП високу ефективність тут забезпечує передусім сам підхід *Zero Trust* з його, так би мовити, «презумпцією винуватості»: кожний суб'єкт уважають джерелом загрози, поки не доведено протилежне.

Глобальна хвиля АчЛП 2020 – 2021 рр. спонукала керівництво розвинених країн, а також провідні дослідницькі центри та ІТ-компанії звернути спеціальну увагу на *Zero Trust* як одну з найефективніших стратегій боротьби з такими атаками. Особливо ретельно до цього питання поставилися в США.

Уже в серпні 2020 р. (очевидно, не у зв'язку з хвилею атак, оскільки розроблення розпочато ще 2019 р.) Національний інститут стандартів та технологій США (*NIST*) оприлюднив **Спеціальну публікацію «Архітектура нульової довіри» (*SP 800-207 Zero Trust Architecture*)**[28]. Суть документа, за визначенням самих авторів, полягала у вивченні напрямів та можливостей використання принципу нульової довіри для планування промислової та корпоративної інфраструктури й робочих процесів. Публікація містить узагальнювальне (*abstract*) визначення *ZTA*, типові моделі її розгортання та випадки використання, коли нульова довіра може поліпшити кібербезпеку підприємства. Автори наголошують, що *Zero Trust* як концепція кібербезпеки сфокусована на захисті ресурсів, а не локацій, – це

[28] Див.: URL: https://csrc.nist.gov/publications/detail/sp/800-207/final#pubs-documentation

«відповідь на тенденції корпоративних мереж», які нині поєднують віддалених користувачів, власний пристрій (*BYOD*) і хмарні активи, розміщені поза її межами[29].

У листопаді 2021 р. **фахівці компанії *UpGuard*[30], базуючись на *SP 800-207*, випрацювали докладні рекомендації** щодо запобігання атакам ланцюга постачань за допомогою *ZTA*, представленою *NIST*[31].

Автори стверджують, що *ZTA* може бути скоригована відповідно до різних вимог екосистеми. Можна впровадити декілька варіацій *ZTA*, які цілком здатні захистити від АчЛП, але організації доцільніше вибрати ту з них, яка вимагає мінімального обсягу зусиль для впровадження. У рекомендаціях пропонують такі конфігурації *ZTA*[32].

Конфігурація 1 *– Розширене управління ідентифікацією*

Найпоширеніший варіант: лише ті, хто має привілейований доступ, можуть під'єднуватися до корпоративних ресурсів. Щоб полегшити цей протокол, політика доступу до корпоративних ресурсів має містити такі компоненти.

- Посвідчення кожного дозволеного користувача.
- Призначені атрибути кожного дозволеного користувача.
- Список дозволених пристроїв.
- Статуси активів.

Корпоративні політики доступу до ресурсів також можна налаштувати на надання часткового доступу до корпоративних ресурсів, якщо виконано певні умови (наприклад, якщо надходить запит на доступ із певних розташувань).

Підприємства, які приймають модель розширеного управління ідентифікацією, зазвичай мають окрему мережу доступу відвідувачів. Це обмежує доступ до корпоративних ресурсів привілейованим користувачам, дозволяючи при цьому доступ до інших, менше вразливих активів.

Модель розширеної ідентичності *ZTA* оптимізовано для виявлення вразливостей безпеки насамперед на рівні користувача.

Конфігурація 2 *– Мікросегментація*

Великим організаційним інфраструктурам, які хочуть швидко впровадити захист від АчЛП, буде важко масштабувати зміну розширеного управління ідентифікацією. У такому разі оптимальною видається модель мікросегментації, оскільки вона зосереджена на забезпеченні вразливих мережевих зон, а не всієї екосистеми.

Ці «зони» або «сегменти» захищено брандмауерами останнього покоління (*NGFW*) або шлюзовими пристроями спеціального призначення. У результаті організація отримує серію захищених сегментів, які надають або відмовляють у доступі до активів через кілька шлюзів ідентифікації та доступу – *PEP (Policy Enforcement Point* – точка застосування політики).

Конфігурація 3 *– Мережева інфраструктура в програмно визначеному периметрі*[33]

---

[29] Там само.
[30] Див.: URL: https://www.upguard.com/
[31] Див.: URL: https://www.upguard.com/blog/prevent-supply-chain-attacks-with-zero-trust-architecture
[32] Там само.
[33] **Програмно визначений периметр (*Software Denied Perimeter – SDP*)** – це спосіб приховати під'єднану до інтернету інфраструктуру (сервери, маршрутизатори тощо), щоб зовнішні сторони та зловмисники не могли

У цій інсталяції всі запити мережі проходять через одну *PEP*, керовану адміністратором корпоративної політики *ZTA*, перш ніж їм буде дозволено/відмовлено в доступі до корпоративних ресурсів.

Конфігурація 4 *– Device agent or gateway-based deployment*[34]

Модель *ZTA*, пропонована в *NIST SP 800-207,* побудована на **таких основних принципах**.

- Постійна перевірка. Перевіряти доступ весь час, всюди, для всіх ресурсів.
- Обмеження «радіусу вибуху» *(blast radius)*. За допомогою мікросегментації та зменшення привілейованого доступу мінімізувати вплив, якщо відбувається зовнішнє або інсайдерне порушення.
- Автоматизація збору даних про безпеку та реагування. Залучення до аналізу поведінкових даних та отримання контексту з усього IT-стека (облікові дані активів, ситуація в мережі, кінцеві точки доступу до даних, навантаження тощо) для найточнішої діагностики та реагування[35].

Автори публікації дійшли висновку, що оптимальною моделлю захисту для корпоративної інфраструктури буде саме *ZTA*, якщо ця інфраструктура містить таке:

- хмарні сервіси, велику кількість одиниць активів;
- не контрольовані системою під'єднані пристрої (наприклад, *IoT*);
- застарілі системи;
- програми *SaaS* (*software as a service* – «ПЗ як сервіс», зазвичай їх постачають провайдери хмарних послуг)[36].

Також, на думку авторів *SP 800-207*, модель *ZTA* нині є найефективнішим захистом проти таких загроз, як вимагачі, АчЛП та інсайдерські загрози[37].

2021 р. Національний центр передового досвіду кібербезпеки США (*National Cybersecurity Center of Excellence – NCCoE*) у співпраці з провідними учасниками галузі ініціював **проєкт «Імплементація архітектури нульової довіри»**. Мета – продемонструвати кілька підходів до *ZTA*, застосованої до звичайної IT-інфраструктури підприємства загального призначення у фізичній локації та в хмарі, відповідно до концепцій та принципів, задокументованих у спеціальній публікації *NIST (SP) 800-207, Zero Trust Architecture*. У кейсах інтегруватимуться комерційне ПЗ та продукти з відкритим кодом (*open-source products*), зроблені в кореляції зі стандартами кібербезпеки та рекомендованими практиками для демонстрації надійних функцій безпеки архітектури нульової довіри.

На кінець 2021 р. проєкт перебував у стадії розгортання. Одним з його результатів буде посібник з практики кібербезпеки *NIST* – загальнодоступний опис

її бачити незалежно від того, розміщена вона локально або в хмарі. Суттю підходу *SDP* є формувати периметр мережі на програмному, а не апаратному забезпеченні. Програмно визначений периметр утворює віртуальну межу навколо активів компанії на мережевому рівні, а не на рівні додатків. Це відокремлює його від інших елементів керування на основі доступу, які обмежують права користувачів, але дозволяють широкий доступ до мережі. Ще одна визначна особливість полягає в тому, що *SDP* автентифікує пристрої, так само як і ідентичність користувача. Компанія, яка використовує *SDP*, власне, робить свою інфраструктуру невидимою для всіх, окрім авторизованих користувачів. Див.: URL: https://www.cloudflare.com/learning/access-management/software-defined-perimeter/

[34] Більше див.: URL: https://arxiv.org/ftp/arxiv/papers/2104/2104.00460.pdf

[35] Див.: URL: https://www.crowdstrike.com/cybersecurity-101/zero-trust-security/

[36] Там само.

[37] Там само.

практичних кроків, необхідних для реалізації довідкових проєктів кібербезпеки для *Zero Trust*[38].

Імовірно, хвиля АчЛП стала одним зі стимулів для того, щоб потенціал і важливість *Zero Trust* зрозуміли й ***керівні кола США***. **У програмному Указі Президента Джо Байдена щодо вдосконалення національної кібербезпеки** від 12 травня 2021 р.[39] питанням захисту національних ланцюгів постачань у кіберпросторі та модернізації кібербезпеки федерального уряду на основі впровадження *ZTA* присвячено по самостійному розділу.

Указ містить покроковий розгорнутий план переходу всіх федеральних відомств на «найліпші практики безпеки; просування до *ZTA*; оптимізацію захисту хмарних сервісів»; на цій основі передбачено «централізувати та спростити доступ до даних кібербезпеки, щоб стимулювати аналітику для виявлення та управління ризиками кібербезпеки; інвестувати як у технології, так і в персонал, аби відповідати таким цілям модернізації». Спеціальну увагу звернено на необхідність: забезпечити ефективний обмін інформацією між федеральними агентствами; створити навчальну програму для забезпечення ефективної підготовки та оснащеності агентств[40].

На виконання положень Указу на початку вересня 2021 р. Управління з питань управління та бюджету (*Office of Management and Budget – OMB*) США опублікувало **проєкт федеральної стратегії[41] щодо запровадження *ZTA* у федеральних відомствах США**. Своєю чергою, Агентство з кібербезпеки та безпеки інфраструктури (*Cybersecurity and Infrastructure Security Agency – CISA*) оприлюднило свою модель зрілості *Zero Trust* для керівництва та надання допомоги агентствам у плануванні їх реалізації[42].

У супровідному меморандумі до проєкту стратегії міститься досить показова констатація, а саме: «У нинішньому середовищі загроз федеральний уряд більше не може залежати від систем захисту, базованих на моделі «безпеки периметра» стосовно критичних систем і даних. Розв'язання цієї проблеми вимагатиме серйозної зміни парадигми в тому, як федеральні агентства підходять до кібербезпеки»[43]. Таким чином, ураховуючи підготовку стратегії як виконання положень президентського Указу, у найвищих керівних колах Сполучених Штатів досягнуто консенсусу щонайменше стосовно магістральних напрямів та інтенцій наступного розвитку глобального протистояння в кіберпросторі.

Надзавданням стратегії визначено створення федеральної архітектури нульової довіри (*ZTA*), яка:

- підтримує надійні (*strong*) практики ідентифікації у федеральних агентствах;
- покладається на шифрування й тестування додатків замість утримання безпеки периметра;
- розпізнає всі пристрої та ресурси, які має Уряд;
- підтримує інтелектуальну автоматизацію дій з безпеки;
- гарантує безпечне та надійне використання хмарних сервісів[44].

---

[38] Див.: URL: https://www.nccoe.nist.gov/projects/implementing-zero-trust-architecture
[39] Див.: URL: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
[40] Див.: URL: Там само.
[41] Див.: URL: https://bit.ly/3Dkpu1B
[42] Див.: URL: https://www.whitehouse.gov/omb/briefing-room/2021/09/07/office-of-management-and-budget-releases-draft-federal-strategy-for-moving-the-u-s-government-towards-a-zero-trust-architecture/
[43] Див.: URL: https://zerotrust.cyber.gov/federal-zero-trust-strategy/
[44] Там само.

Документ констатує, що вихід на означені рубежі з об'єктивних причин не може бути простим та швидким, тому «ця **стратегія** є відправною точкою, а не всеосяжним керівництвом щодо побудови повністю зрілої *ZTA*». Її безпосередня **мета** полягає в тому, щоб «поставити всі федеральні агентства на загальну дорожню карту, викласти початкові кроки, які агентства повинні зробити для забезпечення собі шляху до високозрілої архітектури нульової довіри»[45].

Поряд із цим, у стратегії все ж поставлено конкретні **завдання і терміни** для федеральних агентств. Вони базовані на паралельно розробленій *CISA* (так само на виконання положень Указу) **«Моделі зрілості *Zero Trust*»**, яка містить чіткі цілі (індикатори) безпеки, згруповані у п'ять блоків (*five pillars*)[46]. Агентства мають досягнути таких цілей та показників до кінця 2024 фінансового року.

1. **Ідентифікація:** співробітники агентства використовують корпоративну ідентифікацію для доступу до додатків, які вони використовують у своїй роботі. Стійка до фішингу багатофакторна автентифікація захищає цей персонал від складних онлайн-атак.
2. **Пристрої:** федеральний уряд має ретельно обліковувати кожний пристрій, який він експлуатує та дозволяє використовувати для урядових потреб, і може виявляти та реагувати на інциденти на цих пристроях.
3. **Мережі:** агентства шифрують всі *DNS*-запити та *HTTP*-трафік у своєму середовищі та починають сегментувати мережі навколо своїх додатків. Федеральний уряд визначає найпридатніший шлях (*workable path*) до шифрування електронної пошти під час транзиту.
4. **Додатки:** агентства розглядають всі програми як під'єднані до інтернету, регулярно піддають свої заявки суворому тестуванню та зацікавлені отримувати зовнішні звіти про вразливості.
5. **Дані:** агентства перебувають на чітко визначеному спільному шляху до розгортання захисту, який використовує ретельну категоризацію даних. Агентства послуговуються хмарними службами безпеки для моніторингу доступу до своїх конфіденційних даних, а також упровадили корпоративне ведення журналу та обмін інформацією[47].

Ще до створення цієї стратегії, у лютому 2021 р., Агентство оборонних інформаційних систем (*Joint Defense Information Systems Agency – DISA*) у співробітництві зі спеціальною командою Агентства національної безпеки (*National Security Agency – NSA*) і під егідою Міністерства оборони США представило першу редакцію **«Рекомендованої архітектури нульової довіри» (*Zero Trust Reference Architecture*)** – посібник або фреймворк за жанром і цільовим призначенням[48].

Архітектура, зокрема, описує сім стовпів (базових об'єктів) нульової довіри – користувача, пристрій, мережу/середовище, застосування та навантаження, дані, видимість та аналітику, автоматизацію та управління – і окреслює можливості нульової довіри, узгоджені з кожним. Можливості, скажімо, для стовпа-пристрою передбачають ідентифікацію, автентифікацію, авторизацію, інвентаризацію, ізоляцію, захист, виправлення та контроль всіх пристроїв. Архітектура також

---

[45] Там само.
[46] Див.: URL: https://www.cisa.gov/publication/zero-trust-maturity-model; CISA Zero Trust Maturity Model
[47] Див.: URL: https://zerotrust.cyber.gov/federal-zero-trust-strategy/
[48] Див.: URL: https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v1.1(U)_Mar21.pdf

окреслює технічні, правові нормативні та процедурні стандарти, які застосовують до кожного стовпа[49].

Починаючи з 2020 – 2021 р., спеціальну увагу розвиткові та впровадженню концепції *Zero Trust* (хоча й поза проблематикою АчЛП) стали приділяти також ***профільні відомства Сполученого Королівства***.

Так, у липні поточного року Національний центр кібербезпеки (*National Cyber Security Centre – NCSC*) оприлюднив першу редакцію **«Принципів побудови архітектури нульової довіри» (*Zero trust architecture design principles 1.0*)**[50]. Посібник має формат збірника порад, не містить чітких вимог чи покрокових інструкцій і покликаний передусім допомогти зацікавленому суб'єкту «розробити або переглянути архітектуру нульової довіри, яка відповідає індивідуальним вимогам [його] організацій». Традиційно для британського *NCSC* публікацію написано зрозумілою мовою (*plain language*) і розраховано «на тих, хто реалізує архітектуру нульової довіри в корпоративному середовищі – державний і приватний сектори»[51].

Для побудови оптимальної (для того чи того конкретного суб'єкта) архітектури нульової довіри *NCSC* пропонує завжди дотримуватися восьми принципів.

1. Завжди мати чітке уявлення про свою архітектуру, зокрема інформацію про користувачів, пристрої, служби та дані.
2. Завжди мати чітке уявлення про ідентифікації та облікові дані своїх користувачів, служб та пристроїв.
3. Аналізувати поведінку користувачів, стан пристроїв і роботу сервісів.
4. Дотримуватися політик доступу для авторизації запитів.
5. Автентифікувати та авторизувати скрізь.
6. Постійний моніторинг користувачів, пристроїв і служб.
7. Не довіряти жодній мережі, навіть власній.
8. Обирати обладнання та ПЗ з підтримкою функціонала *Zero Trust* (таку підтримку не всюди інстальовано в базовому рішенні)[52].

Також фахівці *NCSC* радять перед переходом до *ZTA* уважно вивчити питання доцільності й необхідності (наприклад, порівнюючи стару та нову архітектури з погляду ефективності й комфорту) такого переходу, здійснювати його поетапно, відмикаючи старі компоненти захисту лише після того, як цілковито готові до запуску й протестовані нові тощо[53].

Привертає увагу те, що на відміну від керівництва США уряд Сполученого Королівства (принаймні у сфері публічної політики і в стосунках з приватним сектором та громадянським суспільством) не декларує жодних системних проєктів та/чи політики щодо масштабних розробок та імплементацій моделей *ZTA* на національному рівні. Фокусування уваги на цьому питанні збіглося в часі з глобальною хвилею АчЛП (2020 – 2021 рр.), але тільки на рівні профільних відомств і, так би мовити, у штатному режимі.

---

[49] Див.: URL: https://gcn.com/articles/2021/05/17/disa-zero-trust-architecture.aspx
[50] Див.: URL: https://www.ncsc.gov.uk/blog-post/zero-trust-1-0; https://www.ncsc.gov.uk/collection/zero-trust-architecture
[51] Див.: URL: https://www.ncsc.gov.uk/collection/zero-trust-architecture
[52] Див. більше: URL: https://www.ncsc.gov.uk/collection/zero-trust-architecture
[53] Там само.

2.2. Критичне програмне забезпечення: погляд США

Безпека програмного забезпечення, яку використовує федеральний уряд, має життєво важливе значення для його здатності виконувати свої критичні функції. Але розвиток та виробництво комерційного ПЗ часто є «недостатньо прозорим» з погляду «його здатності протистояти атакам та адекватного контролю, щоб запобігти втручанню зловмисників». Є нагальна потреба реалізувати суворіші й передбачуваніші механізми для забезпечення того, щоб ПЗ функціонувало надійно й за призначенням. Особливою проблемою є безпека й цілісність «критичного програмного забезпечення» – такого, що виконує критично важливі довірчі функції, напр., надає або вимагає підвищених привілеїв системи чи прямого доступу до мережевих і обчислювальних ресурсів. Відповідно, федеральний уряд повинен ужити заходів для якнайшвидшого підвищення безпеки та цілісності (*integrity*) ланцюжка постачань програмного забезпечення і передусім – критичного ПЗ[54] в систему федеральних органів виконавчої влади США.

Задля досягнення цієї генеральної мети **Указ Президента США про вдосконалення кібербезпеки нації (*Executive Order on Improving the Nation's Cybersecurity*)**[55] від 12 травня 2021 р. передбачає складний комплекс взаємопов'язаних заходів та завдань для всіх профільних відомств протягом року (до травня 2022 р.). Визначення «критичного ПЗ» є центральним смисловим елементом, теоретичним стрижнем, довкола якого має будуватися як уся концепція, так і планування конкретних дій щодо формування безпечних ланцюгів постачань такого ПЗ у федеральні агентства. Цей Указ покладає на *NIST* (хоча й із залученням Агентства з кібербезпеки та безпеки інфраструктури (*CISA*), Ради національної безпеки (*NSC*), Офісу директора національної розвідки (*ODNI*), Офісу з управління та бюджету (*OMB*)) центральну роль у формуванні розгорнутого, але максимально чіткого (аж до складення конкретних переліків) уявлення-визначення щодо того, який саме продукт треба вважати в цьому разі «критичним ПЗ» і як гарантувати його безпеку для федеральних агентств.

Цю роботу, згідно з Указом, також розраховано на рік. Вона має чіткі етапи, пов'язані з реалізуванням конкретних завдань. На жовтень – листопад *NIST* відзвітував про виконання деяких з них та про перші попередні результати.

2 – 3 червня 2021 р. NIST провів віртуальний експертний семінар за участі представників федеральних агентств, приватного сектора, наукових кіл та інших зацікавлених сторін щодо визначення стандартів, інструментів, найліпших практик та інших керівних принципів для підвищення безпеки ланцюга постачань програмного забезпечення, а також щодо можливого змісту та сенсу самого поняття «критичного ПЗ для федеральних агентств». В обговоренні взяли участь 1400 фахівців, було подано понад 150 позиційних документів[56].

Обговорення охопило п'ять напрямів:

- ***критерії*** для позначення «критичного програмного забезпечення»;

---

[54] Див.: URL: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[55] Там само.

[56] Див.: URL: https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/workshop-and-call-position-papers

- початковий ***список стандартів*** життєвого циклу розроблення безпечного ПЗ, найліпших практик та інших керівних принципів, прийнятних для розроблення ПЗ для купівлі федеральним урядом;

- керівні ***принципи*** для визначення заходів безпеки, що їх має застосовувати федеральний уряд до використання критичного ПЗ, які охоплюють (але цим не обмежуються) найменші привілеї, сегментацію мережі та належну конфігурацію;

- початкові мінімальні ***вимоги*** до тестування вихідного коду програмного забезпечення;

- ***рекомендації*** щодо забезпечення цілісності ланцюгів [постачань] ПЗ та [контролю] його походження[57].

Наприкінці червня *NIST* опублікував перше визначення критичного ПЗ *EO-Critical Software,* де *EO* – це *Executive Order*, тобто адміністративний указ (АУ). Як робочий переклад – АУ-критичне ПЗ*[58]*. Водночас *NIST* дав супровідний коментар із роз'ясненням запропонованої ним назви *EO-Critical Software* для ПЗ, передбаченого нормами Указу: «Більшість з визначень терміну «критичний» засновані на тому, як технології підтримують різні завдання або процеси, як-от критична безпека або критична інфраструктура. Використання (цього) терміна в Указі дещо відрізняється тим, що воно засноване не на контексті використання, а на властивостях цього програмного забезпечення, що робить його, імовірно, критичним у більшості випадків використання. Тобто воно зосереджене на критичних функціях, які стосуються базової інфраструктури для кібероперацій та безпеки»[59]. Такий підхід, на думку експертів *NIST*, означатиме: постачальникам не доведеться заздалегідь прогнозувати, хто і яким чином буде використовувати їхнє ПЗ, перш ніж визначити, яких стандартів безпеки треба дотримуватися[60].

Замість цього вони будуть знати, що певні види продуктів виробляють з обов'язковим дотриманням чітко визначених правил та стандартів.

Отже, на червень – липень 2021 р. під *критично важливим програмним забезпеченням NIST* офіційно розуміє будь-яке ПЗ, що має прямі залежності (зв'язки) між *компонентами* програмного забезпечення (одним або більше), які мають принаймні один із таких атрибутів:

- вимагає для роботи підвищених привілеїв або розроблений для управління привілеями;
- має прямий або привілейований доступ до мережевих або обчислювальних ресурсів;
- розроблений для контролю доступу до даних або для експлуатаційної/операційної технології (тобто для автоматизованих систем управління – АСУ);
- виконує критично важливі довірчі функції[61];

---

[57] Див. більше: URL: https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/workshop-and-call-position-papers

[58] Тобто мова йде не так про універсальне визначення, як про таке, що мається на увазі саме в межах вказаного *Executive Order*.

[59] Див.: URL: https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/critical-software-definition-background-approach#approach

[60] Див.: URL: https://www.govtech.com/security/nist-defines-critical-software-implications-to-follow

[61]Критично важливі довірчі функції (*function critical to trust*) – охоплює категорії програмного забезпечення, що використовують для функцій безпеки, як-от мережеве управління, безпека кінцевих точок та захист мережі. Див.: URL: https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/critical-software-definition-faqs

- вимагає [для виконання своїх функцій] такого рівня довіри, що виходить за межі привілейованого доступу[62].

Визначення застосовують до програмного забезпечення всіх форм (наприклад, автономного ПЗ, невіддільного від конкретних пристроїв або апаратних компонентів ПЗ, хмарного ПЗ), придбаного або розгорнутого у виробничих системах і використовуваного для операційних цілей. Інші випадки використання (як-от ПЗ винятково для досліджень або тестування, не розгорнуті у виробничих системах) перебувають поза сферою застосування цього визначення[63].

NIST рекомендує, щоб початковий етап упровадження *EO* зосередився на автономному локальному ПЗ, яке має критично важливі функції або створює подібний значний потенціал для шкоди, якщо його скомпрометувати. Наступні етапи можуть стосуватися інших категорій програмного забезпечення, таких як:

- ПЗ, яке контролює доступ до даних;
- хмарне та гібридне ПЗ;
- інструменти розроблення ПЗ: системи репозиторію коду, інструменти розроблення, програмне забезпечення для тестування, інтеграції, пакувальне ПЗ тощо;
- програмні компоненти в мікропрограмі завантажувального рівня;
- програмні компоненти в операційних технологіях (ОТ або АСУ)[64].

NIST також наводить розроблений *CISA* попередній список категорій програмного забезпечення, які вважають АУ-критичними (із заувагою про те, що пізніше Агентство надасть «авторитетний список категорій ПЗ»). До актуального натепер списку вміщено одинадцять категорій[65].

У липні 2021 р. на виконання положень Указу про вдосконалення кібербезпеки нації *NIST* видав **рекомендації (*guidance*) щодо заходів безпеки для АУ-критичного ПЗ**[66], базовані на вже розглянутому визначенні ПЗ. У документі спеціально наголошено, що (очевидно, через уже згадану специфіку об'єкта захисту) пропоновані заходи безпеки стосуються винятково **використання (експлуатації)**, а не **розроблення та придбання** АУ-критичного ПЗ. Вони призначені убезпечити експлуатацію цього ПЗ в операційних середовищах федеральних агентств. Це такі заходи.

1. Захищати АУ-критичне ПЗ і базовані на ньому платформи (зокрема кінцеві точки (*endpoints*), сервери, хмарні ресурси) від несанкціонованого доступу та використання.

2. Захищати конфіденційність, цілісність, доступність даних, що їх використовує АУ-критичне ПЗ і базовані на ньому платформи.

3. Ідентифікація та підтримка таких ресурсів, їх захист від неналежного використання.

4. Оперативна детекція, реагування й відновлення в разі загроз та інцидентів.

5. Поглибити розуміння й поліпшити ефективність дій людини (персоналу), що сприяють безпеці АУ-критичного ПЗ і базованих на ньому платформ[67].

---

[62] Див.: URL: https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/critical-software-definition-explanatory
[63] Там само.
[64] Там само.
[65] Більше див.: Critical Software – Definition & Explanatory Material | NIST
[66] Див.: Security Measures for "EO-Critical Software" Use Under Executive Order (EO) 14028 (nist.gov)
[67] Там само.

Документ охоплює як основний обчислювальний інструментарій – захист кінцевої точки (*endpoint protection*), резервне копіювання даних, управління ідентифікацією та обліковими даними, операційні системи та контейнерні середовища тощо, так і ПЗ різного мережного статусу – від локального до хмарного.

Наприкінці жовтня 2021 р. Інститут оприлюднив другу редакцію (проєкт) Спеціальної публікації «Практики управління ризиками ланцюга постачань кібербезпеки для систем та організацій» (*Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (2nd Draft))*[68].

Документ розміщено для публічного обговорення та коментарів. Він надає рекомендації організаціям щодо виявлення, оцінки та пом'якшення ризиків ланцюга кіберпостачань на всіх рівнях своїх організацій. Видання інтегрує управління ризиками кіберланцюга постачань (*Cybersecurity Supply Chain Risk Management – C-SCRM*) у діяльність з управління ризиками, застосовуючи багаторівневий підхід, специфічний для *C-SCRM*, зокрема вказівки щодо випрацювання планів реалізації стратегії *C-SCRM*, політики *C-SCRM*, планів *C-SCRM* та оцінки ризиків *C-SCRM* для продуктів і послуг[69].

2.3. Кіберстрахування та оцінка ризиків

Попри численні кампанії з підвищення обізнаності, переважна більшість малих та середніх підприємств не практикують належної кібербезпеки. Нещодавній звіт про кіберготовність зараховує близько 75 % компаній до категорії «новачки»[70]. Половина всіх невеликих фірм у Німеччині не мають планів реагування на інциденти або відповідального за кібербезпеку співробітника; понад 70 % не проводять тренінгів з кібербезпеки для свого персоналу[71]. Лише п'ята частина опитаних компаній виконує базові вимоги. Якщо такий великий відсоток установ є вразливими до найпростіших шкідливих програм, здатність цифрового ринку бути стійким знижується.

Отже, коли більші компанії, що керують критично важливою інфраструктурою, посилюють захист, менші компанії дедалі частіше стають жертвами кіберзлочинців. Звіт про розслідування порушень даних *Verizon* виявив, що 43 % жертв кібератак – це малий бізнес[72]. Така тенденція особливо виразна щодо програм-вимагачів, де хакери навмисно націлюються на середні компанії – вони досить великі, щоб з них можна було щось вимагати, але недостатньо великі, щоб мати належний захист мережі[73]. Такі компанії є легшими об'єктами, ніж великі корпорації, і пропонують перспективу отримати більший прибуток.

---

[68] Див.: URL: https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/draft

[69] Там само.

[70] Hiscox, 2019. Cyber Readiness Report., p. 10. Див.: URL: https://www.hiscox.co.uk/sites/uk/files/documents/2019-04/Hiscox_Cyber_Readiness_Report_2019.PDF

[71] GDV (Gesamtverband der deutschen Versicherungswirtschaft). 2020, Cyber-Risiken im Mittelstand 2020. (Cyber risks in SMEs). Див.: URL: https://www.gdv.de/resource/blob/61466/0456901217b39a5893bc6829b8d7d156/report-cyberrisiken-im-mittelstand-2020-data.pdf

[72] Verizon. 2019. 2019 Data Breach Investigations Report. Див.: URL: https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

[73] Barlyn Suzanne. Global insurers face quiet strain from hacker ransom demands. *Reuters*. 2019. 25 Oct. URL: https://www.reuters.com/article/us-usa-ransomware-insurance/global-insurersface-quiet-strain-from-hacker-ransom-demands-idUSKBN1X41E3

Попри це багато невеликих компаній дотримуються скептичного погляду на кіберстрахування[74]. А враховуючи те, що кожен страховик дещо по-різному визначає такі ключові терміни, як «вимога» або «втрата даних», внутрішня політика страхових виплат часто є загальною, нечітко виписаною, тому її складно застосувати до кожного конкретного кейса.

Ще серйознішим ризиком є можливість зламу ланцюжка постачань, коли зловмисники використовують слабший захист менших компаній, щоб скомпрометувавши їх проникнути в складніші системи захисту великих компаній або державні установи. Ця тенденція є ключовим висновком Звіту про кіберготовність *Hiscox* за 2019 р., де вказано: 65 % компаній відчували проблеми, пов'язані з кібербезпекою у своїх ланцюгах постачань.

Сполучені Штати є, безумовно, найбільшим ринком полісів кіберстрахування – це близько 90 % світового ринку. Європа та Азія становлять решту 10 %[75]. Однією з головних причин цієї різниці є те, що всі штати США (починаючи з 2003 р. в Каліфорнії) мають закони про обов'язкове повідомлення щодо порушення даних[76].

Упровадження кіберстрахування в Європі певною мірою інтенсифікувалося з моменту набуття чинності законодавства про захист даних (*GDPR*) у травні 2018 р.[77]

Страхові компанії усвідомлюють: є серйозні проблеми з визначеннями, що використовують у різних політиках виплат компаній для опису того, який збиток покривається, а який ні. Особливо це залежить від ринкових умов, які стрімко змінюються[78]. Різноманіття внутрішніх політик виплат компаній та нестандартизованість свідчать – ринок досі не є сформованим[79].

Зараз діапазон покриття кіберризиків на ринку кіберстрахування є сегментованим і складається головно з поєднання традиційних страхових продуктів та незалежних кіберполісів. Світовий ринок кіберстрахування все ще недостатньо розвинений – компанії, що залежать від своїх ІКТ-спроможностей, переважно стимулюють попит на відповідні страхові продукти, але сегмент ринку все ще відносно обмежений. Недостатня прозорість та складність умов страхування є однією з основних причин відсутності корпоративного попиту на кіберстрахування.

Особливою проблемою є так званий «тихий кіберризик» – наслідок хибної практики, коли положення страхового поліса щодо конкретного кіберризику прописано неякісно. Зазвичай у такому разі чинні положення щодо страхування майна, страхування бізнесу або страхування збитків від сторонніх осіб просто доповнюють кількома не специфікованими пунктами про кібербезпеку. Обставини,

---

[74] Why 27 % of U. S. Firms Have No Plans to Buy Cyber Insurance. *Insurance Journal*. 2017. May 31. URL: https://www.insurancejournal.com/news/national/2017/05/31/452647.htm

[75] OECD (2017), Enhancing the Role of Insurance in Cyber Risk Management, OECD Publishing, Paris. http://dx.doi.org/10.1787/9789264282148-en

[76] Lubin, Asaf, The Insurability of Cyber Risk (September 12, 2019). Available at SSRN: https://ssrn.com/abstract=3452833 or http://dx.doi.org/10.2139/ssrn.3452833

[77] Lazaros G. Grigoriadis, 'Cybersecurity Insurance and New EU Cybersecurity and Data Protection Rules', (2017), 38, Business Law Review, Issue 6, pp. 210-218, https://kluwerlawonline.com/journalarticle/Business+Law+Review/38.6/BULA2017032

[78] Rawlings, Philip. (2014). Cyber Risk: Insuring the Digital Age. *Journal of the British Insurance Law Association, 128*, 1–16; Kesan, Jay P. and Hayes, Carol M., "Strengthening Cybersecurity with Cyberinsurance Markets and Better Risk Assessment" (2017). *Minnesota Law Review*. 85. 192–276.

[79] Xie, X., Lee, C. & Eling, M. Cyber insurance offering and performance: an analysis of the U.S. cyber insurance market. Geneva Pap Risk Insur Issues Pract 45, 690–736 (2020). https://doi.org/10.1057/s41288-020-00176-5

за яких можуть бути пред'явлені претензії після такого доповнення і якою може бути максимальна виплата, часто є незрозумілими як для клієнтів, так і для страховиків[80].

До прикладу – нещодавня судова справа. ТОВ «Національна компанія "Інк і Стич"» успішно подала позов проти страхової компанії на оплату заміни всієї ІТ-системи внаслідок атаки *ransomware (Plaintiff National Ink & Stitch, LLC («Plaintiff«)81.* Позивач вимагав відшкодувати витрати не лише щодо викрадених даних, а й щодо сповільненої ефективності власної комп'ютерної системи. Суд постановив, що на додаток до даних та програмного забезпечення позивача, які становлять захищене майно відповідно до умов поліса, позивач також продемонстрував пошкодження самої комп'ютерної системи. Таким чином, цей випадок започаткував прецедент: у страхуванні «фізична шкода» не обмежується фізичним знищенням або пошкодженням комп'ютерних систем, а містить і втрату доступу, і втрату використання та повноцінної функціональності системи.

Визначення кіберстрахування як передачі третій стороні фінансового ризику, пов'язаного з мережевими та комп'ютерними інцидентами, підводить нас до найбільшого системного ризику, з яким стикається страховий сектор із самого його початку – міжнародної війни та конфліктів.

Нині немає міжнародно визнаних загальних правил або достатньої кількості прецедентів, якими керуються страховики в питаннях атрибуції кібератаки, організатор якої – держава, що бере участь у збройному конфлікті з іншою державою.

Судовий процес між «Монделесом» (*Mondelez*) та «Цюрихом» (*Zurich*) ілюструє це щонайліпше. *Mondelez* – американська харчова компанія, одна з багатьох, які зазнали атаки зловмисного програмного забезпечення *NotPetya*. Саме воно мало не знищило корпорацію *Maersk* та спричинило глобальний збиток у близько 10 млрд дол. *Mondelez* утратив близько 100 млн дол. і вимагав повернути їх у свого постачальника страхового майна *Zurich*, оскільки 2015 р. до політики було додано єдине речення – щодо збитків, завданих «машинним кодом»[82]. Увагу до цієї справи привернув не сам позов, а відповідь *Zurich*. Компанія стверджувала: за нападом стоїть Росія, це була частина її конфлікту з Україною, США та іншими країнами, а отже, компанії взагалі не потрібно виплачувати позов, оскільки він потрапляє під політику виключення ризику війни. Справа триває, проте вже зараз оприявнилися слабкі сторони страхової логіки щодо природи інцидентів.

Поки що заохочення до регулювання галузі кіберстрахування проходять дуже повільно – *ENISA* опублікувала звіт, у якому ще в листопаді 2016 р. закликала Європейську комісію розпочати розслідування та врегулювати цей сектор, але

---

[80] Wrede, D., Stegen, T. & Graf von der Schulenburg, JM. Affirmative and silent cyber coverage in traditional insurance policies: Qualitative content analysis of selected insurance products from the German insurance market. *Geneva Pap Risk Insur Issues Pract* 45, 657–689 (2020). https://doi.org/10.1057/s41288-020-00183-6

[81] Civil Case No. SAG-18-2138. Попри те, що позивач здійснив запитуваний платіж, зловмисник і далі вимагав гроші та відмовився віддати програмне забезпечення й дані. Більше див.: URL: https://www.businessinsurance.com/article/20200204/NEWS06/912332879/Ransomware-cases-impact-could-be-far-reaching-National-Ink-&-Stitch-LLC-v-State

[82] Evans, Steve. Mondelez's NotPetya Cyber Attack Claim Disputed by Zurich. Reinsurance News. 2018. 17 Dec. URL: https://www.reinsurancene.ws/mondelezs-notpetya-cyber-attack-claim-disputed-by-zurich-report/

Комісія не дослухалася пропозиції та згодом навіть викреслила це питання зі списку пріоритетів *ENISA*[83].

За межами ЄС деякі країни, схоже, виявляють більше бажання діяти: Індія запровадить систему регулювання та просування кіберстрахування як частину своєї майбутньої національної стратегії кібербезпеки[84], а ізраїльська національна кібердирекція (*Israeli National Cyber Directorate*), працюючи в партнерстві зі страховими компаніями та іноземними урядами, пообіцяла перетворити Ізраїль на майданчик для кіберрегулювання страхування, щоб перевірити можливі шляхи розв'язання проблем, які стримують ринок кіберстрахування[85].

Поряд зі звітом *ENISA* є й інші рекомендації. Так, звіт Організації економічного співробітництва та розвитку для засідання міністрів фінансів G7 рекомендував, що страхування треба розглядати як важливий складник стратегій країн щодо розв'язання проблем цифрової безпеки[86]. У звіті також є звернення до страхових компаній надати більшої ясності стосовно того, що конкретно охоплює їхня внутрішня страхова політика. Запропоновано на державному рівні брати до уваги питання кіберстрахування, розробляючи стратегії управління фінансовими наслідками кіберінцидентів.

2.4. Сертифікація

Сертифікація кібербезпеки є офіційним підтвердженням того, що цифрові продукти, послуги та процеси ІКТ відповідають певним визначеним вимогам. Зокрема, схеми сертифікації кібербезпеки передбачають критерії для проведення оцінки відповідності із вичерпним набором правил, стандартів та процедур. Таким чином, сертифікація забезпечує впевненість користувачів у рівні відповідності та відіграє важливу роль у встановленні й підтримці належного рівня довіри та безпеки до продуктів, послуг і процесів. Хоч до питання розвитку сертифікації у сфері кібербезпеки взялися одразу декілька міжнародних гравців, найцілісніше та найпослідовнішою є політика ЄС. Сьогодні в Європі є *різні схеми сертифікації* безпеки для продуктів ІКТ, що спричиняє фрагментацію ринку та створює надлишкові бар'єри[87].

Сертифікація, яка складається з офіційної оцінки *незалежним акредитованим органом* щодо відповідності визначеному цим уповноваженим органом влади (стосовно Німеччини – це *BSI*, на рівні ЄС – *ENISA*) набору критеріїв, та ***видача сертифіката***, що свідчить про відповідність, **відіграють важливу роль у підвищенні довіри та безпеки до продуктів та послуг**. Хоч оцінка безпеки є цілком технічною сферою, сертифікація інформує покупців та користувачів про

---

[83] Cyber Insurance: Recent Advances, Good Practices and Challenges / ENISA (European Union Agency for Cyber Security). 2016. URL: https://www.enisa.europa.eu/publications/cyber-insurance-recent-advances-good-practices-and-challenges

[84]Chunduru, Aditya. 'National Cyber Security Strategy Will Have Framework For Cyber Insurance': Rajesh Pant / Medianama. 2020. 22 October. https://www.medianama.com/2020/10/223-cybersecurity-policy-to-have-cyber-insurance-framework/

[85] Lubin, Asaf, Cyber Insurance As Cyber Diplomacy (October 11, 2020). Asaf Lubin, Cyber Insurance as Cyber Diplomacy, Cyber War & Cyber Peace in the Middle East: Digital Conflict in the Cradle of Civilization pp.22-37 (Michael Sexton and Eliza Campbell eds., Middle East Institute, 2020)., Available at SSRN: https://ssrn.com/abstract=3709322 or http://dx.doi.org/10.2139/ssrn.3709322

[86] OECD (2017), Enhancing the Role of Insurance in Cyber Risk Management, OECD Publishing, Paris, https://doi.org/10.1787/9789264282148-en

[87] Див.: URL: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework

властивості безпеки продуктів та послуг ІКТ. Це особливо актуально для нових технологій, які вимагають високого рівня безпеки, – технологій на базі штучного інтелекту, електронних систем охорони здоров'я, систем управління промисловою автоматизацією (*IACS*) або інтелектуальних мереж.

У сфері розвитку сертифікації є низка міжнародних ініціатив, зокрема т. зв. Загальні критерії (*Common Criteria – CC*) оцінки безпеки інформаційних технологій (*ISO 15408*). Цей стандарт передбачає сім рівнів забезпечення оцінки (*Evaluation Assurance Levels – EAL*). *CC* та супутня загальна методологія оцінки безпеки інформаційних технологій (*Common Methodology for Information Technology Security Evaluation – CEM*) є технічною основою міжнародного документа – Загальної угоди про визнання критеріїв (*Common Criteria Recognition Arrangement – CCRA*), яка забезпечує визнання сертифікатів *CC* усіма підписантами *CCRA*. Однак у поточній версії *CCRA* взаємно визнаються лише оцінки до *EAL*. Україна не є підписантом[88], хоча може приєднатися до відповідної угоди. Водночас ще Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України (наразі – Держспецзв'язку) прийняв нормативний документ технічного захисту інформації 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу». НД ТЗІ 2.5-004 розроблено на основі т. зв. Канадських критеріїв (*Canadian Trusted Computer Product Evaluation Criteria – CTCPEC*), які також було використано для розроблення *Common Criteria*[89].

Паралельно діє чи впроваджується низка ініціатив із сертифікації ІКТ у державах-членах, що несе ризик фрагментації ринку. Зрештою компанії може знадобитися проходити кілька процедур сертифікації в різних державах-членах, щоб мати можливість пропонувати свою продукцію на різних ринках.

Така ситуація призводить до більших витрат і становить значне адміністративне навантаження для компаній, що працюють у кількох державах-членах ЄС.

Наприклад, вартість отримання сертифіката «*Smart Meter Gateway*» від Німецького федерального міністерства захисту інформації (*Bundesamt für Sicherheit in der Informationstechnik – BSI*)[90] становить понад 1 млн євро (найвищий рівень випробувань і гарантій стосується не лише одного продукту, а й усієї інфраструктури навколо нього). Вартість сертифікації розумних лічильників у Франції становить близько 150 000 євро або й більше[91].

Гармонізація вимог до сертифікації кібербезпеки дає можливість створити єдиний цифровий ринок усіх товарів та послуг. Сьогодні в ЄС немає гармонізованих вимог щодо самооцінки, але є низка стандартів, які організації можуть використовувати для оцінки своєї продукції чи послуг на відповідність.

---

[88] Див.: URL: https://www.commoncriteriaportal.org/ccra/members/

[89] Див.: URL: https://tzi.ua/assets/files/%D0%9D%D0%94-%D0%A2%D0%97%D0%86-2.5-004-99.pdf

[90] Інтелектуальна вимірювальна система Smart Meter Gateway (SMGW) з інтегрованим модулем безпеки є центральним компонентом, який отримує та зберігає дані вимірювань від лічильників і готує їх для учасників ринку. SMGW спілкується з різними компонентами та залученими гравцями ринку для передачі даних про споживання, а також для їх адміністрування. Див.: URL: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Smart-metering/Smart-Meter-Gateway/smart-meter-gateway_node.html

[91] Див.: URL: https://www.ecs-org.eu/documents/uploads/european-cybersecurity-certification-assessment-options.pdf

Метою системи сертифікації кібербезпеки ЄС згідно із Законом ЄС про кібербезпеку 2019/881 (*Регламент (ЄС) 2019/881* Європейського парламенту та Ради від 17 квітня 2019 р. про *ENISA*[92] і про сертифікацію кібербезпеки інформаційно-комунікаційних технологій та скасування Регламенту (ЄС) № 526/2013 (*Закон про кібербезпеку*) / Regulation (EU) 2019/881 of 17 April 2019 *on ENISA on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013* (*Cybersecurity Act*))[93] є встановлення та підтримка довіри й безпеки щодо продуктів, послуг та процесів кібербезпеки. Складання схем сертифікації кібербезпеки на рівні ЄС має на меті надати критерії для проведення оцінки відповідності, щоб установити ступінь відповідності продуктів, послуг та процесів конкретним вимогам.

Як зазначено в Законі (ЄС) 2019/881, система сертифікації кібербезпеки ЄС установлює процедуру створення схем кіберсертифікації ЄС, що охоплює продукти, послуги та процеси ІКТ. Кожна схема визначатиме один або кілька рівнів забезпечення (*базовий, суттєвий або високий)* на основі рівня ризику, пов'язаного з передбачуваним використанням продукту, послуги чи процесу (ст. 52)[94]. Схеми сертифікації кібербезпеки держав-членів перебувають в ієрархічній позиції після сертифікаційних схем ЄС, на базі яких і реалізуються. Відповідності схемам сертифікації ЄС можна досягнути шляхом самооцінки або через третій орган з оцінки відповідності.

Національні органи із сертифікації кібербезпеки (як-от німецьке Федеральне міністерство захисту інформації (*Bundesamt für Sicherheit in der Informationstechnik – BSI*) повинні чітко розподіляти обов'язки між персоналом, який видає сертифікати кібербезпеки, і тими, хто контролює та забезпечує дотримання схеми. Національні органи із сертифікації кібербезпеки підлягають експертній перевірці.

Натепер дотримання схем сертифікації кібербезпеки є добровільним – якщо інше не встановлено законодавством держав-членів. Європейська комісія регулярно оцінює схеми сертифікації кібербезпеки, щоб визначити, чи треба їх робити обов'язковими. Першу таку оцінку мають здійснити до 31 грудня 2023 р.

Водночас Європейський Союз поступово створює цілу інфраструктуру сертифікаційного процесу.

Його основу закладає Закон ЄС про кібербезпеку[95], який: створює систему сертифікації кібербезпеки ЄС та вимагає від держав-членів призначити один або кілька національних органів із сертифікації кібербезпеки; створює органи з оцінки – щоб визначити відповідність імплементації Закону; вимагає від держав-членів окреслити покарання за порушення сертифікації кібербезпеки.

Закон описує 22 необхідні елементи схем сертифікації, зокрема: види продукції, послуг або процесів; критерії оцінки; правила контролю за дотриманням; наслідки для невідповідності; умови взаємного визнання сертифікації з третіми країнами; а також формат та процедури, яких повинен дотримуватися виробник або постачальник під час надання додаткової інформації. Схеми сертифікації мають переглядати що п'ять років[96].

---

[92] Агентство Європейського Союзу з кібербезпеки.
[93] Див.: URL: https://eur-lex.europa.eu/eli/reg/2019/881/oj
[94] Див.: URL: https://eur-lex.europa.eu/eli/reg/2019/881/oj
[95] Див.: URL: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32019R0881
[96] Див.: URL: https://eur-lex.europa.eu/eli/reg/2019/881/oj

Закон передбачає, що загальноєвропейські схеми сертифікації ухвалить Європейська комісія. Кожна схема сертифікації визначатиме:

- категоризацію продуктів;
- вимоги до кібербезпеки для кожного продукту (посилання на стандарти або технічні специфікації);
- тип необхідної оцінки (самооцінка або оцінка третьою стороною);
- запланований рівень безпеки (базовий, суттєвий або високий).

Процес розроблення та прийняття європейської схеми сертифікації проходить у п'ять етапів[97], за які відповідає декілька груп та стейкхолдерів і які діють за чітким алгоритмом:

1. Європейська група сертифікації кібербезпеки *(European Cybersecurity Certification Group – ECCG*) та Група із сертифікації кібербезпеки зацікавлених сторін (*Stakeholder Cybersecurity Certification Group – SCCG*) – робочі групи, що розробляють стандарти схем сертифікації.
2. Європейська Комісія просить *ENISA* підготувати проєкт схеми сертифікації.
3. *ENISA* готує проєкт схеми сертифікації.
4. *ENISA* консультує галузь та зацікавлені сторони.
5. Європейська Комісія ухвалює схему сертифікації. Кожна схема сертифікації може визначати один або декілька рівнів забезпечення: базовий, суттєвий або високий – з огляду на рівень ризику, пов'язаного з товаром, послугою чи процесом.

Обидві групи (*ECCG* та *SCCG*) консультують Європейську комісію з питань сертифікації кібербезпеки, консультують *ENISA* щодо сертифікації та стандартизації і допомагають Європейській комісії в постійній робочій програмі для схем сертифікації. Після того, як Закон набрав чинності 27 червня 2019 р., Європейська комісія опублікувала інформацію про подання заявок на участь у Комісії організаціям приватного сектора з метою долучитися до захисту інтересів своїх організацій.

Відповідно до ст. 62 Закону ЄС про кібербезпеку[98] **Європейська група із сертифікації кібербезпеки** *(European Cybersecurity Certification Group – ECCG)* має складатися з представників національних органів із сертифікації кібербезпеки або представників інших відповідних національних органів.

Зацікавлені сторони та відповідні треті сторони можуть бути запрошені брати участь у роботі групи. Завдання групи:

- консультувати й сприяти Європейській комісії в її роботі з питань політики сертифікації кібербезпеки, координації політичних підходів та підготовки європейських схем сертифікації кібербезпеки;
- допомагати, консультувати та співпрацювати з *ENISA* з питань підготовки схем кандидатів відповідно до ст. 49;
- ухвалити висновок щодо схем кандидатів, підготовлених *ENISA* відповідно до ст. 49;
- ухвалити висновки, адресовані Комісії, щодо обслуговування та перегляду чинних європейських схем сертифікації кібербезпеки;

---

[97] Див.: URL: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework
[98] Див.: URL: EUR-Lex – 32019R0881 – EN – EUR-Lex (europa.eu)

- вивчати відповідні події в галузі сертифікації кібербезпеки й обмінюватися інформацією та передовою практикою щодо схем сертифікації кібербезпеки;
- сприяти співпраці між національними органами із сертифікації кібербезпеки відповідно до цього Розділу, зокрема шляхом установлення методів ефективного обміну інформацією, що стосуються сертифікації кібербезпеки;
- сприяти узгодженню європейських схем сертифікації кібербезпеки з міжнародно визнаними стандартами, зокрема шляхом перегляду чинних європейських схем сертифікації кібербезпеки та, за необхідності, надання рекомендацій *ENISA* щодо взаємодії з відповідними міжнародними організаціями стандартизації – для усунення хиб або прогалин у наявних міжнародно визнаних стандартах.

У регулярному діалозі із цією групою паралельно діє ще одна робоча структура – **Група із сертифікації кібербезпеки зацікавлених сторін** *(Stakeholder Cybersecurity Certification Group – SCCG).* До неї, відповідно до ст. 22 Закону ЄС про кібербезпеку, за прозорим та відкритим конкурсом, на основі пропозиції *ENISA* Європейська комісія обирає членів *для забезпечення* балансу між представниками різних груп інтересів, а також відповідного гендерного балансу та географічної репрезентативності. Група відповідає за консультування Комісії та *ENISA* щодо стратегічних питань кіберсертифікації та надання Комісії допомоги в підготовці постійної робочої програми Європейського Союзу. Це перша *група експертів* з питань сертифікації кібербезпеки, заснована Європейською Комісією.

Загальна *місія* групи полягає в підтримці та сприянні стратегічним питанням, що стосуються європейської системи сертифікації кібербезпеки. За запитом група надає консультації *ENISA* із загальних та стратегічних питань щодо завдань *ENISA* зі стандартизації та сертифікації кібербезпеки. Група має до 50 членів з різних організацій, серед яких – академічні установи, споживчі організації, органи з оцінки відповідності, організації зі стандартизації, компанії і торгові асоціації та інші організації, що діють у Європі та зацікавлені в сертифікації кібербезпеки.

До групи входять представники від європейських організацій стандартизації, як-от: Європейський комітет зі стандартизації *(European Standardisation Organisations*), Європейський комітет з електротехнічної стандартизації (*European Committee for Electrotechnical Standardisation – Cenelec*), Європейський інститут телекомунікаційних стандартів (*European Telecommunications Standards Institute – ETSI*). У групі також беруть участь органи міжнародної стандартизації, серед них: Міжнародна організація зі стандартизації (*International Organisation for Standardisation – ISO*), Міжнародна електротехнічна комісія (*International Electrotechnical Commission – IEC*) та Міжнародний союз телекомунікацій (*International Telecommunication Union – ITU*), Європейська кооперація з акредитації (*European co-operation for Accreditation – EA*) та Європейські рада захисту даних (*European Data Protection Board – EDPB*).

На запит Європейської комісії, відповідно до ст. 48.2 Закону ЄС про кібербезпеку, *ENISA* створила третю робочу групу – т. зв. **Тимчасову робочу групу** (*Ad Hoc Working Group – AHWG*). ЇЇ призначення – підтримати підготовку схеми сертифікації кібербезпеки країн-кандидатів до членства в ЄС на базі чинних схем, що діють за *SOG-IS MRA* (*Senior Officials Group Information Systems Security Mutual Recognition Agreement* – Угода про групу найвищих посадових осіб з питань взаємного визнання інформаційних систем).

Група розпочала свою діяльність 27 листопада 2019 р. і має у складі двадцять членів, що представляють галузь (розробників, оцінювачів), а також близько дванадцяти представників органів з акредитації держав-членів ЄС. У групі проводили регулярні обговорення. Після внутрішнього огляду *ENISA* консолідували таку схему *EUCC* (схема сертифікації кібербезпеки, що базується на Єдиних критеріях), яка розглядає питання сертифікації кібербезпеки продуктів ІКТ на основі Загальних критеріїв, Загальної методології оцінки безпеки інформаційних технологій та відповідних стандартів відповідно до ISO/IEC 15408 та ISO/IEC 18045. Група складається з представників національних органів із сертифікації кібербезпеки або представників інших відповідних національних органів країн не членів ЄС. Зацікавлені сторони (експерти) та відповідні треті сторони (представники країн не членів ЄС) можуть бути запрошені брати участь у засіданнях групи.

Самі **схеми сертифікації кібербезпеки ЄС** забезпечують гармонізовані критерії для проведення оцінки відповідності. Європейські сертифікати кібербезпеки уможливлюють, з одного боку, просте уніфіковане розуміння для споживачів, з іншого – надають складні деталі для використовування товарів у ланцюзі постачань у сертифікованих умовах. Закон ЄС про кібербезпеку чітко зазначає: сертифікація є добровільною, якщо європейським або національним законодавством не передбачено інше. Однак Європейська комісія повинна регулярно оцінювати ефективність та використання прийнятих схем сертифікації – не пізніше як з 31 грудня 2023 р. й далі що два роки. Комісія, зокрема, оцінить, чи має конкретна схема стати обов'язковою через відповідне законодавство Союзу, щоб забезпечити адекватний рівень кібербезпеки продуктів, послуг і процесів та поліпшити функціонування внутрішнього ринку. На основі своєї оцінки Комісія визначить продукти, послуги та процеси, охоплені чинною схемою сертифікації, яка своєю чергою підпорядкована обов'язковій схемі.

Приватні компанії, що пропонують продукт, послугу чи процес у галузі ІКТ на ринках ЄС, зобов'язані:

- моніторити рішення *ENISA* та новини в ЄС щодо оновлення схем сертифікації кібербезпеки ЄС;
- подати заявку на членство у відповідній робочій групі;
- заналізувати ризики, пов'язані з недотриманням схем сертифікації. Закон дозволяє кожній державі-члену визначати штрафи за невиконання або порушення схем сертифікації. Штрафи мають бути «ефективними, пропорційними та переконливими»;
- зрозуміти вимоги щодо надання додаткової інформації або повідомлень про виявлені вразливості чи «помилки» в продукті, послузі чи процесі; а також випрацювати механізми оновлення, відкликання чи вилучення;
- визначити внутрішню інформацію, яка є комерційно конфіденційною та вимагає захисту від розголошення;
- отримати консультації експертів щодо схем сертифікації кібербезпеки ЄС та Закону, особливо зважаючи на потенційні обов'язкові вимоги (зауважмо, що *OES* та постачальники цифрових послуг мають обов'язкові вимоги щодо кібербезпеки згідно з Директивою *NIS*).

Реалізація системи сертифікації кібербезпеки, якій сприяє Закон про кібербезпеку ЄС, є ключем до збільшення довіри та, відповідно, обізнаності про кібербезпеку систем ІКТ. Однак це вимагає спільних зусиль органів сертифікації, виробників та постачальників. Таким чином, сьогодні важливо підвищити

обізнаність щодо проблем сертифікації кібербезпеки, аби кінцеві користувачі могли відчути переваги сертифікації, а отже – надійніших цифрових продуктів.

Попри визнаний європейськими гравцями позитив від сертифікації, є й низка ***викликів***, які можуть ускладнити цей процес – як на етапі впровадження, так і майбутньої реалізації. Розгляньмо їх.

Процеси компонування. Серед викликів сертифікації можна назвати процеси компонування та оновлення програмного забезпечення, які впливають на сертифікацію всієї системи та її компонентів протягом їхнього життєвого циклу – ці аспекти важливі для виробників і постачальників ПЗ, а також фахівців із сертифікації кібербезпеки для визначення взаємозв'язку між різними схемами сертифікації.

Повторна сертифікація. Оновлення ПЗ також може вплинути на сертифікацію кібербезпеки програмних компонентів, адже можливою є повторна сертифікація системи. Через потенційну вартісність процесу повторної сертифікації виробники та постачальники ПЗ можуть неохоче випускати регулярні оновлення для своїх систем або оновлювати системи без використання процесу повторної сертифікації. Проблема заохочення постачальників ПЗ повторно сертифікувати свої оновлені системи досі є предметом дискусій.

Рівні гарантії. Є проблема рівнів гарантії для процесів сертифікації кібербезпеки – що саме необхідно сертифікувати та наскільки глибоко. Оцінюючи компонент ПЗ, треба враховувати систему, у якій цей компонент буде розгорнуто, а також різні рівні гарантії для процесу сертифікації (ці рівні визначає Закон про кібербезпеку ЄС).

Гнучкість. Необхідно також, аби схеми сертифікації забезпечували високий рівень гнучкості для адаптації до мінливого технологічного середовища.

Добровільність проти обов'язковості. Багатьом експертам видається недостатньою схема добровільної сертифікації. Є пропозиції, щоб майбутні схеми сертифікації містили чітко окреслене забезпечення виконання всього життєвого циклу продукту: періоду й частості гарантованих оновлень; санкцій у разі невиконання вимог тощо.

ІІІ. ФОРМУЮЧИ УКРАЇНСЬКУ ВІДПОВІДЬ

Україна перебуває в стадії активних бойових дій та не менш активного кіберпротистояння. РФ шукає все нових шляхів атакувати інформаційні системи як державних органів, так і об'єктів критичної інфраструктури (ОКІ). Наразі публічно відомих даних про успішні кібератаки на ОКІ немає, а ті, що були вдалими для ворожої кіберактивності, не спричинили важких наслідків[99].

Однак раніше Україна вже потерпала від АчЛП – прикладом є зараження вірусом ***NotPetya:*** зловмисники спочатку атакували компанію *розробника популярної бухгалтерської програми M.E.Doc*, а потім вбудували шкідливе ПЗ до регулярних оновлень її програмного забезпечення і, використовуючи довірений канал для оновлень (оскільки такі оновлення не перевірялись системами кібербезпеки), змогли потрапити до систем значної кількості державних та недержавних об'єктів. Найсвіжіший кейс такої кібератаки – подія 13 січня 2022 р. (яку іноді називають ***#attack13***), коли постраждали одразу 70 державних ресурсів, 10 з яких зазнали несанкціонованого втручання. За даними Держспецзв'язку, зловмисники зламали інфраструктуру комерційної компанії, що мала доступ з правами адміністрування до вебресурсів, які постраждали внаслідок атаки[100]. Тобто АчЛП не лише не припиняються, але розвиваються й далі.

В Україні склалася ситуація, властива державам переважно без чіткої та зрозумілої політики або програми протидії АчЛП. Це зумовлено не так новизною атак, як складністю вибудовування системи захисту від них без посилення надмірного державного регулювання, зменшення простору для діяльності приватних ІТ-компаній (та можливості залучати їхні продукти до діяльності державних органів), а також уведення все нових обмежень на використання певних програмних продуктів.

Особливої актуальності це набуває з огляду на стрімку цифрову трансформацію державного управління та зростання кількості державних послуг, що переходять у режим онлайн. Частиною цієї проблеми є зростання рівня інформатизації на об'єктах критичної інфраструктури, які мають власні політики кібербезпеки, що не завжди враховують особливі вимоги до кібербезпеки постачальників. Варто відзначити, що й державні органи лише в обмеженому масштабі висувають такі вимоги до потенційних постачальних послуг. Винятками можна назвати вимогу до операторів (провайдерів) телекомунікації надавати доступ до інтернету органам, підприємствам, установам і організаціям державної форми власності з використанням захищених вузлів доступу, тобто таких, де створено комплексну систему захисту інформації.

Україна у своїх нормативних документах майже не згадує проблему протидії АчЛП. Водночас частину питань розглядають у межах іншої концепції – стійкості щодо відновлення діяльності після деструктивних дій та продовження виконання функцій навіть в умовах атаки.

Уперше «стійкість» як базовий концепт національної системи кібербезпеки згадано в Стратегії національної безпеки 2020 р. – це «здатність суспільства та держави швидко адаптуватися до змін безпекового середовища й підтримувати стале

---

[99] Див.: URL: https://biz.nv.ua/ukr/experts/kiberataki-rosiji-na-ukrajinu-yak-prohodyat-ta-chim-zagrozhuyut-ostanni-novini-50236927.html

[100] Див.: URL: https://cip.gov.ua/ua/news/derzhspeczv-yazku-z-yasuvala-yak-khakeri-zlamali-saiti-derzhustanov-sho-stalosya?fbclid=IwAR0zljYDf2Bc9u7e37SsYvEmT0ibzu27D6WjMuhSElKZadhGOTwUYfCWJUw

функціонування, зокрема шляхом мінімізації зовнішніх і внутрішніх уразливостей». А завдання 52 цього ж документа визначало основним напрямом розвитку системи кібербезпеки «гарантування кіберстійкості та кібербезпеки національної інформаційної інфраструктури, зокрема в умовах цифрової трансформації».

У Стратегії кібербезпеки України 2021 р. для кіберсфери «стійкість» додатково конкретизовано через поняття «кіберстійкість», що визначено як «набуття здатності швидко адаптуватися до внутрішніх і зовнішніх загроз у кіберпросторі, підтримувати та відновлювати стале функціонування національної інформаційної інфраструктури, насамперед об'єктів критичної інформаційної інфраструктури»[101].

Набуття такої здатності реалізують через низку стратегічних цілей:

- **національна кіберготовність та надійний кіберзахист**. У центрі цього завдання – забезпечення економічного добробуту та захисту прав і свобод кожного громадянина України, що неможливо без набуття здатності всіх зацікавлених сторін своєчасно й ефективно реагувати на кібератаки, забезпечити режим постійної готовності до реальних та потенційних кіберзагроз, виявляти та усувати передумови до їх виникнення (фактично реалізуючи цикл *NIST CSF*), забезпечивши тим самим кіберстійкість. У цьому ж контексті вказано на потребі забезпечити кіберстійкість передусім об'єктів критичної інформаційної інфраструктури. Це поняття визначено в нормативних документах окремо: «кіберстійкість критичної інформаційної інфраструктури – стан критичної інформаційної інфраструктури, за якого забезпечується її спроможність надійно функціонувати та надавати основні послуги в умовах кіберзагроз»[102];
- **професійне вдосконалення, кіберобізнане суспільство та науково-технічне забезпечення кібербезпеки**. Кібербезпека – це здебільшого про людей та процеси, а не про технології як такі. Саме тому якісно навчені кадри та передові дослідження (не лише теоретичні, але і впроваджені в практику) є основою успішного розвитку кібербезпеки та забезпечення кіберстійкості. Цього досягають як збільшенням видатків на НДР, так і зміною програм підготовки фахівців, зробивши їх комплекснішими й такими, що відповідають потребам ринку;
- **безпечні цифрові послуги**. Зважаючи на процеси цифровізації державних послуг та загалом економіки, безпека цифрових послуг перебуває в центрі уваги. На цьому шляху важливим є розвиток кваліфікованих електронних довірчих послуг, підвищення ефективності системи захисту персональних даних та багато іншого.

Водночас Стратегія прямо не згадує проблему безпеки ланцюга постачання – ані як загрози, ані як мети захисту. Та цілу низку запропонованих заходів де-факто спрямовано на розв'язання частини цієї проблеми. Зокрема, мова йде про завдання «впровадження системи сертифікації продукції, яка використовується для функціонування та кіберзахисту інформаційно-комунікаційних систем, насамперед об'єктів критичної інформаційної інфраструктури» та «забезпечення функціонування та розвитку Національного центру резервування державних інформаційних ресурсів, проведення модернізації системи захищеного доступу державних органів до мережі Інтернет».

---

[101] Див.: URL: https://www.president.gov.ua/documents/4472021-40013

[102] Порядок проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом. Див.: URL: https://zakon.rada.gov.ua/laws/show/1176-2020-%D0%BF#Text

У підзаконних НПА, прийнятих у 2020 – 2021 рр., частково враховано ризики, пов'язані з АчЛП, і передбачено узгоджений з міжнародними стандартами порядок дій з управління цими ризиками. Так, у наказі Адміністрації Держспецзв'язку від 06 жовтня 2021 р. № 601 Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури, «організація ідентифікує та класифікує постачальників у відповідних ланцюгах постачань», а також визначає «вимоги з обробки ризиків, які пов'язані з безпекою постачання» відповідно до стандартів ДСТУ ISO/IEC 27001:2013, COBIT 5 та NIST SP 800-53 Rev. 5[103]. Однак це стосується лише об'єктів ОКІ й поки що може розглядатися лише як один з елементів цілісної, координованої та стимульованої державою політики в питанні АчЛП , якої в Україні натепер немає.

Частково функцію визначення стану кібербезпеки потенційних підрядників міг би виконувати незалежний аудит інформаційної безпеки, який нині є обов'язковим лише для ОКІ, однак до сьогодні інфраструктуру проведення таких аудитів (порядок, цілі та вимоги до суб'єктів проведення) Кабінет Міністрів України не визначив.

На що Україна має звернути уваги пріоритетно, розглядаючи питання посилення своїх спроможностей протидіяти АчЛП в довгостроковій перспективі?

Передусім – **якісна оцінка наявного**. Кейс *#attack13* показав, що ми досі не зробили повну оцінку уроків з атаки *NotPetya*. Немає адекватних даних про наявність вразливостей, чи дійсно щось змінилось у заходах кібербезпеки або кіберзахисту.

Друге – **стандарти та настанови (і їх практичне впровадження)**. Україна не має наразі аналогів таких настанов, як «Менеджмент ризиків, пов'язаних із забезпеченням безпеки ланцюжка постачань» від *NIST*. Тим часом найліпші практики варто адаптувати та максимально впроваджувати. Форми такої адаптації є предметом діалогу, але однією з них можуть бути «Рекомендації», що їх затверджують спільними рішеннями різні суб'єкти кібербезпеки.

Третє – **поширення найліпших практик у максимально доступній формі**, щоб їх могли зрозуміти навіть ті організації, які не мають істотної експертизи у сфері кібербезпеки. Першим кроком тут могли б стати рекомендації (можливо, поширені НКЦК чи іншими основними суб'єктами національної системи кібербезпеки) для державних установ та приватних організацій стосовно того, чим є АчЛП та що можна зробити вже тут і зараз для того, або зменшити цю загрозу.

Четверте – **політика «нульової довіри»**. Маємо вже зараз почати оцінку нашої *готовності* її впроваджувати, але також і її *доцільності* – треба зважати не лише на потенційні вигоди, але й на наші реальні фінансові та організаційні ресурси. Це не та історія, до якої можна братися винятково романтично – треба оцінювати свої можливості максимально раціонально.

П'яте – **кіберстрахування та сертифікація**. Ринок кіберстрахування в Україні майже не розвивається. Це складна й нова сфера, де правила та механізми оцінки збитків все ще мало опрацьовано. Деякі компанії на українському ринку надають відповідні послуги, але системному впровадженню заважає відсутність адекватної нормативно-правової бази. Страхування частково закладено на рівні закону про критичну інфраструктуру (хоч і з відтермінуванням на три роки) і, найімовірніше, буде згадано в оновленому законі про кібербезпеку. У питанні сертифікації нам важливо зіставити наші підходи з баченням європейських колег та

[103] Див.: URL: https://bit.ly/3CzHUMl (Додаток 1, Таблиця 2).

рухатися синхронно. Зараз це частково функція ліцензування та сертифікації, які реалізує ДССЗЗІ.

Шосте – **міжнародна взаємодія**. Неможливо побороти транскордонну проблему самотужки. Швидкий та ефективний обмін наявною інформацією про вектори атаки, поширення, механізми припинення та оперативний обмін – усе це надзвичайно важливо саме для ситуацій, пов'язаних з АчЛП. Безумовно, це порушує й питання якості партнерства між державними та приватними органами, адже найчастіше жертвами таких атак стають саме останні. Отже, це знову повертає нас до питання розбудови довіри та не просто нормативного врегулювання ДПП, але створення дієвих форм оперативного співробітництва.

ВИСНОВКИ

2020 р. АчЛП активізувались і призвели до масових заражень користувачів з державного й приватного секторів та витоку чутливої для них інформації. Переважно ці атаки не мали прямого відношення до фінансово мотивованих злочинів і можуть вважатись такими, що їх спонсорували держави. Провідні дослідницькі центри звертають увагу на безпрецедентні масштаби хвилі АчЛП, а також на значну частку (близько половини) особливо небезпечних нападів класу *Advanced Persistence Threat (APT)*. Наголошують на таких загрозах: ***«каскадний ефект» атак*** (шкідливе ПЗ після ураження цільового клієнта може ще тривалий час залишатися в мережах і ланцюгах постачань, реплікуватися й ставити під постійну загрозу цілі інфраструктури, бізнес-сегменти і т. ін.) та ***багатоетапні вдосконалені АчЛП*** класу *APT*, які, окрім завдання величезних логістичних, фінансово-економічних та інших утрат, можуть виконувати кібершпигунські завдання. Загалом проведений аналіз інцидентів та реагування на них офіційних структур різних країн доводить до таких висновків.

• Агентство Європейського Союзу з кібербезпеки (*ENISA*) констатує, що навіть найдосконаліших локальних систем кібербезпеки недостатньо для захисту організацій в умовах розгортання нинішньої хвилі АчЛП, а отже, ситуація вимагає термінових спільних дій, послідовного впровадження найліпших практик (*good practices*) на рівні ЄС. За ініціативою Єврокомісії нині триває формування моделі кібербезпеки ЄС на засадах створення єдиної відкритої міжгалузевої платформи з кібербезпеки, зокрема – створення Спільного кіберпідрозділу ЄС (*Joint Cyber Unit – JCU*).

• Найпоказовішою виявилася кібератака *Sunburst* (США), унаслідок якої постраждали як урядові агенції, так і транснаціональні ІТ-компанії США (зокрема й ті, що професійно займаються кібербезпекою). Це свідчить про тотальну вразливість компаній будь-якого рівня перед АчЛП. Звіт Рахункової палати США від 15 грудня 2020 р. показав, що більшість американських урядових агентств не врахували рекомендації Національного інституту технологічних стандартів США (*NIST*) щодо заходів із протидії таким атакам, що підвищило їхню вразливість.

• Більшість розгорнутих у США систем раннього виявлення кібератак виявилися неспроможними зреагувати на ворожу кіберактивність. Це засвідчує потребу вдосконалювати заходи кібербезпеки не тільки щодо встановлення сенсорів раннього виявлення підозрілої активності, але й щодо зміни організаційних підходів до кібербезпеки – концепцію «периметра захисту» заступає «екосистема кібербезпеки», що охоплює не лише сам об’єкт захисту, але й сукупність його постачальників.

• США ставлять на власні відпрацьовані моделі функціонування виконавчої влади та міжвідомчої взаємодії, а також на експертну підтримку *NIST*. У виданому в травні 2021 р. **Указі Президента США щодо вдосконалення національної кібербезпеки (*Executive Order on Improving the Nation’s Cybersecurity*)** проблемі АчЛП присвячено окремий розділ, де викладено однорічний багатоетапний план підвищення спроможностей захисту від цієї загрози. Суть плану полягає в тотальній перевірці ПЗ федеральних агентств та вилученні з ужитку (видаленні) того програмного продукту, який не відповідає новим критеріям «критичного ПЗ».

• Концепцію *Zero Trust* (*ZTA*) розроблено понад 10 років тому, але її ніколи не розглядали як пріоритетну модель та/чи стратегію кібербезпеки – вона мала статус

«однієї з багатьох». У фокусі уваги урядів та дослідницьких центрів *ZTA* опинилася лише на межі 2020 і 2021 рр. у зв'язку з глобальною хвилею АчЛП. *ZTA* фокусується на захисті об'єктів, а не локацій, на принципах тотальної перевірки («презумпція винуватості») та мікросегментації мереж.

• У низці експертних напрацювань **обґрунтовано також високу ефективність** застосування архітектури нульової довіри *ZTA* в боротьбі з АчЛП – насамперед через фундаментальні, системні переваги цього підходу, як порівняти з традиційними (довірені з'єднання, захист периметра тощо).

• Особливий інтерес до *ZTA* протягом останніх двох років виявило керівництво США: розпочалося санкціоноване президентським Указом реформування системи кібербезпеки федеральних відомств на засадах архітектури нульової довіри, *NIST* розробив відповідний стандарт і фреймворк, під егідою Міністерств оборони та внутрішніх справ підготовлено проєкти стратегій, розгорнуто активну експертну роботу з підготовки нормативного та науково-технологічного підґрунтя. Складається враження, що в найвищих керівних колах Сполучених Штатів досягнуто консенсусу щодо розуміння магістральних напрямів та інтенцій розвитку глобального протистояння в кіберпросторі.

• Уряд Сполученого Королівства не декларує жодних системних проєктів та/чи політик щодо масштабних розробок та імплементацій моделей *ZTA* на національному рівні. Зосередження уваги на цьому питанні збіглося в часі з глобальною хвилею АчЛП (2020 – 2021 рр.), але тільки на рівні профільних відомств, і обмежилося, власне, підготовкою та оприлюдненням тематичного посібника для державних і приватних суб'єктів.

• ЄС лише береться до оцінки перспектив упровадження підходу *ZTA* в практику кібербезпеки[104]. Дискусії на цьому етапі зосереджено на оцінці: доцільності системної імплементації *ZTA;* впливу динаміки (інерції) прийняття експертних висновків та політичних/управлінських рішень; наявності в ЄС розвиненої, нормативно підкріпленої (*Regulation (EC) 910/2014 etc.*) і добре апробованої *екосистеми* електронних довірчих послуг (*Trust Services, eIDAS etc.*), яку в певних аспектах можна розглядати як дієву альтернативу *ZTA*.

• Натепер теза про системну ефективність *ZTA* як «стратегії майбутнього» в кібербезпеці не має достатнього практичного (емпіричного) обґрунтування. Потрібного для цього масиву даних наразі не зібрано, оскільки ніхто до цього не намагався апробувати *ZTA* в таких якості й масштабі.

• Комплекс заходів, передбачений положеннями Указу Президента США[105] щодо критичного ПЗ, зводиться до досягнення трьох цілей:

1) створення вичерпного переліку тих функцій ІТ-інфраструктур системи федеральних органів виконавчої влади США, які є критично важливими для збереження її безпеки, цілісності та функціональності;
2) визначення категорій, а також максимально точного (аж до конкретних назв продукту) переліку того ПЗ, яке забезпечує виконання цих функцій ІТ-інфраструктур певної системи;

[104] Див.: URL: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/etl-review-folder/etl-2020-emerging-trends
[105] Див.: URL: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

3) забезпечення ефективного контролю виробництва такого ПЗ, а також його постачання та використання в системі федеральних органів виконавчої влади США.

• У сполученні з широкомасштабною роботою, розгорнутою довкола запровадження *ZTA* у федеральних відомствах США, заходи щодо критичного ПЗ можна розглядати як докорінне реформування системи кібербезпеки урядових структур Сполучених Штатів на засадах нової стратегії – екстенсивної, затратної, але найефективнішої на 2021 – 2022 рр. з погляду максимізації контролю, безпеки та кіберстійкості ІТ-систем та об'єктів.

• З урахуванням того, що повна реалізація завдань стосовно критичного ПЗ та *ZTA* розрахована в цілому щонайменше на 3 – 5 років, можна говорити про консолідовану позицію керівництва США в питанні оптимальної стратегії кіберзахисту в середньостроковій перспективі – принаймні для структур державного управління та, очевидно, об'єкти критичної інфраструктури (ОКІ).

• Водночас для систем та організацій недержавного сектора уряд США в галузі захисту АчЛП наразі обмежується здебільшого рекомендаційними заходами: окрім відповідних Спеціальних публікацій, *NIST* наприкінці 2021 р. оприлюднив для відкритого обговорення другу редакцію (проєкт) Спеціальної публікації «Практики управління ризиками ланцюга постачань кібербезпеки для систем та організацій» щодо виявлення, оцінки та пом'якшення ризиків ланцюга кіберпостачань на всіх рівнях своїх організацій.

• Попри очікувані переваги сертифікації кібербезпеки з погляду прозорості для кінцевих користувачів і використання передового досвіду, постачальники програмного забезпечення досі вважають сертифікацію кібербезпеки дорогим і складним процесом. Справді, сертифікація може призвести до затримок запуску нових систем, що може спричинити значні економічні втрати для індустрії. Отже, з погляду представників галузі, немає чіткої відповіді на питання, чому компанії повинні вкладати час і гроші в сертифікацію компонентів і систем ІКТ.

• Під час кібератак фахівці з кібербезпеки повинні мати можливість співпрацювати в транскордонному режимі. Саме взаємно визнана професійна сертифікація, яку зараз створюють в ЄС, сприятиме транскордонному співробітництву експертів, створюючи можливості забезпечувати загальний рівень реагування.

• Режими сертифікації наразі так само фрагментовані, сертифікати й реєстри не є загальновизнаними та зазвичай охоплюють лише підсектори кібербезпеки, а не становлять цілісних підходів до кібербезпеки. Сертифікаційні схеми й далі неузгоджено множаться. Витрати, пов'язані з потребою отримати низку сертифікатів на той самий продукт чи послугу в кількох організаціях різних країнах, перешкоджають функціонуванню ринку. Транскордонне визнання сертифікатів може слугувати інструментом протидії цьому.

• Органи державного сектора та промисловості в ЄС сприяють ініціативам на кшталт Європейської схеми кіберсертифікації (*European cybersecurity certification scheme*), які допомагають підвищувати прозорість та впевненість у послугах кібербезпеки, зокрема за допомогою загальновизнаних міжнародних схем сертифікації постачальників послуг кібербезпеки.

• Дотримання всіма компаніями мінімальних стандартів кібербезпеки зі страховим забезпеченням дасть змогу спростити управління кіберризиками в

ланцюгу постачань. Також кіберстрахування має очевидні переваги для економіки в цілому, і взаємодія позитивних наслідків означає, що якби кожне мале та середнє підприємство було застраховане, єдиний цифровий ринок був би набагато безпечнішим середовищем для всіх компаній та їхніх споживачів.

• Натепер страховий ринок має багато перспектив, є не до кінця сформованим. Страхові компанії мусили б чіткіше сформулювати дефініції та внутрішні політики страхування, окреслюючи, що саме охоплює їхня політика; з іншого боку, держави також мали б розпрацювати стратегії управління фінансовими наслідками кіберподії.

• Страхові компанії мають створити цілісну стратегію управління тихими кіберризиками з метою випрацювати позитивні страхові рішення. Це також було б вигідно наглядовим органам та рейтинговим агентствам, позаяк дало б змогу продемонструвати ефективне управління страховими кіберризиками.

• Україна перебуває лише на початку шляху запровадження реальних інструментів протидії АчЛП і не має на сьогодні чіткої та зрозумілої політики чи офіційних настанов, які мали б убезпечити як державні органи, так і приватні організації (передусім ОКІ) від АчЛП.

РЕКОМЕНДАЦІЇ *(попередні)*

Апарату Ради національної безпеки і оборони України (НКЦК):

1) створити тимчасову робочу групу для аналізу вразливості перед АчЛП критичних (державних та об'єктів критичної інфраструктури) інформаційно-телекомунікаційних систем. Аналіз має виявити реальні та потенційні загрози від можливої реалізації атаки, аналогічній *Sunburst*, та оцінити ефективність ужитих державою заходів кібербезпеки після вірусу *NotPetya* та *#attack13*. До робочої групи можуть бути залучені як постійні члени НКЦК, так і науковці, експерти, а також іноземні консультанти;

2) розглянути можливість адаптації принципів «Менеджменту ризиків, пов'язаних із забезпеченням безпеки ланцюжка постачань», розробленого *NIST* як офіційного (із наступним затвердженням Рішенням КМУ) для центральних органів виконавчої влади та ОКІ з можливістю розширення сфери дії на інші організації (усіх форм власності);

3) опрацювати можливість розроблення та затвердження «Стратегії зниження кіберризиків у ланцюжках постачань» як загальнодержавної політики щодо убезпечення критичних секторів економіки та державного управління від таких атак;

4) урахувати небезпеку АчЛП під час розроблення заходів із забезпечення національної стійкості;

5) спільно з постійними членами НКЦК розробити рекомендації для державних установ та приватних організацій щодо впровадження першочергових кроків на шляху убезпечення їх від АчЛП (як частини розвитку моделі кіберзрілості організації);

6) підготувати публічний документ з аналізом базових методів проведення АчЛП, прикладами таких атак для посилення публічної обізнаності про актуальні кіберзагрози (за зразком британського Національного центру кібербезпеки[106]);

7) з метою визначити стан законодавчої, організаційної, технічної та інших форм готовності держави до протидії АчЛП ініціювати проведення відповідного комплексного оцінювання із залученням членів НКЦК, наукового та експертного товариства, профільних парламентських комітетів. Результатом діяльності може бути доповідь (звіт) «Про пріоритетні напрями посилення кіберстійкості держави до АчЛП» з визначеними першочерговими нормативно-правовими, організаційними, технічними тощо заходами. Відповідне завдання може бути вирішено як через структуровані консультації між різними суб'єктами (наприклад, у формі робочих груп), так і через короткострокові науково-дослідні роботи;

8) підготувати Методичні рекомендації для ОКІ та органів державної влади щодо можливих заходів запобігання АчЛП;

9) на засадах дотримання зрозумілої мови (*plain language*) підготувати стислий публічний документ з адаптацією рекомендацій для приватних підприємств та громадян, що містяться в «Посібнику щодо убезпечення ланцюгів постачань» (*Supply chain security guidance*) Національного центру з кібербезпеки Сполученого Королівства (*NCSC*), а також у «Найліпших практиках управління кіберризиками в ланцюгах постачань» (*Best Practices in Cyber Supply Chain Risk Management*)[107] Національного інституту стандартів і технологій (*NIST*).

---

[106] Див.: URL: https://www.ncsc.gov.uk/collection/supply-chain-security/supply-chain-attack-examples

[107] Див.: URL: Microsoft Word – Workshop Brief on Cyber Supply Chain Best Practices.docx (nist.gov)

Кабінету Міністрів України:

1) завершити процедури щодо впровадження механізму незалежного аудиту інформаційної безпеки в практику державного управління, прийнявши відповідні підзаконні акти, що регламентують його проведення. Розглянути можливість активного залучення української експертної спільноти (з тих представників приватного сектора, що займаються питаннями кібербезпеки) для створення зазначеного механізму;

2) після запровадження цієї процедури визначити загальну вимогу до всіх постачальників, що пропонують послуги державним організаціям (зокрема через майданчик *Prozorro*), які пов'язані з можливістю їх доступу до інформаційно-телекомунікаційних мереж замовників; обов'язково надавати сертифікат за результатами проведення незалежного аудиту інформаційної безпеки.

Міністерству закордонних справ (спільно з ДССЗЗІ та НКЦК):

- у межах наявних та нових кібердіалогів проводити консультації з метою обміну досвідом стосовно: боротьби з АчЛП; оптимізації міжвідомчої взаємодії і публічного управління в галузі кібербезпеки; останніх досягнень у розробленні відповідних політик та законодавчих ініціатив; підвищення публічної обізнаності про актуальні кіберзагрози тощо.

ДОДАТОК 1. НІМЕЦЬКИЙ КЕЙС

Зміни до законодавства в контексті підвищення стійкості до кібератак на прикладі Німеччини

З 28 травня 2021 р. в Німеччині набув чинності Другий закон про підвищення безпеки систем інформаційних технологій (*Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme,* Закон про безпеку ІКТ 2.0 / *IT-Sicherheitsgesetz 2.0*)[108]. Через посилення зобов'язань щодо ІТ-безпеки та посилення покарань численні поправки до центрального законодавства Німеччини про ІТ-безпеку – до Закону про Федеральне управління з питань інформаційної безпеки (*the Act on the Federal Office for Information Security / Gesetz über das Bundesamt für Sicherheit in der Informationstechnik – BSI-Gesetz*) – стосуються як операторів критичної інфраструктури, на які вже поширено дію Закону *BSI*, так і компаній, що працюють у сфері утилізації побутових відходів, виробників ІТ-продуктів, використовуваних у критично важливих інфраструктурах, та компаній, що становлять особливий суспільний інтерес. Розширена сфера застосування Закону про *BSI* є однією з головних змін, унесених Законом про безпеку ІКТ 2.0.

На додаток до критичних секторів, які вже закріплено в Законі про *BSI* (енергетика, інформаційні технології й телекомунікації, транспорт, охорона здоров'я, водопостачання, харчування, а також фінанси та страхування), заведено ще один сектор – утилізації побутових відходів.

На постачальників, тобто виробників критично важливих компонентів, також покладатимуться певні зобов'язання – це має на меті захистити весь ланцюг постачань. Критичні компоненти – це ІТ-продукти: а) які використовують у критично важливих інфраструктурах; б) для яких порушення доступності, цілісності, автентичності та конфіденційності можуть призвести до збою або значного погіршення функціональності критичної інфраструктури чи до загрози громадській безпеці; в) що на основі закону стосовно цього положення визначено як важливий складник або такий, що реалізує функцію, визначену як критичну на базі закону.

«Компанії, що становлять особливий суспільний інтерес» – це нова категорія. До них належать компанії, що не є операторами критично важливих об'єктів інфраструктури, але які: а) виробляють або розробляють товари відповідно до розділу 60 § 1 п. 1 та 3 Німецького Положення про зовнішню торгівлю та платежі (*Außenwirtschaftsverordnung – AWV*[109]) – виробники оборонних підприємств, а також виробники ІТ-продуктів для оброблення секретної державної інформації; б) компанії, що мають значний економічний вплив, або компанії-постачальники з огляду на унікальність пропозиції (хто чітко підпадає під цю категорію, буде

[108] Див.: URL: https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/IT-SiG/2-0/it_sig-2-0_node.html
[109] Див.: URL: https://www.gesetze-im-internet.de/awv_2013/__60.html

зазначено в додатковій постанові); в) оператори установ найвищого рівня (що продукують небезпечні матеріали) у значенні Постанови про небезпечні аварії (*Störfall-Verordnung*[110]) чи еквівалентні таким операторам відповідно до ст. 1 § 2 Постанови про небезпечні інциденти.

Закон Про безпеку ІКТ 2.0 доповнює зобов'язання, що вже існують згідно із Законом *BSI*[111], та вводить **нові зобов'язання**:

1. Для операторів критичних інфраструктур це стосується, зокрема, таких нових ***зобов'язань***:

Зареєструвати критичну інфраструктуру у Федеральному відомстві з інформаційної безпеки (*BSI*)	Це зобов'язання реалізується на додаток до вже чинного зобов'язання призначати контактний пункт для критичної інфраструктури, яку вони використовують
Використовувати системи виявлення атак	Зобов'язання операторів критичних інфраструктур уживати відповідних організаційних та технічних заходів, що є визначальними для функціонування критичної інфраструктури (див. Розділ 8a Закону про *BSI*[112]). Зараз це зобов'язання також містить використання систем виявлення нападів (*attack detection systems*)
Подати документи, необхідні для оцінки з погляду *BSI*	У зв'язку з цим *BSI* може вимагати інформацію про ключові дані, якщо оператор не виконує свого обов'язку з реєстрації
Оприлюднювати інформацію, необхідну для управління в кризовій ситуації	Під час значної атаки *BSI* може за погодженням з відповідним компетентним федеральним наглядовим органом вимагати від постраждалих операторів критичної інфраструктури або компаній, що становлять особливий суспільний інтерес, передачу інформації, зокрема персональні дані, необхідні для усунення наслідків кризової ситуації

[110] Див.: URL: https://www.gesetze-im-internet.de/bimschv_12_2000/12._BImSchV.pdf
[111] Див.: URL: https://www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html
[112] Ibid.

Щодо використання критичних компонентів	На операторів критичної інфраструктури покладено зобов'язання щодо використання критичних компонентів (складників, необхідних для функціонування критичної інфраструктури). Закон про безпеку ІКТ 2.0 запроваджує, з одного боку, обов'язок операторів критичних інфраструктур повідомляти Федеральне міністерство внутрішніх справ, будівництва та громади (*BMI*) про заплановане перше використання критичного компонента. З іншого боку, оператор критичної інфраструктури зобов'язаний отримати декларацію від виробника критичних компонентів про її надійність – т. зв. гарантійна декларація. Лише після її отримання оператор критичної інфраструктури може використовувати критичні компоненти

На підставі цього повідомлення й декларації про гарантію Федеральне міністерство внутрішніх справ проводить попередню та наступну експертизи щодо використання критичних компонентів і може заборонити початкове або наступне використання критичного компонента стосовно оператора критичної інфраструктури за погодженням із відповідними міністерствами, переліченими в Законі про *BSI* та Федеральним міністерством закордонних справ. Заборона на використання критично важливих компонентів виробника може мати наслідки для виробника в майбутньому.

2. ***Зобов'язання*** операторів критичної інфраструктури використовувати критично важливі компоненти лише тих виробників, які видали їм декларацію про свою надійність; виробники повинні видавати відповідні гарантійні декларації щодо оператора критичної інфраструктури щодо всього ланцюга постачань.

3. ***Зобов'язання*** щодо *операторів критичної інфраструктури* поширюються в дещо зміненій формі на інші економічні сектори – *компанії, що становлять особливий суспільний інтерес* (виробники оборонної сфери, оброблення секретної державної інформації, значні за розмірами та часткою економічної вартості).

Повністю переглянуто каталог положень про штрафи – адміністративне правопорушення було введено для тих операторів критичної інфраструктури, які не забезпечили створення контактного пункту з безперебійним доступом до нього (*Critical Infrastructure Protection Points of Contact*), або якщо компанія особливого

суспільного інтересу, відповідно до Розділу 2 § 14 п. 1 і 2 Закону про *BSI*, не подавали декларацію чи подали її неправильно або невчасно.

Штрафи до 100 000 євро або до 50 000 євро передбачено попереднім Законом про *BSI*. Тепер за адміністративні правопорушення – залежно від випадку – може бути накладено штраф: а) до 2 000 000 євро; б) до 1 000 000 євро; в) до 500 000 євро; г) до 100 000 євро.

Закон узгоджується з Директивою *NIS 2*, опублікованою 16 грудня 2020 р. Обидва нормативні акти доповнюють вимоги щодо IT-безпеки.