ЗАТВЕРДЖЕНО
Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України
06 жовтня 2021 року № 601

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ
щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури

І. Загальні положення

1. Методичні рекомендації щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури (далі – Рекомендації) розроблено відповідно до підпункту 1 частини другої та пункту 3 частини третьої статті 8 Закону України «Про основні засади забезпечення кібербезпеки України», абзацу другого частини першої статті 3, пунктів 85, 86 і 88 частини першої статті 14 Закону України «Про Державну службу спеціального зв'язку та захисту інформації України», абзацу другого підпункту 1 пункту 3 Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України, затвердженого постановою Кабінету Міністрів України від 3 вересня 2014 року № 411, та Загальних вимог до кіберзахисту об'єктів критичної інфраструктури, затверджених постановою Кабінету Міністрів України від 19 червня 2019 року № 518, з метою підвищення рівня кіберзахисту критичної інформаційної інфраструктури.

2. Рекомендації розроблено з урахуванням Настанови для підвищення кібербезпеки критичної інфраструктури (Framework for Improving Critical Infrastructure Cybersecurity[1]), виданої у 2014 році та оновленої[2] у 2018 році Національним інститутом стандартів та технології Сполучених Штатів Америки (National Institute of Standards and Technology).

3. Рекомендації не є нормативно-правовим актом, мають інформаційний та рекомендаційний характер, не встановлюють правових норм і є добровільними для використання.

ІІ. Терміни та визначення понять

У цих Рекомендаціях терміни вживаються в такому значенні:

активи – дані, персонал, пристрої та носії інформації, що дозволяють організації забезпечити надання життєво важливих послуг та функцій;

Примітки
[1] https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf
[2] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

віртуальна приватна мережа (Virtual Private Network, VPN) – технологія, що дозволяє створити окремо виділені віртуальні мережі із одним або кількома зашифрованими з'єднаннями через мережу Інтернет;

екосистема – сукупність об’єктів критичної інфраструктури, які взаємодіють та/або взаємозалежать одні від одних як постачальники або отримувачі основних послуг, або об’єднані між собою за галузевою (секторальною) ознакою та/або процесом надання основної послуги, або які безпосередньо впливають на можливість надання основної послуги;

організація – орган державної влади, підприємство, установа, організація будь-якої форми власності, юридична та/або фізична особа, якому/якій на правах власності, оренди або на інших законних підставах належить ОКІ або який/яка відповідає за його поточне функціонування;

профіль кіберзахисту – структурований опис заходів кіберзахисту, які реалізовані на ОКІІ, що враховує практику реалізації заходів кіберзахисту та потреби діяльності ОКІ;

система (таксономія) заходів кіберзахисту – впорядкований набір заходів з кіберзахисту, бажаних результатів кіберзахисту та відповідних нормативних та інформативних посилань, що є загальними в усіх галузях критичної інфраструктури;

Інші терміни вживаються у значеннях, наведених у Законах України «Про основні засади кібербезпеки України», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про телекомунікації», «Про стандартизацію», постановах Кабінету Міністрів України від 09 жовтня 2020 року № 943 «Деякі питання об’єктів критичної інфраструктури», від 09 жовтня 2020 року № 1109 «Деякі питання об’єктів критичної інформаційною інфраструктури», від 19 червня 2019 року № 518 «Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури» (далі – постанова № 518).

ІІІ. Скорочення

У цих Рекомендаціях наведено такі скорочення:

КСЗІ – комплексна система захисту інформації;

ОКІ – об’єкт критичної інфраструктури;

ОКІІ – об’єкт критичної інформаційної інфраструктури;

СУІБ – система управління інформаційної безпеки.

IV. Мета, складові та застосування Рекомендацій

1. Рекомендації запроваджують однаковий опис застосованих механізмів кіберзахисту, визначених постановою № 518, національними та міжнародними стандартами, керівництвами та практиками, а також механізмів захисту інформації, що вже впроваджені на ОКІ організаціями в будь-яких секторах економіки.

2. Рекомендації можуть використовуватися під час упровадження заходів кіберзахисту, які спрямовані на управління ризиками кібербезпеки для ОКІІ, що є елементами одного ОКІ, і у співпраці з іншими ОКІ свого та інших секторів критичної інфраструктури, а також для використання іншими суб'єктами забезпечення кібербезпеки.

3. Рекомендації описують загальний підхід до забезпечення кібербезпеки, що дозволяє:

здійснити аналіз та надати характеристику поточного стану кібербезпеки ОКІІ;

описати цільовий стан кібербезпеки ОКІІ;

ідентифікувати та визначити пріоритети, рівень упровадження заходів кіберзахисту в контексті безперервного та повторюваного процесу управління ризиками у сфері кібербезпеки ОКІІ;

оцінити прогрес у досягненні цільового стану кібербезпеки ОКІІ;

забезпечити комунікацію між суб'єктами, які безпосередньо знаходяться на ОКІ, та із суб'єктами, які є партнерами організації щодо управління ризиками у сфері кібербезпеки.

4. Рекомендації складаються з трьох основних частин:

системи (таксономії) заходів кіберзахисту;

рівнів упровадження заходів кіберзахисту;

профілю кіберзахисту.

5. Підхід, що визначається у Рекомендаціях, не є єдиним підходом для управління ризиком кібербезпеки, оскільки ОКІ, що належать різним секторам такої інфраструктури, можуть мати як однакові ризики, так і різні унікальні ризики – унікальні загрози, різні вразливості, різні допустимі рівні ризику. Підхід до забезпечення кібербезпеки залежить від того, яким чином організація буде впроваджувати заходи кіберзахисту, що наведені у цих Рекомендаціях.

6. ОКІ може використовувати Рекомендації для впровадження системного процесу для визначення, оцінки та управління ризиками у сфері

кібербезпеки, розроблення плану удосконалення цієї діяльності для відповідного затвердження організацією та планування фінансування заходів з його реалізації.

ОКІ може зіставляти діяльність із захисту інформації, яка проводиться відповідно до галузевих вимог безпеки, або впроваджену КСЗІ із заходами кіберзахисту, що викладені у цих Рекомендаціях, з метою визначення недоліків у поточній діяльності із захисту інформації та управління ризиками кібербезпеки, а також вдосконалити систему захисту інформації.

7. Рекомендації можуть застосовуватися на всіх етапах створення КСЗІ, СУІБ, систем інформаційної безпеки або інших систем захисту інформації, що визначені міжнародними та національними стандартами.

8. На етапі планування захисту інформації описуються вимоги до кібербезпеки. На етапі проєктування системи захисту інформації враховуються вимоги до кібербезпеки як частина вимог із захисту інформації та частина більшого процесу проєктування системи надання основних послуг. Ключовим моментом на етапі проектування є підтвердження того, що специфікація вимог з кібербезпеки відповідає потребам ОКІ та ризикам кібербезпеки.

9. Рівень ризиків кібербезпеки ОКІ пропонується знижувати шляхом:

покращення практик застосування засобів захисту інформації;

удосконалення організаційних заходів із кіберзахисту на ОКІ;

упровадження політик управління ризиками кібербезпеки у контексті надання основних послуг ОКІ;

налагодження та/або покращення взаємодії ОКІ з іншими об’єктами сектору критичної інфраструктури та пов’язаними об’єктами з інших секторів з метою покращення кібербезпеки в цілому.

V. Система заходів кіберзахисту

1. Система заходів кіберзахисту базується на нормативних документах, національних та міжнародних стандартах, усталеній практиці захисту інформації та забезпечення кібербезпеки, що розвиваються разом з технологіями забезпечення кібербезпеки. Це забезпечує ефективність реалізації заходів кіберзахисту та можливість підтримки нових технологій і методів забезпечення кібербезпеки.

2. Рекомендації визначають систему (таксономію) заходів кіберзахисту для досягнення конкретного цільового стану кібербезпеки. Систему заходів кіберзахисту не слід розглядати як вичерпний перелік заходів. Рекомендації з кібербезпеки сформульовано у вигляді результатів,

що очікуються у разі впровадження заходів кіберзахисту.

3. Діяльність із забезпечення кібербезпеки спрямована на зниження ризиків кібербезпеки, носить безперервний циклічний характер та формує цикл управління кібербезпекою, який складається з п’яти функцій кібербезпеки (рис. 1):

ідентифікація ризиків;

кіберзахист;

виявлення кіберінцидентів;

реагування;

відновлення поточного стану кібербезпеки.

Рисунок 1 – Цикл управління кібербезпекою

4. Функції кібербезпеки забезпечують:

прийняття рішення з управління ризиками кібербезпеки на ОКІІ;

вибір та впровадження заходів кіберзахисту;

реагування на загрози кібербезпеки;

удосконалення кіберзахисту, враховуючи набутий досвід.

Функції кібербезпеки узгоджені з чинними підходами щодо управління ризиками кібербезпеки та допомагають продемонструвати ефективність інвестицій в кібербезпеку. Наприклад, планування забезпечення кібербезпеки та тренування персоналу покращують своєчасне реагування на кіберінциденти та відновлення функціонування ОКІІ, в результаті чого знижується негативний вплив кіберінцидентів на своєчасність та безперервність надання життєво важливих послуг та функцій.

5. Система (таксономія) заходів кіберзахисту складається з чотирьох елементів (рис. 2):

клас заходів кіберзахисту;

категорія заходів кіберзахисту;

підкатегорія заходів кіберзахисту;

інформаційні посилання.

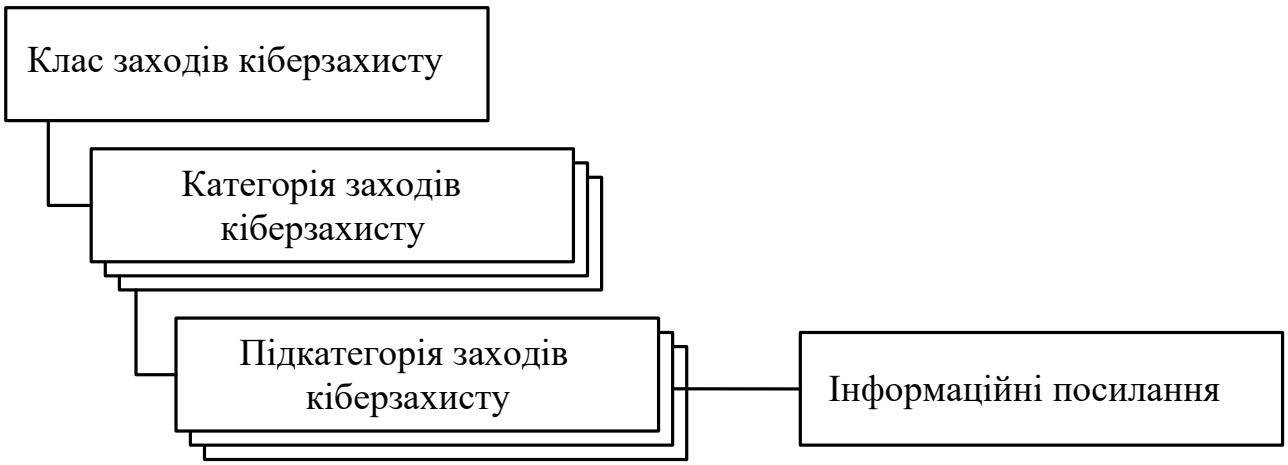

Рисунок 2 – Система заходів кіберзахисту

6. Клас заходів кіберзахисту організовує заходи кіберзахисту на системному рівні та визначає зміст циклу управління кібербезпекою.

П’ять класів заходів кіберзахисту:

ідентифікація ризиків;

кіберзахист;

виявлення кіберінцидентів;

реагування на кіберінциденти;

відновлення поточного стану кібербезпеки.

Кожний клас заходів кіберзахисту має свій ідентифікатор, що складається з двох літер.

Клас заходів кіберзахисту «Ідентифікація ризиків кібербезпеки» (ID) передбачає заходи, реалізація яких спрямована на поглиблення знань керівництва та персоналу ОКІІ щодо наявних ризиків, способів управління ризиками кібербезпеки для інформаційних систем, активів, даних, що використовуються для надання життєво важливих послуг та функцій. Реалізація заходів кіберзахисту класу «Ідентифікація ризиків» є чинником для ефективного використання Рекомендацій, розуміння умов, ресурсів, що підтримують надання життєво важливих послуг та функцій, а також пов'язаних ризиків кібербезпеки, обґрунтованого вибору конкретних заходів для впровадження. Це дозволяє визначити пріоритетність ризиків кібербезпеки потребами надання життєво важливих послуг та функцій, а також розподіляти ресурси і зусилля відповідно до встановлених пріоритетів.

Клас заходів кіберзахисту «Кіберзахист» (PR) визначає діяльність із розробки та впровадження відповідних методів, засобів, процедур кіберзахисту для забезпечення стійкого, безперервного та безпечного надання життєво важливих послуг та функцій ОКІ. Ці заходи дозволяють обмежити або стримати вплив кіберінцидентів.

Клас заходів кіберзахисту «Виявлення кіберінцидентів» (DE) містить заходи своєчасного виявлення кіберінцидентів.

Клас заходів кіберзахисту «Реагування на кіберінцидентів» (RS) містить заходи реагування на кіберінциденти та кібератаки. Реалізація заходів спрямована на зниження потенційного негативного впливу кіберінциденту (кібератаки) на надання життєво важливих послуг та функцій.

Клас заходів кіберзахисту «Відновлення стану кібербезпеки» (RC) визначає діяльність щодо забезпечення спроможностей ОКІІ щодо стійкого, надійного та безперервного надання життєво важливих послуг та функцій, які були порушені внаслідок кіберінциденту (кібератаки). Ці заходи забезпечують своєчасне відновлення штатної роботи ОКІІ та зменшення негативного впливу кіберінциденту (кібератаки).

7. Категорія заходів кіберзахисту являє собою складові елементи класу заходів кіберзахисту, упорядковані за групою цільових результатів забезпечення кібербезпеки та тісно пов'язані із завданнями забезпечення кібербезпеки та конкретними групами заходів кіберзахисту. Прикладами категорій заходів кіберзахисту є «Управління активами», «Управління доступом» тощо. Кожна категорія заходів кіберзахисту має власний ідентифікатор, який складається з ідентифікатора класу заходів кіберзахисту (перші дві літери) та ідентифікатора категорії (останні дві літери). Наприклад, управління активами – ID.AM.

8. Підкатегорія заходів кіберзахисту являє собою складовий елемент категорії заходів кіберзахисту. Підкатегорії заходів кіберзахисту містять сукупність конкретних заходів кіберзахисту, які сформульовані у вигляді

конкретного результату, що має бути досягнутий під час упровадження заходів кіберзахисту. По суті це набір результатів, які, хоча і не є вичерпними, але допомагають досягти цільових результатів забезпечення кібербезпеки за кожною категорією заходів кіберзахисту. Прикладами підкатегорій є «Зовнішні інформаційні системи задокументовано», «Дані, що зберігаються, захищено», «Повідомлення систем виявлення вторгнення досліджено». Кожна підкатегорія заходів кіберзахисту має свій власний ідентифікатор, що складається з ідентифікатора категорії заходів кіберзахисту та порядкового номера підкатегорії. Наприклад: ID.AM-1

9. Інформаційне посилання являє собою елемент системи заходів кіберзахисту, який містить посилання на стандарти, нормативні документи, рекомендації та загальноприйняті практики, поширені у галузях (секторах) критичної інфраструктури для забезпечення безпеки ОКІІ. Ці посилання ілюструють методи, способи та технології досягнення цільових результатів (показників) для кожної підкатегорії заходів кіберзахисту. Інформаційні посилання, наведені в Рекомендаціях, є довідковими та не є вичерпними. Нормативні посилання базуються на національних стандартах, нормативних документах, прийнятих в Україні. Довідкові посилання базуються на міжнародних і регіональних стандартах, нормативних документах інших країн.

У таблиці 1 наведено систему заходів кіберзахисту. Повну класифікація заходів кіберзахисту наведено у додатку 1 до цих Рекомендацій.

Таблиця 1

Система заходів кіберзахисту

Категорія заходів кіберзахисту	Опис	Заходи кібер-захисту
1	2	3
Клас заходів кіберзахисту «Ідентифікація ризиків кібербезпеки» (ID)		
ID.AM Управління активами	Описуються дані, персонал, пристрої та носії інформації, інформаційні системи, що дозволяють забезпечити надання життєво важливих послуг та функцій до рівня важливості для організації відносно життєво важливих послуг та функцій, а також описується політика управління ризиками.	ID.AM-1 ID.AM-2 ID.AM-3 ID.AM-4 ID.AM-5 ID.AM-6
ID.BE Середовище надання життєво важливих послуг та функцій	Формування обов'язків персоналу щодо забезпечення кібербезпеки, а також рішень з управління ризиками у сфері кібербезпеки.	ID.BE-1 ID.BE-2 ID.BE-3 ID.BE-4 ID.BE-5

1	2	3
ID.GV Управління безпекою	Формування правил, процедур і процесів для управління й моніторингу впроваджених нормативних, екологічних та експлуатаційних вимог, а також вимог щодо забезпечення кібербезпеки.	ID.GV-1 ID.GV-2 ID.GV-3 ID.GV-4
ID.RA Оцінка ризиків	Визначення ризиків у сфері кібербезпеки для процесів надання життєво важливих послуг та функцій, а також активів організації.	ID.RA-1 ID.RA-2 ID.RA-3 ID.RA-4 ID.RA-5 ID.RA-6
ID.RM Стратегія управління ризиками організації	Визначення пріоритетів, обмежень, допустимого рівня ризику для підтримки рішень щодо зниження ризиків кібербезпеки.	ID.RM-1 ID.RM-2 ID.RM-3
ID.SC Управління ризиками системи постачання	Визначення пріоритетів, обмежень, допустимого рівня ризику щодо системи постачання для підтримки рішень щодо ризиків, пов’язаних із системою постачання послуг третіми особами.	ID.SC-1 ID.SC-2 ID.SC-3 ID.SC-4
Клас заходів кіберзахисту «Кіберзахист» (PR)		
PR.AC Управління ідентифікацією, автентифікацією та контроль доступу	Забезпечення доступу до фізичних і логічних ресурсів ОКІ та пов'язаних з ними об'єктів тільки для авторизованих користувачів, адміністраторів або процесів. Управління здійснюється з урахуванням встановленого допустимого рівня ризику несанкціонованого доступу.	PR.AC-1 PR.AC-2 PR.AC-3 PR.AC-4 PR.AC-5 PR.AC-6
PR.AT Обізнаність та навчання	Забезпечення інформування та обізнаності організації та партнерів організації щодо питань кібербезпеки. Співробітники мають освіту або пройшли спеціалізовану підготовку для покращення інформованості з питань кібербезпеки, пройшли належну підготовку для виконання своїх обов'язків щодо забезпечення кібербезпеки відповідно до встановлених політик, правил, процедур та угод.	PR.AT-1 PR.AT-2 PR.AT-3 PR.AT-4 PR.AT-5
PR.DS Безпека даних	Забезпечення управління інформацією та документацією, з метою захисту конфіденційності, цілісності та доступності інформації.	PR.DS-1 PR.DS-2 PR.DS-3 PR.DS-4 PR.DS-5 PR.DS-6 PR.DS-7 PR.DS-8
PR.IP Процеси та процедури кіберзахисту	Забезпечення підтримання та управління політикою (правилами) безпеки, процесами та процедурами, які використовуються для управління захистом інформаційних систем і активів організації.	PR.IP-1 PR.IP-2 PR.IP-3 PR.IP-4

1	2	3
		PR.IP-5 PR.IP-6 PR.IP-7 PR.IP-8 PR.IP-9 PR.IP-10
PR.MA Технічне обслуговування	Технічне обслуговування та ремонт компонентів системи управління виробничими процесами, компонентів інформаційно-телекомунікаційних систем виконуються з дотриманням правил та процедур безпеки.	PR.MA-1 PR.MA-2
PR.PT Технології кіберзахисту	Управління технічними рішеннями (технологіями) кіберзахисту з метою забезпечення безпеки та стійкості систем і активів організації з дотриманням правил, процедур з безпеки.	PR.PT-1 PR.PT-2 PR.PT-3 PR.PT-4 PR.PT-5
Клас заходів кіберзахисту «Виявлення кіберінцидентів» (DE)		
DE.AE Аномалії та кіберінциденти	Своєчасне виявлення аномальної активності та передбачення потенційного впливу кіберінцидентів.	DE.AE-1 DE.AE-2 DE.AE-3 DE.AE-4 DE.AE-5
DE.CM Безперервний моніторинг кібербезпеки	Відстеження безпеки інформаційних систем та активів організації через дискретні інтервали для виявлення кіберінцидентів та перевірки ефективності заходів кібербезпеки.	DE.CM-1 DE.CM-2 DE.CM-3 DE.CM-4 DE.CM-5 DE.CM-6 DE.CM-7 DE.CM-8
DE.DP Процеси виявлення кіберінцидентів	Підтримання і тестування процесів й процедур виявлення кіберінцидентів для забезпечення своєчасного та адекватного оповіщення про аномальні кіберінциденти.	DE.DP-1 DE.DP-2 DE.DP-3 DE.DP-4 DE.DP-5
Клас заходів кіберзахисту «Реагування на кіберінциденти» (RS)		
RS.RP Планування реагування	Процеси та процедури реагування на кіберінциденти виконуються та підтримуються з метою забезпечення своєчасного реагування на виявлені кіберінциденти.	RS.RP-1
RS.CO Комунікації	Координація заходів з реагування між внутрішніми та зовнішніми партнерами організації (у разі доцільності).	RS.CO-1 RS.CO-2 RS.CO-3 RS.CO-4 RS.CO-5

1	2	3
RS.AN Аналіз	Проведення аналізу кіберінцидентів для забезпечення адекватних заходів реагування та підтримки відновлення.	RS.AN-1 RS.AN-2 RS.AN-3 RS.AN-4
RS.MI Мінімізація наслідків.	Виконання заходів з метою запобігання розширенню кіберінциденту, мінімізації його наслідків та унеможливлення його повторення.	RS.MI-1 RS.MI-2 RS.MI-3
RS.IM Удосконалення	Удосконалення заходів з реагування шляхом врахування досвіду з поточних або виконаних заходів виявлення/реагування.	RS.IM-1 RS.IM-2
Функція кібербезпеки «Відновлення стану кібербезпеки» (RC)		
RC.RP Планування відновлення	Процеси та процедури відновлення виконуються та підтримуються з метою своєчасного відновлення систем або активів, постраждалих від кіберінцидентів.	RC.RP-1
RC.IM Удосконалення	Планування відновлення та процеси відновлення удосконалюються шляхом урахування отриманого досвіду.	RC.IM-1 RC.IM-2
RC.CO Комунікації	Заходи з відновлення координуються з внутрішніми та зовнішніми партнерами організації, такими як координаційні центри, оператори, провайдери телекомунікацій, власники атакуючих систем, інші групи реагування на інциденти, пов'язані з інформаційною та/або кібербезпекою (CSIRT), та постачальники.	RC.CO-1 RC.CO-2 RC.CO-3

VI. Рівні впровадження заходів з кіберзахисту

1. Рівні впровадження заходів кіберзахисту характеризують ступінь практичного впровадження організацією заходів із кіберзахисту, здатність організації досягти запланованих результатів кіберзахисту та надають інструментарій оцінювання ступеня впровадження процесів управління кібербезпекою.

Визначаються чотири рівні впровадження заходів кіберзахисту:

1 рівень – частковий;

2 рівень – ризик-орієнтований;

3 рівень – повторюваний;

4 рівень – адаптивний.

Під час вибору рівня впровадження, організації доцільно розглянути свою поточну практику управління ризиками, навколишнє середовище загроз, юридичні та нормативні вимоги, цілі бізнесу/місії та організаційні обмеження.

2. Рекомендації визначають чотири ієрархічних рівні впровадження заходів кіберзахисту (рисунок 3.)

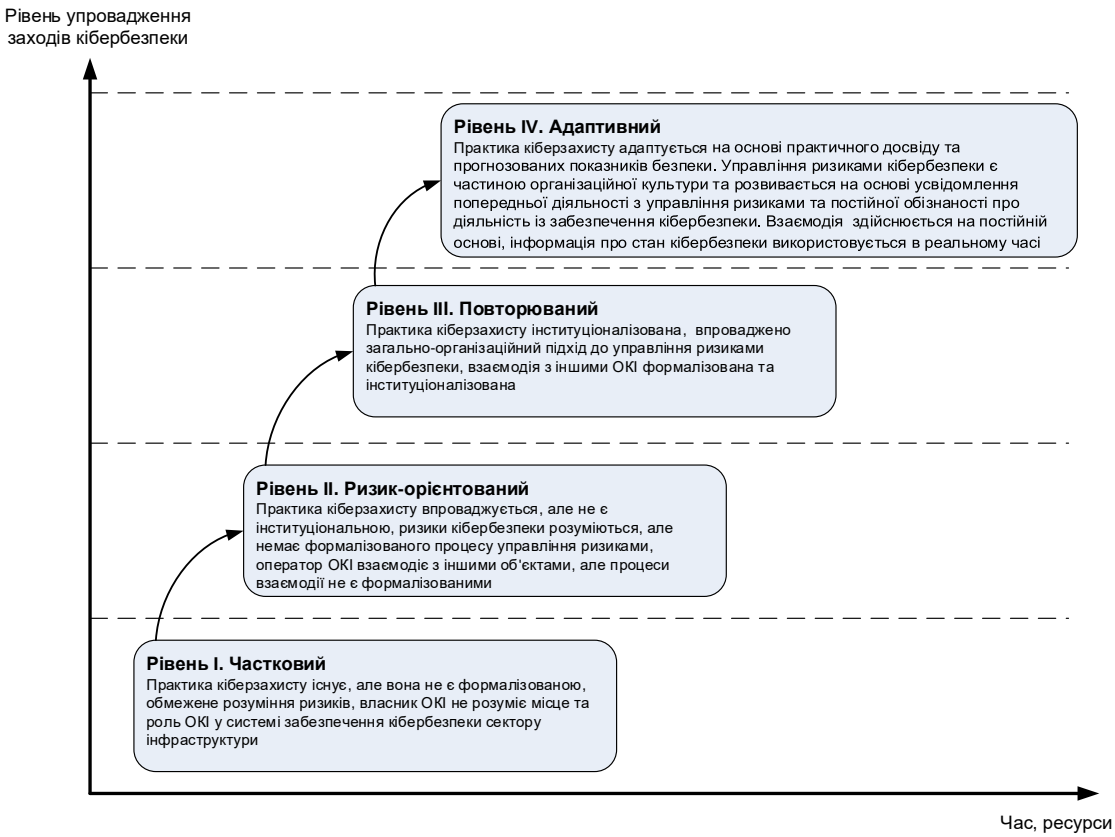

Рисунок 3 – Рівні впровадження заходів кіберзахисту

3. Процес вибору рівня впровадження (таблиця 2) враховує поточну практику щодо реалізації заходів кіберзахисту та управління ризиками кібербезпеки на ОКІІ, характеристики загроз кібербезпеки, законодавчі та нормативні вимоги, комерційні та стратегічні цілі ОКІ, вимоги до кібербезпеки в ланцюзі поставок програмного/апаратного забезпечення та організаційні обмеження, а також інші наявні обмеження.

Рекомендовано визначати цільовий рівень впровадження, переконавшись, що вибраний рівень зменшує ризик кібербезпеки до критично важливих активів і ресурсів, прийнятних для організації. Рекомендується враховувати вимоги галузевих (секторальних) нормативних актів, нормативно-правових актів у сфері кібербезпеки та захисту інформації, рекомендації урядової або секторальної/міжсекторальної команди реагування на комп'ютерні інциденти (CERT-UA/CERT)/інциденти комп'ютерної безпеки (CSIRT) або галузевих

(секторальних) центрів управління безпекою (SOC), існуючі моделі зрілості або інші джерела, які допоможуть визначити бажаний рівень ризику кібербезпеки.

ОКІІ, що досягли певного рівня впровадження, рекомендується розглянути можливість просування до наступного або більшого рівня. Рівні призначено для підтримки прийняття організаційних рішень про те, як керувати ризиком кібербезпеки, які заходи для ОКІІ мають вищий пріоритет та на які заходи можуть виділятися додаткові ресурси.

Успішність упровадження заходів з кіберзахисту базується на досягненні результатів, описаних у цільовому профілі організації, а не на визначеному рівні впровадження.

Таблиця 2

Рівні впровадження заходів з кіберзахисту

Рівень	Практика кіберзахисту	Політика управління ризиками	Взаємодія з іншими ОКІ
1	2	3	4
Частковий	Практична діяльність із реалізації заходів кіберзахисту та управління ризиками кібербезпеки не є формалізованою. Діяльність з упровадження заходів кіберзахисту та управління ризиками носить довільний та ситуативний характер. Пріоритетність виконання заходів кіберзахисту безпосередньо не враховує цілі ОКІІ щодо управління ризиками, характеристики загроз, завдання щодо надання життєво важливих послуг та функцій.	Обмежене розуміння ризику кібербезпеки на організаційному рівні. Інформованість керівництва та персоналу організації про ризики кібербезпеки є недостатньою. Загальний підхід до управління ризиками кібербезпеки в масштабі всього ОКІІ не встановлено. Заходи кіберзахисту впроваджуються нерегулярно, ситуативно, використовуючи різноманітний практичний досвід або інформацію, отриману із зовнішніх джерел. Процесів, що забезпечують внутрішній обмін інформацією про стан кібербезпеки, не зафіксовано.	Організація не розуміє свою роль у екосистемі щодо своїх власних залежностей або залежних від неї інших суб’єктів. Організація не опрацьовує або отримує інформацію (дослідження загроз, кращі практики, технології) від інших організацій (споживачі, постачальники, залежні від неї або від яких вона залежить організацій, організацій аналізу та поширення інформації, дослідники, державні органи) та не поширює таку інформацію. Організація взагалі не усвідомлює ризиків кібербезпеки, пов'язаних з послугами, які вона надає та якими користується.
Ризик-орієнтований	Практика реалізації заходів кіберзахисту та управління	Існує усвідомлення ризику кібербезпеки на організаційному рівні, але	Загалом організація розуміє свою роль у екосистемі щодо своїх

1	2	3	4
	ризиками затверджується керівництвом організації, але може не встановлюватися як загальна політика для організації. Пріоритетність діяльності з кібербезпеки та потреби захисту безпосередньо залежать від цілей організаційного ризику, середовища загроз або вимог щодо надання життєво важливих послуг та функцій.	загальний підхід організації до управління ризиком кібербезпеки не встановлено. Інформація про кібербезпеку поширюється в межах організації на неофіційній основі. Розгляд кібербезпеки в цілях та програмах організації може відбуватися на деяких, але не на всіх рівнях організації. Оцінка ризиків кібербезпеки для організаційних та зовнішніх активів відбувається, але зазвичай не повторюється або однаково не проводиться.	власних залежностей або залежних від неї інших суб'єктів, але не їх обох. Організація опрацьовує та отримує деяку інформацію від інших організацій, створює на підставі неї власну інформацію, але може не поширювати таку інформацію між іншими організаціями. Крім того, організація усвідомлює ризики кібербезпеки, пов'язані з послугами, які вона надає та якими користується, але не діє послідовно або за затвердженими правилами.
Повторюваний	Практика реалізації заходів кіберзахисту та управління ризиками в організації є офіційно затвердженою і визначена як політика. Результати кіберзахисту регулярно відстежуються та заходи кіберзахисту регулярно оновлюються на основі застосування процесів управління ризиками до змін у вимогах щодо надання життєво-важливої функції, мінливих загроз та технологічного ландшафту.	В організації існує загальний підхід до управління ризиками кібербезпеки. Політики інформування про ризики, процеси та процедури визначені, реалізуються за призначенням та переглядаються. Існують послідовні методи ефективного реагування на зміни ризику. Персонал володіє знаннями та вміннями виконувати призначені їм обов'язки. Організація послідовно і точно контролює ризик кібербезпеки для активів організації. Пов'язані та не пов'язані з кібербезпекою головні виконавці регулярно спілкуються щодо ризику кібербезпеки.	Організація розуміє свою роль у екосистемі щодо своїх власних залежностей або залежних від неї інших суб'єктів та може сприяти ширшому розумінню спільнотою ризиків. Організація регулярно опрацьовує та отримує інформацію від інших організацій, що доповнює власну створену інформацію та поширює її між іншими організаціями. Організація усвідомлює ризики кібербезпеки, пов'язані з послугами, які вона надає та якими користується.
Адаптивний	Організація адаптує свою практику в галузі кібербезпеки	В організації існує загальний підхід до управління ризиком	Організація розуміє свою роль у екосистемі щодо своїх власних

1	2	3	4
	на основі попередніх та поточних заходів з кібербезпеки, включаючи отримані результати та прогнозні показники. Завдяки процесу безперервного вдосконалення, що передбачає передові технології та практики кібербезпеки, організація активно адаптується до мінливих кіберзагроз та своєчасно й ефективно реагує на кіберзагрози, що розвиваються та ускладнюються.	кібербезпеки, який використовує політику, процеси та процедури з урахуванням ризиків для вирішення потенційних кіберінцидентів. Взаємозв'язок між ризиком кібербезпеки та цілями організації чітко усвідомлюється та враховується під час прийняття рішень. Головні виконавці контролюють ризик кібербезпеки в тому самому контексті, що і фінансовий ризик та інші ризики для організації. Управління ризиками кібербезпеки є частиною організаційної культури і розвивається на основі усвідомлення попередньої діяльності та постійного усвідомлення діяльності у своїх системах та телекомунікаційних мережах. Організація може швидко та ефективно враховувати зміни у тому, як підходити до опрацювання та повідомляти про ризик.	залежностей або залежних від неї інших суб'єктів, сприяє ширшому розумінню спільнотою ризиків. Організація отримує, генерує та переглядає пріоритетну інформацію для продовження аналізу цих ризиків по мірі розвитку ландшафту загроз та технологій. Організація поширює цю інформацією як в середині організації, так і назовні для подальшого опрацювання. Організація використовує інформацію в режимі реального часу або майже в режимі реального часу і послідовно реагує на ризики кібербезпеки, пов'язані з послугами, які вона надає та якими користується.

VII. Профіль кіберзахисту ОКІІ

1. Профіль кіберзахисту розробляється на основі системи заходів кіберзахисту, а також з урахуванням:

вимог галузевих стандартів, керівних принципів безпеки, політик безпеки та практик організації;

особливих вимог до кожного ОКІІ або ОКІ;

вимог до захисту інформації.

2. Профіль кіберзахисту дозволяє розробити план впровадження заходів кіберзахисту з метою зниження ризиків кібербезпеки, узгоджений з

цілями ОКІ та галузі (сектору) критичної інфраструктури, врахувати законодавчі та нормативні вимоги та передовий галузевий досвід із забезпечення кібербезпеки, а також відображає пріоритети управління ризиками кібербезпеки. Оскільки більшість ОКІІ мають складну організаційно-технічну структуру, використовують різні інформаційні, інформаційно-телекомунікаційні та автоматизовані системи управління технологічними процесами для надання життєво важливих послуг та функцій, можна розробляти кілька профілів кіберзахисту, узгоджених з конкретними системами, процесами та потребами ОКІІ, що призначені для надання життєво важливих послуг та функції.

3. Профіль кіберзахисту використовують для опису поточного стану реалізованих заходів кіберзахисту на ОКІІ (поточний профіль кіберзахисту) або бажаного цільового стану реалізації конкретних заходів кіберзахисту (цільовий профіль кіберзахисту).

У поточному профілі кіберзахисту зазначаються заходи та результати ефективності впроваджених заходів кіберзахисту, реалізовані та досягнуті на ОКІІ на цей час.

4. Цільовий профіль кіберзахисту зазначає заходи та цільові показники забезпечення кібербезпеки, необхідні для досягнення бажаних цілей управління ризиками кібербезпеки. Профілі підтримують стратегічні цілі ОКІ та допомагають обмінюватися даними про ризики кібербезпеки всередині ОКІІ та між ОКІІ всередині сектору критичної інфраструктури та об’єктами, що належать різним секторам критичної інфраструктури. У додатках 2 та 3 до Рекомендацій наведено приклади розробки профілів кіберзахисту. Ці приклади носять інформативний характер, що забезпечує гнучкість застосування Рекомендацій.

Профіль кіберзахисту рекомендується розробляти відповідно до вимог галузевих нормативних документів із захисту інформації та практичного досвіду забезпечення інформаційної безпеки та кібербезпеки ОКІ з урахуванням особливостей забезпечення кібербезпеки у відповідній сфері або галузі.

5. Порівняння профілів кіберзахисту (наприклад, поточного та цільового профілів) сприяє виявленню недоліків, що повинні бути усунуті для досягнення цілей управління ризиками кібербезпеки. Рекомендовано використання плану усунення недоліків як складової частини плану захисту інформації (плану кіберзахисту) ОКІІ. Пріоритетність заходів усунення недоліків базується на потребах ОКІ щодо надання основних послуг і процесах управління ризиками.

VIII. Розробка та впровадження профілю кіберзахисту ОКІІ

1. Розробку та впровадження профілю кіберзахисту рекомендується проводити за такими етапами:

І етап. Визначення пріоритетів та сфери застосування Рекомендацій. Визначаються цілі та організаційні пріоритети щодо надання життєво важливих послуг та функцій. За допомогою отриманої інформації приймається рішення щодо реалізації заходів кіберзахисту та визначається обсяг інформаційних систем та активів, які підтримують надання життєво важливих послуг та функцій. Рекомендації можуть бути адаптовані для підтримки різних напрямів діяльності, процесів та систем (інформаційно-телекомунікаційних систем, інформаційних систем, комп'ютерних систем, автоматизованих систем управління технологічними процесами тощо), необхідних для надання життєво важливих послуг та функцій;

ІІ етап. Аналіз середовища для надання життєво важливих послуг та функцій. Визначаються відповідні системи та активи, що безпосередньо забезпечують надання життєво важливих послуг та функцій, аналізуються нормативні вимоги та загальний підхід до управління ризиками для цих систем. На цьому етапі необхідно провести консультації із суб'єктами забезпечення кібербезпеки та отримати інформацію щодо визначення загроз та вразливостей, що застосовуються саме для цих систем та активів і притаманні їм;

ІІІ етап. Створення поточного профілю кіберзахисту. Розробляється поточний профіль кіберзахисту, вказуючи, які заходи кіберзахисту, що містяться в Рекомендаціях, реалізовані на цей час. По суті розробка поточного профілю кіберзахисту є етапом самоаналізу, який дозволяє ОКІІ з'ясувати, які заходи захисту інформації впроваджено на ОКІІ та на якому рівні вони реалізовані. Методичні рекомендації щодо розробки поточного профілю кіберзахисту наведено у додатку 2 до цих Рекомендацій.;

IV етап. Проведення оцінки ризику. Оцінка ризику кібербезпеки має базуватися на процесі оцінки ризику, який вже впроваджено на ОКІІ або на основі результатів попередньої оцінки ризиків (наприклад, отримані під час створення КСЗІ, СУІБ, системи інформаційної безпеки або проведення аудиту безпеки). Аналіз середовища експлуатації інформаційних систем та активів проводиться з метою визначення ймовірності настання кіберінцидентів/реалізації кібератак та оцінки наслідків, які можуть настати у результаті настання такої події. Важливо враховувати нові ризики, дані про загрози та вразливості, що сприяє надійному розумінню ймовірності та наслідків кіберінцидентів;

V етап. Створення цільового профілю кіберзахисту. Розробляється цільовий профіль кіберзахисту, що базується на аналізі заходів кіберзахисту цих Рекомендацій. Цільовий профіль кіберзахисту описує бажані результати

із забезпечення кібербезпеки ОКІІ. Організація може впроваджувати власні заходи кіберзахисту з метою врахування унікальних ризиків, що притаманні системам і процесам надання життєво важливих послуг та функцій. При створенні цільового профілю кіберзахисту мають бути розглянуті та враховані вплив та вимоги з кібербезпеки зовнішніх партнерів організації. Методичні рекомендації щодо розробки цільового профілю кіберзахисту наведено у додатку 3 до цих Рекомендацій.;

VI етап. Визначення, аналіз та пріоритизація недоліків. Проводиться порівняння поточного профілю кіберзахисту із цільовим профілем кіберзахисту для визначення недоліків. Далі рекомендується розроблення Плану дій щодо усунення виявлених недоліків, який відображає завдання, результати аналізу витрат/вигоди, а також ризики досягнення результатів цільового профілю кіберзахисту. Далі ОКІІ може визначити необхідні ресурси (фінансові, матеріальні, людські), потрібні для усунення недоліків. Методичні рекомендації щодо виявлення розривів наведено у додатку 4 до цих Рекомендацій.;

VII етап. Реалізація плану удосконалення заходів кіберзахисту. Визначається, які дії слід вживати для усунення виявлених недоліків. Під час реалізації плану постійно відстежуються відповідність поточної практики кіберзахисту цільовому профілю кіберзахисту. При цьому визначаються стандарти, нормативні документи, у тому числі ті, що стосуються сектору критичної інфраструктури та впроваджуються для забезпечення кібербезпеки.

2. Визначені етапи повторюються з метою постійної оцінки стану кібербезпеки та вдосконалення практики кіберзахисту. Термін повторення етапів встановлюється організацією, але рекомендується це робити не рідше одного разу в рік. Відстеження прогресу проводиться шляхом ітеративного оновлення поточного профілю кіберзахисту, а потім порівняння його із цільовим профілем кіберзахисту.

IX. Вимоги до інформування з кібербезпеки партнерів організації

1. Рекомендації визначають однаковий спосіб здійснення інформування з кібербезпеки взаємозалежними партнерами організації, відповідальними за надання ОКІ основних послуг. Приклади передбачають ситуації, коли:

організація може використовувати цільовий профіль кіберзахисту, щоб висловити вимоги щодо управління ризиками кібербезпеки зовнішньому постачальнику послуг;

організація може визначити свій стан кібербезпеки через поточний профіль кіберзахисту для звітування про результати або для порівняння з вимогами щодо придбання товарів і послуг;

організація, визначивши зовнішнього партнера, від якого залежить критична інфраструктура, може використовувати цільовий профіль кіберзахисту для вираження необхідних категорій і підкатегорій заходів кіберзахисту;

сектор критичної інфраструктури може створити цільовий профіль кіберзахисту, який може бути використаний серед його складових як початковий базовий профіль для побудови їх спеціальних цільових профілів кіберзахисту;

організація може краще управляти ризиками кібербезпеки своїх партнерів, оцінюючи їхнє становище у критично важливій інфраструктурі та більш широкій цифровій економіці, використовуючи рівні впровадження.

2. Комунікація та обмін інформацією з кібербезпеки особливо важливі серед партнерів організації «зверху-вниз» по ланцюгах постачання товарів і послуг.

Директор Департаменту кіберзахисту
Адміністрації Держспецзв’язку Данило МЯЛКОВСЬКИЙ