Н А К А З

АДМІНІСТРАЦІЇ ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ’ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

від 06 жовтня 2021 року

№ 601

Київ 2021

Прим. № __

АДМІНІСТРАЦІЯ ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ’ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

Н А К А З

м. Київ

№ 601

06.10.2021

Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної структури

Зміни затверджено наказами Адміністрації Держспецзв’язку від 12.10.2021 № 616 та від 10.07. 2022 № 343

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

НАКАЗУЮ:

1. Затвердити Методичні рекомендації щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури, що додаються.

2. Директору Департаменту кіберзахисту Адміністрації Державної служби спеціального зв’язку та захисту інформації України забезпечити протягом десяти робочих днів оприлюднення цього наказу на офіційному вебсайті Державної служби спеціального зв’язку та захисту інформації України.

3. Контроль за виконанням цього наказу покласти на заступника Голови Державної служби спеціального зв’язку та захисту інформації України відповідно до розподілу обов’язків.

Голова Служби
підполковник Юрій ЩИГОЛЬ

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

Зміни затверджено наказом Адміністрації Держспецзв'язку від 12.10.2021 № 616

Зміни затверджено наказом Адміністрації Держспецзв'язку від 10.07.2022 № 343

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ
щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури

I. 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.

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

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;

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-комунікаційних системах», «Про електронні комунікації», «Про стандартизацію», постановах Кабінету Міністрів України від 29 грудня 2021 року № 1426 «Про затвердження Положення про організаційно-технічну модель кіберзахисту», від 09 жовтня 2020 року № 943 «Деякі питання об'єктів критичної інфраструктури», від 09 жовтня 2020 року № 1109 «Деякі питання об'єктів критичної інформаційної 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 проєктування 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.

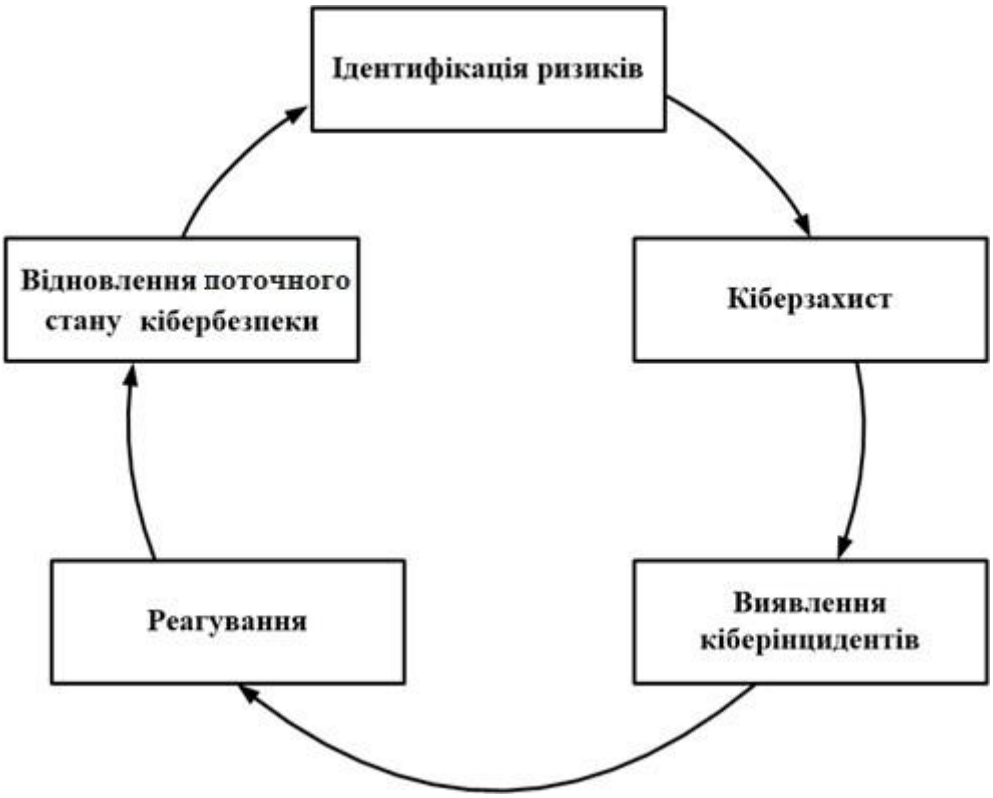

Рисунок 1 – Цикл управління кібербезпекою

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.

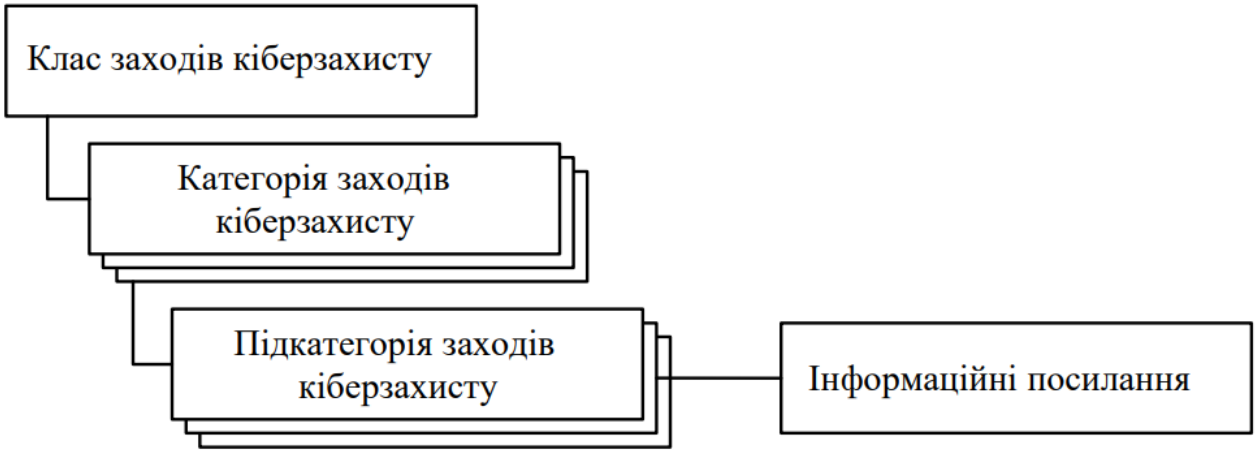

Рисунок 2 – Система заходів кіберзахисту

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 класифікацію 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
ID.GV Управління безпекою	Формування правил, процедур і процесів для управління й моніторингу впроваджених нормативних, екологічних та експлуатаційних вимог,	ID.GV-1 ID.GV-2 ID.GV-3

1	2	3
	а також вимог щодо забезпечення кібербезпеки.	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 ID.SC-5
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.AC-7
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 PR.IP-5 PR.IP-6 PR.IP-7 PR.IP-8 PR.IP-9 PR.IP-10

1	2	3
		PR.IP-11 PR.IP-12
PR.MA Технічне обслуговування	Технічне обслуговування та ремонт компонентів системи управління виробничими процесами, компонентів інформаційно-комунікаційних 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
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.AN-5
RS.MI Мінімізація наслідків	Виконання заходів з метою запобігання розширенню кіберінциденту, мінімізації його наслідків та	RS.MI-1 RS.MI-2

1	2	3
	унеможливлення його повторення.	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, постачальники електронних комунікаційних мереж та/або послуг, власники атакуючих систем, інші групи реагування на інциденти, пов’язані з інформаційною та/або кібербезпекою (CSIRT).	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.)

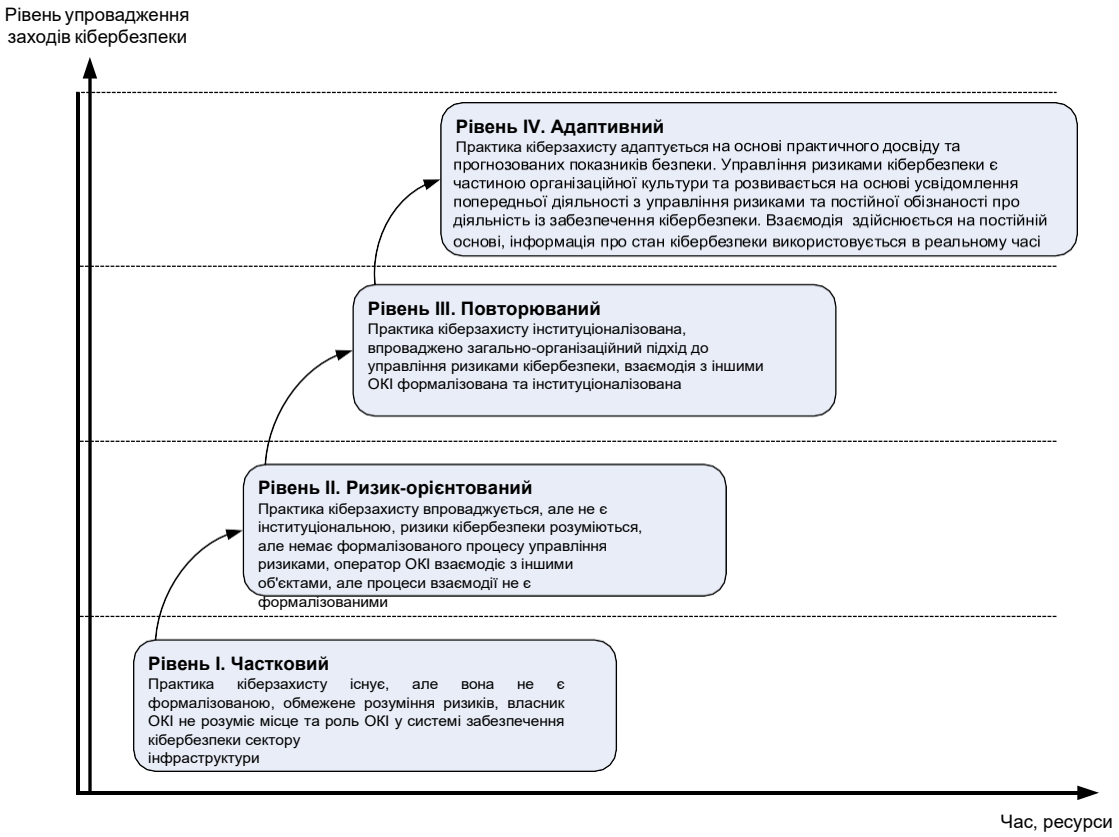

Рисунок 3 – Рівні впровадження заходів кіберзахисту

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	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	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

1	2	3	4
	ситуативний характер. Пріоритетність виконання заходів кіберзахисту безпосередньо не враховує цілі ОКІІ щодо управління ризиками, характеристики загроз, завдання щодо надання життєво важливих послуг та функцій.	впроваджуються нерегулярно, ситуативно, використовуючи різноманітний практичний досвід або інформацію, отриману із зовнішніх джерел. Процесів, що забезпечують внутрішній обмін інформацією про стан кібербезпеки, не зафіксовано.	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 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.	Існує усвідомлення ризику кібербезпеки на організаційному рівні, але 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.	Загалом організація розуміє свою роль у екосистемі щодо своїх 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	В організації існує загальний підхід до управління ризиками кібербезпеки. Політики інформування про ризики, процеси та процедури визначені,	Організація розуміє свою роль у екосистемі щодо своїх власних залежностей або залежних від неї інших суб'єктів та може сприяти ширшому розумінню спільнотою

1	2	3	4
	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.	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.	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 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	В організації існує загальний підхід до управління ризиком 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	Організація розуміє свою роль у екосистемі щодо своїх власних 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

1	2	3	4
	ефективно реагує на кіберзагрози, що розвиваються та ускладняються.	усвідомлення попередньої діяльності та постійного усвідомлення діяльності у своїх системах та комунікаційних мережах. Організація може швидко та ефективно враховувати зміни у тому, як підходити до опрацювання та повідомляти про ризик.	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-комунікаційні 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 - комунікаційних 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;

III 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

Додаток 1
до Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури, затверджених наказом Адміністрації Держспецзв'язку від 6 жовтня 2021 р. № 601 (у редакції наказу Адміністрації Держспецзв'язку від 10 липня 2022 р. № 343)

Класифікація заходів кіберзахисту

1. Клас заходів кіберзахисту ID – Ідентифікація ризиків кібербезпеки.

1.1. Категорія заходів кіберзахисту ID.AM – Управління активами.

Дані, персонал, обладнання, системи, пристрої та носії інформації, інформаційні системи, що дозволяють забезпечити надання життєво важливих послуг та функцій, виявлені та управляються відповідно до їх важливості відносно критично важливих послуг та функцій та стратегії управління ризиками ОКІ.

Таблиця 1 – Заходи кіберзахисту категорії ID.AM

Заходи кіберзахисту		
Захід кіберзахисту	Нормативні та додаткові посилання	Опис
1	2	3
ID.AM-1. Фізичне обладнання та системи на ОКІ ідентифіковано та задокументовано.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 - A.8.1.1, A.8.1.2; Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури, затверджені постановою № 518 (далі – Загальні вимоги) – пп. 3, 5, 6, 10; НД ТЗІ 1.4-001-2000 – п. Д3.1; НД ТЗІ 2.5-004-99 – п. 10.1; НД ТЗІ 3.6-006-21 – CM-8, PM-5; НД ТЗІ 3.7-001-99 – п. 6.3; НД ТЗІ 3.7-003-05 – п. 6.1.2; Довідкові посилання: COBIT 5 – BAI09.01, BAI09.02; IEC 62443-2-1:2010 – 4.2.3.4; IEC 62443-3-3:2013 – SR 7.8; NIST SP 800-53 Rev. 5 – CM-8, PM-5.	На ОКІ проводиться ідентифікація всіх пристроїв, носіїв інформації, інформаційних систем, що використовуються для надання життєво важливих послуг та функцій, здійснюється їх реєстрація.
ID.AM-2. Програмне забезпечення, що використовуються ОКІ	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 A.8.1.1, A.8.1.2;	Програмне забезпечення, що використовуються для забезпечення роботи ОКІІ

1	2	3
для надання життєво важливих послуг та функцій, ідентифіковано та задокументовано.	Загальні вимоги – пп. 3, 5, 6, 10; НД ТЗІ 1.4-001-2000 – п. Д3.1; НД ТЗІ 2.5-004-99 – п. 10.1; НД ТЗІ 3.6-006-21 – CM-8, PM-5; НД ТЗІ 3.7-001-99 – п. 6.3; НД ТЗІ 3.7-003-05 – п. 6.1.2; Довідкові посилання: COBIT 5 – BAI09.01, BAI09.02, BAI09.05; IEC 62443-2-1:2015 – 4.2.3.4; IEC62443-3-3:2016 – SR 7.8; NIST SP 800-53 Rev. 5 – CM-8, PM-5.	ОКІ, які забезпечують надання життєво важливих послуг та виконання життєво важливих функцій, повинні бути ідентифіковані та задокументовані.
ID.AM-3. Електронні комунікації та потоки даних ОКІ ідентифіковано та задокументовано.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.13.2.1; Загальні вимоги – пп. 5, 6, 53; НД ТЗІ 1.4-001-2000 – п. Д 3.2; НД ТЗІ 2.5-004-99 – п. 6.1, 6.2, 9.3; НД ТЗІ 3.6-006-21 – AC-4, CA-3, CA-9, PL-8. НД ТЗІ 3.7-001-99 – п. 6.3, 6.4.1; НД ТЗІ 3.7-003-05 – п. 6.1.2. Довідкові посилання: COBIT 5 – DSS05.02; IEC62443-2-1:2015 – 4.2.3.4; NIST SP 800-53 Rev. 5 – AC-4, CA-3, CA-9, PL-8.	Здійснюється інвентаризація електронних комунікацій та потоків даних, які в них циркулюють в тому числі із визначенням всіх підмереж, які використовуються для забезпечення надання основної послуги/виконання основної функції ОКІ. Розроблено структурну схему інформаційних потоків, яка відображає інформаційну взаємодію між основним компонентами (завданнями, об’єктами). Визначено, з прив’язкою до кожного елемента схеми, категорії інформації та рівні доступу до неї. Ця інформація є важливою для організацій, задля представлення цілісного уявлення про активи, що підтримують її інфраструктуру електронної комунікаційної мережі та існуючі потоки даних.
ID.AM-4. Зовнішні інформаційні та інформаційно-комунікаційні системи, промислові системи, які	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.11.2.6; Загальні вимоги – пп. 5, 7, 52; НД ТЗІ 2.5-004-99 – п. 9.7;	Інформаційні та інформаційно-комунікаційні системи, які взаємодіють з ОКІІ ОКІ (в тому числі, які

1	2	3
взаємодіють з інформаційно-комунікаційними та іншими системами ОКІ обліковано.	НД ТЗІ 3.6-006-21 – AC-20, SA-9; НД ТЗІ 3.7-001-99 – пп. 6.3, 6.4.1; НД ТЗІ 3.7-003-05 – п.6.1.2; Довідкові посилання: COBIT 5 – APO02.02; NIST SP 800-53 Rev. 5 – AC-20, SA-9.	розташовані, або можуть використовуватись за межами ОКІ), слід віднести до певного каталогу. Необхідно забезпечити безпечну роботу обладнання, яке може санкціоновано використовуватись поза межами ОКІ.
ID.AM-5. Критичність активів (обладнання, устаткування, даних, програмного забезпечення) ОКІ визначено відповідно до оцінки їх впливу на надання життєво важливих послуг та функцій ОКІ.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.8.2.1; Загальні вимоги – пп. 3, 5, 7; НД ТЗІ 1.4-001-2000 – п. Д5.6.2, 5.6.2.1; НД ТЗІ 3.6-006-21 – CP-2, RA-2, SA-14, SC-6; НД ТЗІ 3.7-001-99 – п. 5.2; НД ТЗІ 3.7-003-05 – п. 6.1.3. Довідкові посилання: COBIT 5 – APO03.03, APO03.04, BAI09.02; IEC 62443-2-1:2015 – 4.2.3.6; NIST SP 800-53 Rev. 5 – CP-2, RA-2, SA-14, SC-6.	Організація класифікує свої активи, враховуючи критичність процесів, для яких такі активи використовуються. Під час процесу інвентаризації організація визначає та затверджує метод класифікації активів.
ID.AM-6. Обов'язки штатного персоналу ОКІ та персоналу партнерів організації (наприклад – постачальників, клієнтів, тощо) щодо забезпечення кібербезпеки визначено та закріплено у відповідних документах.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.6.1.1; Загальні вимоги – пп. 5, 7, 8, 9; НД ТЗІ 1.4-001-2000 – п. 6, 7, 8, 9, 10; НД ТЗІ 2.5-004-99 – п. 9.4; НД ТЗІ 3.6-006-21 – CP-2, PS-7, PM-11; НД ТЗІ 3.7-001-99 – п. 6.3. Довідкові посилання: COBIT 5 – APO01.02, DSS06.03; IEC 62443-2-1:2015 – 4.3.2.3.3; NIST SP 800-53 Rev. 5 – CP-2, PS-7, PM-11.	Визначаються та описуються всі обов’язки та відповідальність штатного персоналу ОКІ та персоналу партнерів організації пов’язаних із забезпеченням кібербезпеки, взаємодією з іншими підрозділами організації та зовнішніми організаціями. На ОКІ затверджується та доводиться до персоналу політика інформаційної безпеки. Впроваджуються програми підвищення обізнаності/навчання працівників з питань забезпечення кібербезпеки.

1.2. Категорія заходів кіберзахисту ID.BE – Середовище надання життєво важливих послуг та функцій.

Мета, цілі, постачальники, клієнти, партнери тощо організації та діяльність ОКІ відносно надання життєво важливих послуг та функцій є зрозумілими та їх пріоритетність встановлено. Ця інформація використовується для формування обов'язків персоналу щодо забезпечення кібербезпеки, а також рішень з управління ризиками кібербезпеки.

Таблиця 2 – Заходи кіберзахисту категорії ID.BE

Заходи кіберзахисту		
Захід кіберзахисту	Нормативні та додаткові посилання	Опис
1	2	3
ID.BE-1. Роль ОКІ в ланцюгу постачання товарів і послуг визначено та повідомлено всім постачальникам організації.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – А.15.1.3, А.15.2.1, А.15.2.2; Загальні вимоги – п. 7; НД ТЗІ 3.6-006-21 – СР-2, SA-12. Довідкові посилання: COBIT 5 – APO08.04, APO08.05, APO10.03, APO10.04, APO10.05; NIST SP 800-53 Rev. 5 – CP-2, SA-12.	Організація ідентифікує та класифікує постачальників у відповідних ланцюгах поставок, враховуючи товари і послуги, що надаються згідно з чинними угодами та законодавством. В угодах з постачальниками можуть бути визначені вимоги з обробки ризиків, які пов’язані з безпекою постачання, послуги моніторяться та регулярно переглядаються та змінюються з урахуванням результатів повторної оцінки ризиків.
ID.BE-2. Місце та роль ОКІ в системі надання життєво важливих послуг та функцій сектору (підсектору) критичної інфраструктури визначено і повідомлено всім постачальникам організації.	Нормативні посилання: Загальні вимоги – п. 7; НД ТЗІ 3.7-001-99 – п. 6.3; НД ТЗІ 3.7-003-05 – п. 6.1.2; НД ТЗІ 3.6-006-21 – РМ-8. Довідкові посилання: COBIT 5 – APO02.06, APO03.01; NIST SP 800-53 Rev. 5 – PM-8.	ОКІ має визначити роль в своєму секторі критичної інфраструктури, категорію критичності, а також ідентифікувати та категоризувати власні ОКІІ.
ID.BE-3. Пріоритетність цілей, завдань і заходів щодо забезпечення кібербезпеки, надання життєво важливих	Нормативні посилання: Загальні вимоги – п. 7; НД ТЗІ 3.7-001-99 – п. 6.4.1; НД ТЗІ 3.7-003-05 – п. 6.1.3; НД ТЗІ 3.6-006-21 – РМ-11, SA-14.	На ОКІ визначаються пріоритети цілей, завдань і заходів щодо забезпечення кібербезпеки ОКІІ, що забезпечують надання життєво важливих послуг та

1	2	3
послуг та функцій встановлено та повідомлено.	Довідкові посилання: COBIT 5 – APO02.01, APO02.06, APO03.01; IEC 62443-2-1:2015 – 4.2.2.1, 4.2.3.6; NIST SP 800-53 Rev. 5 – PM-11, SA-14.	функцій. Такі пріоритети на ОКІ встановлюються та здійснюється інформування щодо них.
ID.BE-4. Залежності та найважливіші процеси для забезпечення надання життєво важливих послуг та функцій встановлено.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.11.2.2, A.11.2.3, A.12.1.3; Загальні вимоги – п. 7; НД ТЗІ 3.6-006-21 – CP-8, PE-9, PE-11, PM-8, SA-14; НД ТЗІ 3.7-001-99 – п. 6.3; НД ТЗІ 3.7-003-05 – п. 6.1.3/ Довідкові посилання: NIST SP 800-53 Rev. 5 – CP-8, PE-9, PE-11, PM-8, SA-14.	Організація забезпечує ідентифікацію та реєстрацію критично важливих активів, необхідних для надання життєво важливих послуг та функцій. Реєстрація містить принаймні таку інформацію: електронні комунікаційні мережі та інформаційні системи, що підтримують надання критично важливих послуг та функцій, які потребують захисту від відмови енергії або інших збоїв, спричинених аномаліями в службах підтримки; електронні комунікаційні мережі, які підтримують важливі послуги та потребують захисту від фальсифікації та перехоплення; планування потенціалу та моніторинг електронних комунікаційних мереж, інформаційних систем, що підтримують критично важливі послуги та функції, що дасть змогу зробити обґрунтовані прогнози майбутніх потреб і забезпечить стійкість до збоїв та кібератак.
ID.BE-5. Вимоги до стійкості ОКІ щодо забезпечення надання життєво важливих послуг та функцій встановлено.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1; Загальні вимоги – п. 7; НД ТЗІ 3.6-006-21 – CP-2, CP-11, SA-13, SA-14; НД ТЗІ 3.7-003-05 – п. 6.1.3.	Організація ідентифікує та визначає відповідні вимоги для забезпечення стійкості надання критично важливих послуг та функцій.

1	2	3
	Довідкові посилання: COBIT 5 – DSS04.02; NIST SP 800-53 Rev. 5 – CP-2, CP-11, SA-13, SA-14.	

1.3. Категорія заходів кіберзахисту ID.GV – Управління безпекою.

Правила, процедури і процеси для управління й моніторингу товарів і послуг нормативних, правових, екологічних та експлуатаційних вимог, а також вимог щодо забезпечення кібербезпеки ОКІ усвідомлено.

Таблиця 3 – Заходи кіберзахисту категорії ID.GV

Заходи кіберзахисту		
Захід кіберзахисту	Нормативні та додаткові посилання	Опис
1	2	3
ID.GV-1. Правила (політики) кібербезпеки ОКІ встановлено та задокументовано.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – А.5.1.1; Загальні вимоги – пп. 1, 2, 4, 7, 8; НД ТЗІ 1.1-002-99 – п. 6.2; НД ТЗІ 1.4-001-2000 – п. Д5; НД ТЗІ 2.5-004-99 – п. 6, 7, 8, 9; НД ТЗІ 3.6-006-21 – 1 засоби контролю всіх серій; НД ТЗІ 3.7-001-99 – п. 6.4.1; НД ТЗІ 3.7-003-05 – п. 6.2. Довідкові посилання: COBIT 5 – APO01.03, EDM01.01, EDM01.02; IEC 62443-2-1:2015 – 4.3.2.6; NIST SP 800-53 Rev. 5 – 1 засоби контролю всіх серій.	Організація: визначає політику інформаційної/ кібербезпеки; повідомляє про існування та зміст політики інформаційної/кібербезпеки для партнерів організації.
ID.GV-2. Обов'язки щодо забезпечення кібербезпеки ОКІ скоординовано та узгоджено з обов’язками персоналу ОКІ та із зовнішніми партнерами.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – А.6.1.1, А.7.2.1; Загальні вимоги – п. 2, 5, 7; НД ТЗІ 1.1-002-99 – п. 7.2.4; НД ТЗІ 1.4-001-2000 – п. 6; НД ТЗІ 2.5-004-99 – п. 9.4; НД ТЗІ 3.6-006-21 – PM-1, PM-2, PS-7; НД ТЗІ 3.7-001-99 – п. 6.4.1. Довідкові посилання: COBIT 5 – APO13.12; IEC 62443-2-1:2015 – 4.3.2.3.3; NIST SP 800-53 Rev. 5 – PM-1, PM-2, PS-7.	На ОКІ визначаються усі обов’язки, пов’язані із забезпеченням кібербезпеки ОКІ. Керівництво безпосередньо підтримує впровадження культури кібербезпеки, виконує вимоги з кібербезпеки та забезпечує дотримання вимог з кібербезпеки відповідно до прийнятих політик та процедур організації всім персоналом. ОКІ може взаємодіяти з державними органами, установами та підприємствами,

1	2	3
		що займаються питанням забезпечення кіберзахисту. У разі потреби до виконання робіт із забезпечення кіберзахисту можуть залучатися зовнішні організації, що мають ліцензії на відповідний вид діяльності у сфері кібербезпеки. У випадку укладення договору, у ньому можуть бути викладені чіткі вимоги із забезпечення кібербезпеки, як постачальником послуг, так і клієнтом.
ID.GV-3. Правові та нормативні вимоги щодо забезпечення кібербезпеки ОКІ, в тому числі зобов'язання щодо захисту недоторканості особистого життя (приватності), усвідомлено та управління ними здійснюється.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – А.18.1; Загальні вимоги – п. 5, 7, 8, 9; НД ТЗІ 2.5-004-99 – п. 9.4; НД ТЗІ 3.6-006-21 – 1 засоби контролю всіх серій; НД ТЗІ 3.7-001-99 – п. 6.4.1. Довідкові посилання: COBIT 5 – MEA03.01, MEA03.04; IEC 62443-2-1:2015 – 4.4.3.7; NIST SP 800-53 Rev. 5 – 1 засоби контролю всіх серій.	Організація узагальнює та виконує нормативно-правові та нормативні вимоги щодо кібербезпеки, дотримуючись національних та європейських норм, в тому числі щодо захисту недоторканості особистого життя (приватності).
ID.GV-4. Процеси управління безпекою та управління ризиками спрямовано на вирішення питання оброблення ризиків кібербезпеки.	Нормативні посилання: Загальні вимоги – п. 4, 5; НД ТЗІ 1.4-001-2000 – п. Д4; НД ТЗІ 3.6-006-21 – PM-3, PM-7, PM-9, PM-10, PM-11, SA-2. НД ТЗІ 3.7-001-99 – п. 6.8. Довідкові посилання: IEC 62443-2-1:2015 – 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3; NIST SP 800-53 Rev. 5 – PM-3, PM-7, PM-9, PM-10, PM-11, SA-2.	На ОКІ проводиться оцінка ризиків. Для проведення аналізу ризиків складаються переліки суттєвих загроз, вразливостей, через які загрози можуть бути реалізовано, описуються методи та способи обробки ризиків. Рекомендується оцінювати достатність заходів, які застосовуються для обробки, в тому числі зменшення ризиків кібербезпеки ОКІ, під час проведення аудиту інформаційної безпеки ОКІ або державної експертизи КСЗІ ОКІІ ОКІ

1.4. Категорія заходів кіберзахисту ID.RA – Оцінка ризиків.

ОКІ усвідомлює ризик кібербезпеки для процесів надання життєво важливих послуг та функцій (включаючи імідж або репутацію), а також активів ОКІ.

Таблиця 4 – Заходи кіберзахисту категорії ID.RA

Заходи кіберзахисту		
Захід кіберзахисту	Нормативні та додаткові посилання	Опис
1	2	3
ID.RA-1. Вразливості активів ОКІ проаналізовано, ідентифіковано та задокументовано.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.12.6.1, A.18.2.3; Загальні вимоги – п. 4, 5; НД ТЗІ 1.1-002-99 – п. 6.1, 6.5; НД ТЗІ 1.4-001-2000 – п. Д1.2, Д4, Д5.6.2.4; НД ТЗІ 3.6-006-21 – CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5. Довідкові посилання: COBIT 5 – APO12.01, APO12.02, APO12.03, APO12.04; IEC 62443-2-1:2015 – 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12; NIST SP 800-53 Rev. 5 – CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5.	Управління вразливістю є одним із процесів, який відбувається в організації для пом'якшення ризику в контексті кібербезпеки. Усі відомі вразливості були виявлені, але ще не пом'якшені чи не виправлені, оцінюються в організації та розглядаються шляхи їх виправлення або необхідність впровадження додаткових заходів із кіберзахисту.
ID.RA-2. Інформацію про загрози безпеки та вразливості отримано з форумів обміну інформацією та офіційних джерел.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.6.1.4; Загальні вимоги – п. 5, 6; НД ТЗІ 3.6-006-21 – PM-15, PM-16, SI-5. Довідкові посилання: IEC 62443-2-1:2015 – 4.2.3, 4.2.3.9, 4.2.3.12; NIST SP 800-53 Rev. 5 – PM-15, PM-16, SI-5.	Організація встановлює контакти з групами, які обмінюються інформацією про проблеми кібербезпеки та вразливості, обмінюються ідеями та досвідом, отримує доступ до постійно оновленої інформації про кіберзагрози, в тому числі, яка отримується іншими суб'єктами забезпечення кіберзахисту в наслідок проведення технічного розслідування кіберінцидентів/кібератак.
ID.RA-3. Загрози кібербезпеки (модель загроз) як внутрішні, так і зовнішні визначено й	Нормативні посилання: Загальні вимоги – п. 4, 5; НД ТЗІ 1.1-002-99 – п. 6.1, 6.4, 6.5; НД ТЗІ 1.4-001-2000 – п. Д4.2.3, Д4.3, Д4.4;	Відповідно до стратегії (політики) управління ризиками організація визначає та документує можливі загрози, які

1	2	3
задокументовано.	НД ТЗІ 3.6-006-21 – RA-3, SI-5, PM-12, PM-16; НД ТЗІ 3.7-003-05 – п. 6.1.2.9. Довідкові посилання: COBIT 5 – APO12.01, APO12.02, APO12.03, APO12.04; IEC 62443-2-1:2015 – 4.2.3, 4.2.3.9, 4.2.3.12; NIST SP 800-53 Rev. 5 – RA-3, SI-5, PM-12, PM-16.	можуть бути реалізовані через ідентифіковані вразливості в її активах.
ID.RA-4. Потенційні наслідки (рівень шкоди),які можуть завдати загрози в наслідок їх реалізації на безперервне надання життєво важливих послуг та функцій та ймовірності їх реалізації визначено.	Нормативні посилання: Загальні вимоги – п. 4, 5; НД ТЗІ 1.1-002-99 – п. 6.1, 6.5; НД ТЗІ 1.4-001-2000 – п. Д5.6.2.4; НД ТЗІ 3.6-006-21 – RA-2, RA-3, PM-9, PM-11, SA-14; НД ТЗІ 3.7-003-05 – п. 6.1.2.9. Довідкові посилання: COBIT 5 – DSS04.02; IEC 62443-2-1:2015 – 4.2.3, 4.2.3.9, 4.2.3.12; NIST SP 800-53 Rev. 5 – RA-2, RA-3, PM-9, PM-11, SA-14.	Виконується кількісна або якісна оцінка збитків, що можуть бути нанесені ОКІ внаслідок реалізації загроз. Оцінка складається з величин очікуваних збитків від втрати інформації або кожної з її властивостей (конфіденційність, доступність та цілісність) або від втрати керованості ОКІ внаслідок реалізації загрози.
ID.RA-5. Для визначення ризику застосовуються данні щодо загроз, вразливостей, їх ймовірностей та рівня шкоди використано для визначення ризику кібербезпеки.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.12.6.1; Загальні вимоги – п. 4, 5; НД ТЗІ 1.1-002-99 – п. 6.1 6.5; НД ТЗІ 1.4-001-2000 – п. Д5.6.2; НД ТЗІ 3.6-006-21 – RA-2, RA-3, PM-16; НД ТЗІ 3.7-003-05 – п. 6.1.2.9. Довідкові посилання: COBIT 5 – APO12.02; NIST SP 800-53 Rev. 5 – RA-2, RA-3, PM-16.	Організація визначає у методології управління ризиками, які є критерії для визначення ймовірності та впливу ризику. Ці критерії визначають рівень ризику. Вразливість та загрози враховуються під час процесу ідентифікації ризиків.
ID.RA-6. Заходи реагування на ризик кібербезпеки визначено та їх пріоритетність встановлено.	Нормативні посилання: Загальні вимоги – п. 4,5; НД ТЗІ 1.4-001-2000 – п. 8.1, 8.2, Д5.6.3; НД ТЗІ 3.6-006-21 – PM-4, PM-9. Довідкові посилання: COBIT 5 – APO12.05, APO13.02; NIST SP 800-53 Rev. 5 – PM-4, PM-9.	На підставі визначеної методології організація впроваджує заходи реагування на ризики, які ідентифіковані та рівні яких розраховано, з урахуванням їх пріоритетності.

1.5. Категорія заходів кіберзахисту ID.RM – Стратегія управління ризиками організації.

Пріоритети, обмеження, допустимий рівень ризику та припущення визначено та використано для підтримки операційних рішень щодо зниження (обробки) ризиків кібербезпеки.

Таблиця 5 – Заходи кіберзахисту категорії ID.RM

Заходи кіберзахисту		
Захід кіберзахисту	Нормативні та додаткові посилання	Опис
1	2	3
ID.RM-1. Процеси управління ризиками визначено, узгоджено із партнерами організації та управляються.	Нормативні посилання: Загальні вимоги – п. 4, 5; НД ТЗІ 1.4-001-2000 – п. Д4; НД ТЗІ 3.6-006-21 – PM-9. Довідкові посилання: COBIT 5 – APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02; IEC 62443-2-1:2015 – 4.3.4.2; NIST SP 800-53 Rev. 5 – PM-9.	Організація забезпечує належне визначення процесу управління ризиками та керується ними відповідно до попередніх угод із партнерами організації. Відповідно до стратегії (політики) управління ризиками організація: формулює комплексний підхід до управління ризиками, пов'язаний з використанням комп'ютерних мереж та інформаційних систем (ОКІІ); переконується, що визначений підхід послідовно застосовується в ОКІ; вказує осіб відповідальних за процес управління ризиками; вказує осіб відповідальних за обробку ризиків.
ID.RM-2. Допустимий рівень ризику кібербезпеки визначено та чітко виражено.	Нормативні посилання: Загальні вимоги – п. 4, 5; НД ТЗІ 1.4-001-2000 – п. Д4; НД ТЗІ 3.6-006-21 – PM-9. Довідкові посилання: COBIT 5 – APO12.06; IEC 62443-2-1:2015 – 4.3.2.6.5; NIST SP 800-53 Rev. 5 – PM-9.	Організація формулює в методології управління ризиками свій підхід до обробки ризиків та відповідний допустимий рівень ризику, встановлений в організації.
ID.RM-3. Визначення допустимого рівня ризику ґрунтується на ролі ОКІ як складової частини сектору критичної інфраструктури та аналізі ризиків, притаманних	Нормативні посилання: Загальні вимоги – п. 4, 5; НД ТЗІ 1.4-001-2000 – п. Д4; НД ТЗІ 3.6-006-21 – PM-8, PM-9, PM-11, SA-14. Довідкові посилання: NIST SP 800-53 Rev. 5 – PM-8, PM-9, PM-11, SA-14.	Організація визначає порядок обробки ризиків, врахування наявності остаточних ризиків з запобіганням їх взаємовпливу та можливих каскадних ефектів з урахуваннями визначеного рівня допустимості ризиків.

1	2	3
відповідному сектору критичної інфраструктури.		

1.6. Категорія заходів кіберзахисту ID.SC – Управління ризиками системи постачання.

Пріоритети, обмеження, допустимий рівень ризику та припущення щодо системи постачання ОКІ визначені та використовуються для підтримки рішень щодо ризиків, які пов'язані з системою постачання послуг третіми особами (ланцюгами постачання).

Таблиця 6 – Заходи кіберзахисту категорії ID.SC

Заходи кіберзахисту		
Захід кіберзахисту	Нормативні та додаткові посилання	Опис
1	2	3
ID.SC-1. Процеси управління ризиками кібербезпеки системи постачання визначено, узгоджено з партнерами організації та управляються.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1,A.15.2.2; Загальні вимоги – п. 4, 5; НД ТЗІ 1.4-001-2000 – п. Д7.1; НД ТЗІ 3.6-006-21 – SA-9, SA-12, PM-9. Довідкові посилання: COBIT 5 – APO12.02; IEC 62443-2-1:2015 – 4.3.4.2; NIST SP 800-53 Rev. 5 – SA-9, SA-12, PM-9.	Організація проводить аудит постачальників товарів і послуг, використовуючи ту саму методологію, яку вона використовує внутрішньо для управління ризиками.
ID.SC-2. Постачальники (розпорядники) інформаційних систем, товарів і послуг для ОКІ ідентифіковано, рівень їх критичності оцінено у відповідності до політики управління ризиками кібербезпеки з урахуванням ризиків, притаманних системі постачання.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.15.2.1, A.15.2.2; Загальні вимоги – п. 4, 5; НД ТЗІ 1.4-001-2000 – п. Д7.1; НД ТЗІ 3.6-006-21 – RA-2, RA-3, SA-12, SA-14, SA-15, PM-9. Довідкові посилання: COBIT 5 – APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03; IEC 62443-2-1:2015 – 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.12, 4.2.3.14; NIST SP 800-53 Rev. 5 – RA-2, RA-3, SA-12, SA-14, SA-15, PM-9.	Постачальники товарів і послуг для ОКІ ідентифікується. Організація класифікує своїх постачальників за: доступом до конфіденційної інформації; можливим впливом на ланцюг поставок; товарами і послугами, що надаються.
ID.SC-3.	Нормативні посилання:	У випадку укладення

1	2	3
Постачальники товарів і послуг та партнери, у відповідності до договору, можуть впроваджувати заходи, спрямовані на досягнення мети політики інформаційної безпеки/кібербезпеки ОКІ та плану управління ризиками постачання.	ДСТУ ISO/IEC 27001:2013 – A.15.1.1, A.15.1.2, A.15.1.3; Загальні вимоги – п. 4, 5; НД ТЗІ 1.4-001-2000 – п. Д7.1; НД ТЗІ 3.6-006-21 – SA-9, SA-11, SA-12, PM-9. Довідкові посилання: COBIT 5 – APO10.01, APO10.02, APO10.03, APO10.04, APO10.05; IEC 62443-2-1:2015 - 4.3.2.6.4, 4.3.2.6.7; NIST SP 800-53 Rev. 5 – SA-9, SA-11, SA-12, PM-9.	договору із постачальниками товарів і послуг у ньому можуть бути прямо вказані вимоги із забезпечення належного рівня надання послуг, в тому числі взаємні обов'язки із кіберзахисту інформації, до якої постачальник може отримати доступ (обробка, зберігання, взаємодія), або ОКІІ. Здійснюється періодичний контроль виконання постачальником своїх зобов'язань, обзори результатів аудитів, або інші, еквівалентні перевірки постачальників.
ID.SC-4. Постачальники товарів і послуг та партнери регулярно оцінюються за допомогою аудитів, результатів тестів або інших форм оцінки, щоб підтвердити, що вони виконують свої договірні зобов'язання.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.15.2.1, A.15.2.2; Загальні вимоги – п. 4, 7; НД ТЗІ 3.6-006-21 – AU-2, AU-6, AU-12, AU- 16, PS-7, SA-9, SA-12. Довідкові посилання: COBIT 5 – APO10.01, APO10.03, APO10.04, APO10.05, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05 ISA 62443-2-1:2009 – 4.3.2.6.7 ISA 62443-3-3:2013 – SR 6.1 NIST SP 800-53 Rev. 5 – AU-2, AU-6, AU-12, AU- 16, PS-7, SA-9, SA-12.	Організація відстежує на постійній основі ринок постачальників товарів і послуг, партнерів та проводить аудит, щоб встановити, яким чином здійснюється надання послуг, чи виконуються ними договірні зобов'язання в повному обсязі. Необхідним є відстеження змін у наданні послуг постачальниками та партнерами, включаючи підтримку і покращення існуючих політик інформаційної безпеки, процедур і засобів управління, з урахуванням критичності інформації, яка циркулює в організації, систем і процесів, які використовуються, та повторної оцінки ризиків
ID.SC-5. З постачальниками здійснюється планування та тестування реагування за відповідними політиками реагування	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.17.1.3; Загальні вимоги – п. 4,5; НД ТЗІ 1.4-001-2000 – п. Д7.1; НД ТЗІ 3.6-006-21 – CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9. Довідкові посилання:	Організація визначає, які постачальники братимуть участь у опрацюванні заходів реагування та планах відновлення, щоб забезпечити їх участь у запланованих навчаннях з

1	2	3
на кіберінциденти та відновлення стану кібербезпеки.	COBIT 5 – DSS04.04; IEC 62443-2-1:2015 – 4.3.3.5.1; IEC 62443-3-3:2016 – SR 2.8, SR 3.3, SR 6.1, SR 7.3, SR 7.4; NIST SP 800-53 Rev. 5 – CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9.	реагування на кіберінциденти. Плани реагування існують та регулярно тестуються та покращуються.

2. Клас заходів кіберзахисту PR – Кіберзахист.

2.1. Категорія заходів кіберзахисту PR.AC – Управління ідентифікацією, автентифікацією та контроль доступу.

Доступ до фізичних і логічних ресурсів ОКІ та пов'язаних з ними об'єктів надається тільки авторизованим користувачам, адміністраторам, процесам або пристроям та управляється відповідно до встановленого рівня ризику несанкціонованого доступу.

Таблиця 7 – Заходи кіберзахисту категорії PR.AC

Заходи кіберзахисту		
Захід кіберзахисту	Нормативні та додаткові посилання	Опис
1	2	3
PR.AC-1. Ідентифікатори та дані автентифікації для авторизованих користувачів, адміністраторів та процесів призначаються, верифікуються, адмініструються, відкликаються (скасовуються) та перевіряються.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3; Загальні вимоги – п. 11, 12, 13, 14, 15, 16, 17; НД ТЗІ 1.1-002-99 – п. 7.2, 7.2.2; НД ТЗІ 1.4-001-2000 – п. Д5.7; НД ТЗІ 2.5-004-99 – п.8.1; НД ТЗІ 3.7-001-99 – п. 6.4.1; НД ТЗІ 3.6-006-21 – AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11. Довідкові посилання: COBIT 5 – DSS05.04, DSS06.03; IEC 62443-2-1:2015 - 4.3.3.5.1; IEC 62443-3-3:2016 - SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9; NIST SP 800-53 Rev. 5 – AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11.	Організація забезпечує управління та перевірку, періодичний перегляд особистих обов’язків та повноважень користувачів, адміністраторів організації, керує ними, перевіряє, скасовує відповідно до встановлених внутрішніх процесів.
PR.AC-2. Фізичний доступ до ОКІІ	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 –	Організація охороняє та керує фізичним доступом до своїх

1	2	3
захищений та управляється.	A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8; Загальні вимоги – п. 27, 28, 31, 49, 50, 51; НД ТЗІ 1.1-002-99 – п. 7.2, 7.2.2, 7.2.3; НД ТЗІ 1.4-001-2000 – п. Д5.7; НД ТЗІ 3.7-001-99 – п. 6.4.1; НД ТЗІ 3.6-006-21 – PE-2, PE-3, PE-4, PE5, PE-6, PE-8. Довідкові посилання: COBIT 5 – DSS01.04, DSS05.05; IEC 62443-2-1:2015 - 4.3.3.3.2, 4.3.3.3.8; NIST SP 800-53 Rev. 5 – PE-2, PE-3, PE-4, PE5, PE-6, PE-8.	об'єктів та інфраструктури, що підтримують її електронні комунікаційні мережі та інформаційні системи. Цей контроль застосовується до всіх співробітників та відвідувачів, «чутливих» зон, до яких доступ обмежений, або до «чутливих» районів, в яких обробляється конфіденційна інформація, в яких розміщені електронні комунікаційні мережі або інформаційні системи.
PR.AC-3. Здійснюється контроль та управління віддаленого доступу.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1; Загальні вимоги – п. 18; НД ТЗІ 1.1-002-99 – п. 7.2, 7.2.2, 7.2.3; НД ТЗІ 1.4-001-2000 – п. Д5.7; НД ТЗІ 2.5-004-99 – п. 8.1, 9.8; НД ТЗІ 3.6-006-21 – AC-1, AC-17, AC-19, AC-20, SC-15. Довідкові посилання: COBIT 5 – APO13.01, DSS01.04, DSS05.03; IEC 62443-2-1:2015 – 4.3.3.6.6; IEC 62443-3-3:2016 – SR 1.13, SR 2.6; NIST SP 800-53 Rev. 5 – AC-1, AC-17, AC-19, AC-20, SC-15.	Організація має політику віддаленого доступу у відповідності до якої здійснюється управління ним та контролюється віддалений доступ до своїх електронних комунікаційних мереж та інформаційних систем. Віддалений доступ включає всі види доступу до мережевих або інформаційних систем через зовнішні електронні комунікаційні мережі, які не підконтрольні організації. VPN в разі їх створення, розглядаються як внутрішні засоби доступу і мають принаймні однаковий контроль безпеки; доступ до публічної інформації не вважається віддаленим доступом.
PR.AC-4. Права доступу встановлено із застосуванням принципів мінімальних привілеїв та розподілу обов'язків.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5; Загальні вимоги – п. 11, 12; НД ТЗІ 1.1-002-99 – п. 7.2, 7.2.2, 7.2.3; НД ТЗІ 1.4-001-2000 – п. Д5.7; НД ТЗІ 2.5-004-99 – п.8.1; НД ТЗІ 3.6-006-21 – AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24.	Доступ надається на основі принципів мінімальних привілеїв і поділу обов'язків. Принципи мінімальних привілеїв свідчать, що доступ до електронних комунікаційних мереж та інформаційних систем необхідний користувачам для виконання обов’язків. Розподіл обов'язків передбачає, що привілеї діляться між кількома особами, щоб особливо критичні процеси не

1	2	3
	Довідкові посилання: COBIT 5 – DSS05.04; IEC 62443-2-1:2015 – 4.3.3.7.3; IEC 62443-3-3:2016 – SR 2.1; NIST SP 800-53 Rev. 5 – AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24.	виконувалися однією особою. Основною причиною розподілу обов'язків є запобігання кіберінцидентам, які можуть вплинути на операційну діяльність організації. Тимчасово встановлені привілеї щодо прав доступу постійно переглядаються та скасовуються одразу після виконання завдання, задля виконання якого такі привілеї було встановлено.
PR.AC-5. Цілісність електронної комунікаційної мережі захищено (наприклад, сегментація мережі).	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3; Загальні вимоги – п. 18, 25, 26, 27, 28, 29, 30, 31, 32, 35; НД ТЗІ 2.5-004-99 – п. 9.5; НД ТЗІ 3.6-006-21 – AC-4, AC-10, SC-7; НД ТЗІ 3.7-001-99 – п. 6.4.1. Довідкові посилання: COBIT 5 – DSS01.04, DSS05.05; IEC 62443-2-1:2015 – 4.3.3.4; IEC 62443-3-3:2016 – SR 3.1, SR 3.8; NIST SP 800-53 Rev. 5 – AC-4, AC-10, SC-7.	Цілісність електронної комунікаційної мережі захищена за допомогою поділу і сегментації мережі. Проєктування електронної комунікаційної мережі унеможливлює отримання доступу до будь-якої системи з будь-якої підмережі. Зони безпеки визначаються з чітко сформульованими цілями та чітко визначеними бар'єрами, які забезпечують обладнання безпеки.
PR.AC-6. Ідентичність особи підтверджується і прив’язується до облікових даних та затверджується під час взаємодії	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.7.1.1, A.9.2.1; Загальні вимоги – п. 13 -18; НД ТЗІ 2.5-010-03 – п. 7.2.9, 7.2.10; НД ТЗІ 2.5-004-99 – п. 9.2, 9.7, A.2.2, A.2.7; НД ТЗІ 2.5-008-2002 –п. 6.5.3, 6.5.4, 6.5.12, 7.4.5; НД ТЗІ 3.6-006-21 – AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3. Довідкові посилання: CIS CSC 16; COBIT 5 – DSS05.04, DSS05.05, DSS05.07, DSS06.03; ISA 62443-2-1:2009 – 4.3.3.2.2,	Перевірка кандидатів при прийманні на роботу проводиться відповідно до вимог чинного законодавства та етичних норм. Організація оцінює чи відповідає кандидат наявним бізнес-вимогам, присвоює категорію інформації, до якої передбачається доступ, оцінює ризики. Організація забезпечує процес реєстрації і відміни такої реєстрації всіх користувачів організації з можливістю надання відповідних прав доступу.

1	2	3
	4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4; ISA 62443-3-3:2013 – SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1; NIST SP 800-53 Rev. 5 – AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3	
PR.AC-7. Автентифікація користувачів, адміністраторів, пристроїв та інших активів здійснюється (наприклад методами однофакторної, багатофакторної автентифікації) відповідно до встановленого ризику порушення безпеки.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.9.2.1., A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4; Загальні вимоги – п. 15; НД ТЗІ 2.5-004-99 – п. 9.7, 9.8, 9.9; НД ТЗІ 3.6-006-21 – AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11; НД ТЗІ 3.7-001-99 – п. 6.4.1. Довідкові посилання: COBIT 5 – DSS05.04, DSS05.10, DSS06.10; IEC 62443-2-1:2015 – 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9; IEC 62443-3-3:2016 – SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10; NIST SP 800-53 Rev. 5 – AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11.	Механізми автентифікації визначаються та оновлюються з метою забезпечення цілісності та конфіденційності інформації.

2.2. Категорія заходів кіберзахисту PR.AT – Обізнаність та навчання.

Співробітники ОКІ та партнерів організації поінформовані та обізнані з питаннями кібербезпеки, 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 правил, процедур, вимог договорів.

Таблиця 8 – Заходи кіберзахисту категорії PR.AT

Заходи кіберзахисту		
Захід кіберзахисту	Нормативні та додаткові посилання	Опис
1	2	3
PR.AT-1. Усі співробітники ОКІ	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 –	Організація формує план дій для навчання працівників з питань

1	2	3
обізнані та пройшли підготовку з питань кібербезпеки.	А.7.2.2; Загальні вимоги – п. 1, 2, 9; НД ТЗІ 1.1-002-99 – п. 7.2.4; НД ТЗІ 1.4-001-2000 – п. 8.3; НД ТЗІ 3.6-006-21– АТ-2, РМ-13. Довідкові посилання: COBIT 5 – APO07.03, BAI05.07; IEC 62443-2-1:2015 – 4.3.2.4.2; NIST SP 800-53 Rev. 5 – АТ-2, РМ-13.	кібербезпеки. Розробляє процеси і процедури для забезпечення належного проведення заходів і стежить за успіхом навчальних заходів.
PR.AT-2. Користувачі (адміністратори) з превагами доступу розуміють свої обов’язки з питань кібербезпеки.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – А.6.1.1, А.7.2.2; Загальні вимоги – п. 1,2; НД ТЗІ 3.6-006-21 – АТ-3, РМ-13. Довідкові посилання: COBIT 5 – APO07.02, DSS06.03; IEC 62443-2-1:2015 – 4.3.2.4.2, 4.3.2.4.3; NIST SP 800-53 Rev. 5 – АТ-3, РМ-13.	Співробітники, яким надано привілеї доступу до мереж або інформаційних систем ретельно вивчають свої обов'язки, необхідні для своїх функцій. Організація окреслює програму необхідного навчання, забезпечує його ефективність.
PR.AT-3. Партнери організації розуміють свої обов’язки з питань кібербезпеки.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – А.6.1.1, А.7.2.2; Загальні вимоги – п. 7; НД ТЗІ 3.6-006-21 – PS-7, SA-9, SA-16. Довідкові посилання: COBIT 5 – APO07.03, APO10.04, APO10.05; IEC 62443-2-1:2015 – 4.3.2.4.2; NIST SP 800-53 Rev. 5 – PS-7, SA-9, SA-16.	Партнери організації знають та розуміють свої обов'язки в рамках програми кібербезпеки організації. Організація проводить навчальні семінари для партнерів організації, та регулярно надає їх оновлені дані щодо політик і процедур організації, суттєвих для виконання їх зобов’язань по відношенню до ОКІ.
PR.AT-4. Керівництво ОКІ розуміє свої обов’язки з питань кібербезпеки.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – А.6.1.1, А.7.2.2; Загальні вимоги – п. 2; НД ТЗІ 3.6-006-21 – АТ-3, РМ-13. Довідкові посилання: IEC 62443-2-1:2015 – 4.3.2.4.2; COBIT 5 – APO07.03; NIST SP 800-53 Rev. 5 – АТ-3, РМ-13.	Керівництво усвідомлює свої обов'язки з питань кібербезпеки, спрямовує роботу підрозділу кібербезпеки, здійснює відповідне забезпечення.
PR.AT-5. Персонал із забезпечення	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 –	Визначаються та призначаються всі обов’язки, пов’язані із забезпеченням

1	2	3
фізичної та інформаційної безпеки розуміє свої обов'язки.	A.6.1.1, A.7.2.2; Загальні вимоги – п. 2; НД ТЗІ 2.5-004-99 – п. 9.4; НД ТЗІ 3.6-006-21 – AT-3, IR-2, PM-13. Довідкові посилання: COBIT 5 – APO07.03; IEC 62443-2-1:2015 – 4.3.2.4.2; NIST SP 800-53 Rev. 5 – AT-3, IR-2, PM-13.	фізичної та інформаційної безпеки. Персонал має належну кваліфікацію, на постійній основі проводиться підвищення кваліфікації, він розуміє межі своїх повноважень.

2.3. Категорія заходів кіберзахисту PR.DS – Безпека даних.

Інформація та документація (дані) управляються відповідно до стратегії (політики) управління ризиками кібербезпеки ОКІ з метою захисту конфіденційності, цілісності та доступності інформації.

Таблиця 9 – Заходи кіберзахисту категорії PR.DS

Заходи кіберзахисту		
Захід кіберзахисту	Нормативні та додаткові посилання	Опис
1	2	3
PR.DS-1. Дані, що зберігаються, захищено	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.8.2.3; Загальні вимоги – п. 21, 38, 40, 42, 43, 50; НД ТЗІ 2.5-004-99 – 6.1, 6.2, 6.3, 7.1, 7.2; НД ТЗІ 3.6-006-21 – MP-8, SC-12, SC-28. Довідкові посилання: COBIT 5 – APO01.06, BAI02.01, BAI06.01, DSS06.06; IEC 62443-3-3:2016 – SR 3.4, SR 4.1; NIST SP 800-53 Rev. 5 – MP-8, SC-12, SC-28.	В електронних комунікаційних мережах та інформаційних системах забезпечують конфіденційність, цілісність та доступність даних організації. Криптографічна перевірка збережених даних проводиться.
PR.DS-2. Дані, що передаються, захищено.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3; Загальні вимоги – п. 34, 35, 36, 37; НД ТЗІ 2.5-004-99 – 6.5, 7.1,7.2, 7.4; НД ТЗІ 3.6-006-21 – SC-8, SC-11, SC-12. НД ТЗІ 3.7-001-99 – п. 6.4.2. Довідкові посилання: COBIT 5 – APO01.06, DSS06.06; IEC 62443-3-3:2016 – SR 3.1, SR 3.8,	Організація забезпечує захист даних, що передаються.

1	2	3
	SR 4.1, SR 4.2; NIST SP 800-53 Rev. 5 – SC-8, SC-11, SC-12.	
PR.DS-3. Управління активами здійснюється з дотриманням правил видалення, передачі та розміщення.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.7; Загальні вимоги – п. 19, 20; НД ТЗІ 2.5-004-99 – 7.3, 8.1; НД ТЗІ 3.6-006-21 – CM-8, MP-6, PE-16. Довідкові посилання: COBIT 5 – BAI09.03; IEC 62443-2-1:2015 – 4.3.3.3.9, 4.3.4.4.1; IEC 62443-3-3:2016 – SR 4.2; NIST SP 800-53 Rev. 5 – CM-8, MP-6, PE-16.	В організації встановлені правила безпечного видалення, передачі та утилізації інформації або активів, які її містять. У тих випадках, коли така інформація більше не є актуальною для організації, застосовуються механізми її безпечного видалення з урахуванням політики класифікації інформації. При передачі на знищення обладнання стороннім організаціями забезпечується видалення робочої інформації організації, персональних даних та ліцензій ПЗ.
PR.DS-4. Необхідні спроможності для забезпечення доступності активів створено та підтримуються.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.12.3.1; Загальні вимоги – п. 38, 39; НД ТЗІ 2.5-004-99 – п. 8.1,8.2, 8.3, 8.4; НД ТЗІ 3.6-006-21 – AU-4, CP-2, SC-5. Довідкові посилання: COBIT 5 – APO13.01; IEC 62443-3-3:2016 – SR 7.1, SR 7.2; NIST SP 800-53 Rev. 5 – AU-4, CP-2, SC-5.	Спроможність електронної комунікаційної мережі та інформаційної системи контролюється задля забезпечення доступності активів. При плануванні їх розвитку передбачаються майбутні потреби на основі прогнозів, результатів минулого використання, з метою забезпечення відповідної продуктивності системи вимогам щодо надання життєво важливих послуг та функцій.
PR.DS-5. Захист від витоку даних впроваджено.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3; Загальні вимоги – п. 28 ,29, 32 ,37, 51; НД ТЗІ 2.5-004-99 – п. 6.4; НД ТЗІ 3.6-006-21 – AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4;	Організація запроваджує контроль безпеки на периметрах електронної комунікаційної мережі та інформаційних систем, ОКІІ для виявлення несанкціонованих витоків даних.

1	2	3
	НД ТЗІ 3.7-001-99 – п. 6.4.2. Довідкові посилання: COBIT 5 – APO01.06; IEC 62443-3-3:2016 – SR 5.2; NIST SP 800-53 Rev. 5 – AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4.	
PR.DS-6. Механізми перевірки цілісності використовуються для верифікації програмного забезпечення, програмно-апаратних засобів та цілісності інформації.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3; Загальні вимоги – п. 44, 45, 46, 47, 48; НД ТЗІ 2.5-004-99 – 7.1, 7.2, 7.3, 7.4; НД ТЗІ 3.6-006-21 – SC-16, SI-7. Довідкові посилання: IEC 62443-3-3:2016 – SR 3.1, SR 3.3, SR 3.4, SR 3.8; NIST SP 800-53 Rev. 5 – SC-16, SI-7.	Організація використовує механізми перевірки для забезпечення верифікації програмного забезпечення і цілісності даних. Ці заходи контролю призначені для виявлення несанкціонованого втручання або непередбачених помилок, викликаних неправомірним використанням.
PR.DS-7. Середовища розробки та тестування відокремлені від виробничого середовища.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 A.12.1.4; Загальні вимоги – п. 28, 39; НД ТЗІ 2.5-004-99 – п. 10.2, 10.3; НД ТЗІ 3.6-006-21 – CM-2. Довідкові посилання: COBIT 5 – BAI07.04; NIST SP 800-53 Rev. 5 – CM-2.	Організація забезпечує розділення середовищ виробництва, випробувань та розробок, логічно чи фізично. Середовища розробки та тестування розділені не тільки за доступом, але й за рівнем даних.
PR.DS-8. Механізми перевірки цілісності використовуються для перевірки цілісності обладнання	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.11.2.4; НД ТЗІ 2.5-004-99 – п. 5, п. 7, А.2; НД ТЗІ 3.6-006-21 – SA-10, SI-7; НД ТЗІ 3.7-001-99 – п. 6.1, п. 10. Довідкові посилання: COBIT 5 – BAI03.05; NIST SP 800-53 Rev. 5 – SA-10, SI-7; ISA 62443-2-1:2009 4.3.4.4.4	Організація забезпечує цілісність обладнання, запроваджуючи періодичні перевірки та перевірки виробником самого обладнання або сертифікованим постачальником цього самого обладнання

2.4. Категорія заходів кіберзахисту PR.IP – Процеси та процедури кіберзахисту.

Забезпечення підтримання та управління політикою (правилами) безпеки, процесами та процедурами, які стосуються мети, області дії, ролей, сфер відповідальності, прихильності керівництва і координації між підрозділами організації (ОКІ) та які використовуються для управління захистом інформаційних систем і активів ОКІ.

Таблиця 10 – Заходи кіберзахисту категорії PR.IP

Заходи кіберзахисту

Захід кіберзахисту	Нормативні та додаткові посилання	Опис
1	2	3
PR.IP-1. Базова конфігурація інформаційно-комунікаційних систем/систем управління виробничими процесами створена й підтримується.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4; Загальні вимоги – п. 7, 41, 43; НД ТЗІ 1.1-002-99 – п. 7.4 НД ТЗІ 2.5-004-99 – п. 10.1; НД ТЗІ 3.6-006-21 – CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10. Довідкові посилання: COBIT 5 - BAI10.01, BAI10.02, BAI10.03, BAI10.05; IEC 62443-2-1:2015 – 4.3.4.3.2, 4.3.4.3.3; IEC 62443-3-3:2016 – SR 7.6; NIST SP 800-53 Rev. 5 – CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10.	Організація встановлює базову конфігурацію інформаційно-комунікаційних систем/систем управління виробничими процесами. Базова конфігурація передбачає: програмне забезпечення, встановлене на робочих станціях; персональне обладнання, ноутбуки, принтери та кінцеве обладнання; сервери та елементи електронної комунікаційної мережі; конфігурацію та параметри у відповідності до встановлених правил (політик); відповідність запланованій топології електронної комунікаційної мережі та архітектурі логічних мереж та інформаційних систем.
PR.IP-2. Життєвий цикл розробки, експлуатації та управління системами (SDLC) впроваджено.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5; Загальні вимоги – п. 5; НД ТЗІ 1.1-002-99 – п. 7.4; НД ТЗІ 2.5-004-99 – п. 10.3; НД ТЗІ 3.7-001-99 – п. 6.4; НД ТЗІ 3.6-006-21 – PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI- 13, SI-14, SI-16, SI-17. Довідкові посилання: COBIT 5 – APO13.01; IEC 62443-2-1:2015 – 4.3.4.3.3; NIST SP 800-53 Rev. 5 – PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI- 13, SI-14, SI-16, SI-17.	Організація застосовує обґрунтовані інженерні принципи захисту інформації щодо специфікації, проєктування, розробки, впровадження та зміни електронних комунікаційних мереж та інформаційних систем. Ці принципи застосовуються як до систем, що створюються, так і до існуючих, які зазнають значних змін. До застарілих систем ці принципи застосовуються по можливості, враховуючи стан обладнання, програмного забезпечення тощо.
PR.IP-3. Процеси (заходи) управління змінами конфігурації впроваджено.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4;	Організація запроваджує процес управління змінами конфігурації.

1	2	3
	Загальні вимоги – п. 10; НД ТЗІ 1.1-002-99 – п. 7.4; НД ТЗІ 2.5-004-99 – п. 10.3, 10.6; НД ТЗІ 3.7-001-99 – п. 6.7; НД ТЗІ 3.6-006-21 – CM-3, CM-4, SA-10. Довідкові посилання: COBIT 5 – BAI06.01, BAI01.06; IEC 62443-2-1:2015 - 4.3.4.3.2, 4.3.4.3.3; IEC 62443-3-3:2016 – SR 7.6; NIST SP 800-53 Rev. 5 – CM-3, CM-4, SA-10.	
PR.IP-4. Резервне копіювання інформації проводиться, підтримується та періодично тестується.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3; Загальні вимоги – п. 38; НД ТЗІ 2.5-004-99 – п. 8.3, 8.4; НД ТЗІ 3.6-006-21 – CP-4, CP-6, CP-9. Довідкові посилання: COBIT 5 – APO13.01; IEC 62443-2-1:2015 – 4.3.4.3.9; IEC 62443-3-3:2016 – SR 7.3, SR 7.4; NIST SP 800-53 Rev. 5 – CP-4, CP-6, CP-9.	Організація має політику резервного копіювання та забезпечує відновлення резервних копій, якщо це необхідно. Копії регулярно тестуються та перевіряються шляхом виконання тестів.
PR.IP-5. Правила (політика) та норми фізичної безпеки операційного середовища та обладнання організації (ОКІ) виконуються.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3; Загальні вимоги – п. 49, 50, 51; НД ТЗІ 2.5-004-99 – п. 8.1; НД ТЗІ 3.6-006-21 – PE-10, PE-12, PE-13, PE-14, PE-15, PE-18. Довідкові посилання: COBIT 5 – DSS01.04, DSS05.05; IEC 62443-2-1:2015 – 4.3.3.3.1, 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6; NIST SP 800-53 Rev. 5 – PE-10, PE-12, PE-13, PE-14, PE-15, PE-18.	Організація дотримується національної політики та правил захисту електронних комунікаційних мереж та інформаційних систем від природних катастроф, відключення електроенергії, пожежі та повені.
PR.IP-6. Дані знищуються відповідно до політики безпеки.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7; Загальні вимоги – п. 7; НД ТЗІ 3.6-006-21 – MP-6. Довідкові посилання: COBIT 5 – BAI09.03; IEC 62443-2-1:2015 – 4.3.4.4.4; IEC 62443-3-3:2016 – SR 4.2; NIST SP 800-53 Rev. 5 – MP-6.	Цифрова та фізична інформація підлягає відповідним методам знищення згідно з їх класифікацією і конфіденційністю.

1	2	3
PR.IP-7. Процеси кіберзахисту постійно вдосконалюються.	Нормативні посилання: НД ТЗІ 1.4-001-2000 – п. 8.2; НД ТЗІ 3.6-006-21 – CA-2, CA-7, CP-2, IR-8, PL-2, PM-6. Довідкові посилання: COBIT 5 – APO11.06, DSS04.05; IEC 62443-2-1:2015 – 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8; NIST SP 800-53 Rev. 5 – CA-2, CA-7, CP-2, IR-8, PL-2, PM-6.	Організація оцінює та регулярно оновлює свої процеси захисту, щоб на систематичній основі виявляти можливі існуючі вразливості задля визначення їх, як цілі у плані усунення.
PR.IP-8. Інформація про ефективність технологій захисту розподіляється	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.16.1.6; НД ТЗІ 2.3-025 -21- п. 5; НД ТЗІ 2.6-004-21 – п. 5; НД ТЗІ 3.6-004-21 – п. 6 – 8; НД ТЗІ 3.6-005-21 – п. 5; НД ТЗІ 3.6-006-21 – AC-21, CA-7, SI-4; НД ТЗІ 3.6-007-21- п. 5; НД ТЗІ 3.6-008-21 – п. 5 Довідкові посилання: COBIT 5 – BAI08.04, DSS03.04; NIST SP 800-53 Rev. 5 – AC-21, CA-7, SI-4	Організація забезпечує безперервне вдосконалення, проводить навчання та аналізує минулі кіберінциденти. Ці навчання проводяться з метою зменшення ризику виникнення подібних кіберінцидентів у майбутньому
PR.IP-9. Плани реагування (реагування на кіберінциденти та забезпечення безперервності бізнесу) і плани відновлення (відновлення після кіберінциденту та відновлення після аварії) наявні та управляються.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3; Загальні вимоги – п. 74; НД ТЗІ 1.4-001-2000 – п. Д5.8, Д.5.6.2; НД ТЗІ 3.6-006-21 – CP-2, CP-7, CP-12, CP- 13, IR-7, IR-8, IR-9, PE-17. Довідкові посилання: COBIT 5 – DSS04.03; IEC 62443-2-1:2015 – 4.3.2.5.3, 4.3.4.5.1; NIST SP 800-53 Rev. 5 – CP-2, CP-7, CP-12, CP- 13, IR-7, IR-8, IR-9, PE-17.	Плани реагування на кіберінциденти, безперервності бізнесу, обробки аварій та аварійних ситуацій регулярно оновлюються. Організація забезпечує, щоб партнери організації як внутрішні, так і зовнішні, були обізнані про оновлення.
PR.IP-10. Плани реагування та відновлення тестуються.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.17.1.3; Загальні вимоги – п.39; НД ТЗІ 3.6-006-21 – CP-4, IR-3, PM-14. Довідкові посилання: IEC 62443-2-1:2015 – 4.3.2.5.7, 4.3.4.5.11; ДСТУ EN ISO 22301:2017; IEC 62443-3-3:2016 – SR 3.3; NIST SP 800-53 Rev.4 – CP-4, IR-3,	Організація забезпечує на систематичній основі тестування та оцінку планів реагування на кіберінциденти, планів забезпечення безперервності діяльності та планів відновлення для визначення їх ефективності та можливих вразливих місць.

1	2	3
	РМ-14.	
PR.IP-11: Кібербезпека, внесена до практики роботи з персоналом (наприклад, деініціалізація, перевірка персоналу)	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – А.7.1.1; А.7.1.2, А.7.2.1, А.7.2.2, А.7.2.3; А.7.3.1, А.8.1.4; НД ТЗІ 3.6-006-21 – PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21. Довідкові посилання: CIS CSC 5, 16; COBIT 5 – APO07.01, APO07.02; APO07.03, APO07.04, APO07.05; ISA 62443-2-1:2009 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3; NIST SP 800-53 Rev. 5 – PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21.	Організаційні заходи для персоналу: відбір кандидатів, укладання контрактів, категоризація ролей і звільнення з роботи. Визначені організацією заходи оцінюються та переглядаються відповідно до встановлених вимог безпеки
PR.IP-12. План управління вразливостями розроблено й впроваджено.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – А.12.6.1, А.14.2.3, А.16.1.3, А.18.2.2, А.18.2.3; НД ТЗІ 3.6-006-21 – RA-3, RA-5, SI-2. Довідкові посилання: CIS CSC – 4, 18, 20; COBIT 5 – BAI03.10, DSS05.01, DSS05.02; NIST SP 800-53 Rev. 5 – RA-3, RA-5, SI-2.	В організації (на ОКІ) розроблено та впроваджено план управління вразливостями для електронних комунікаційних мереж та інформаційних систем, ризики, пов'язані з вразливостями враховані.

2.5. Категорія заходів кіберзахисту PR.MA – Технічне обслуговування.

Технічне обслуговування та ремонт компонентів систем управління виробничими процесами, компонентів інформаційно-комунікаційних систем виконуються з дотриманням правил та процедур безпеки.

Таблиця 11 – Заходи кіберзахисту категорії PR.MA

Заходи кіберзахисту		
Захід кіберзахисту	Нормативні та додаткові посилання	Опис
1	2	3
PR.MA-1. Технічне обслуговування та ремонт активів ОКІ виконуються та своєчасно документуються з використанням визначених та контрольованих засобів.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – А.11.1.2, А.11.2.4, А.11.2.5; Загальні вимоги – п. 10, 39; НД ТЗІ 1.4-001-2000 – п. Д5.6.5; НД ТЗІ 3.6-006-21 – MA-2, MA-3, MA-5. Довідкові посилання: COBIT 5 – BAI09.03;	Організація регулярно та за розкладом виконує технічне обслуговування своїх критичних активів. Технічне обслуговування реєструється та проводиться під наглядом уповноваженого персоналу з належними технічними знаннями.

1	2	3
	IEC 62443-2-1:2015 – 4.3.3.3.7; NIST SP 800-53 Rev. 5 – MA-2, MA-3, MA-5.	
PR.MA-2. Дистанційне обслуговування активів ОКІ схвалено, задокументовано та виконується в спосіб, що унеможливлює несанкціонований доступ.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.11.2.4, A.15.1.1, A.15.2.1; Загальні вимоги – п. 36; НД ТЗІ 3.6-006-21 – MA-4. Довідкові посилання: COBIT 5 – DSS05.04; IEC 62443-2-1:2015 – 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.4.4.6.8; NIST SP 800-53 Rev. 5 – MA-4.	Віддалене обслуговування систем і електронних комунікаційних мереж підлягає реєстрації та виконується безпечно, щоб уникнути несанкціонованого доступу.

2.6. Категорія заходів кіберзахисту PR.PT – Технології кіберзахисту.

Технічні рішення (технології) кіберзахисту управляються з метою забезпечення безпеки та стійкості систем і активів ОКІ з дотриманням політик, правил, процедур з безпеки.

Таблиця 12 – Заходи кіберзахисту категорії PR.PT

Заходи кіберзахисту		
Захід кіберзахисту	Нормативні та додаткові посилання	Опис
1	2	3
PR.PT-1. Записи аудиту (журналів подій) визначено, задокументовано, впроваджено й перевірено відповідно до політик, правил, процедур з безпеки.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1; Загальні вимоги – п. 19, 20, 21, 22, 23; НД ТЗІ 2.5-004-99 – 9.1; НД ТЗІ 3.6-006-21 – AU Клас. Довідкові посилання: COBIT 5 – APO11.04; IEC 62443-2-1:2015 - 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4; IEC 62443-3-3:2016 – SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12; NIST SP 800-53 Rev. 5 – AU Family.	Записи аудиту (журналів подій) визначаються, документуються, впроваджуються та регулярно переглядаються відповідно до політик, правил, процедур з безпеки. Забезпечено їх захист від несанкціонованого доступу та фальсифікації.
PR.PT-2. Змінні носії захищено, а їх використання обмежено відповідно до правил, процедур з безпеки.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9; Загальні вимоги – п. 38, 40, 41, 42, 43; НД ТЗІ 3.6-006-21 – MP-2, MP-3,	Організація запроваджує політики (процедури), що забезпечують застосування правил використання змінних носіїв інформації, враховуючи застосовану політику класифікації інформації.

1	2	3
	MP-4, MP- 5, MP-7, MP-8. Довідкові посилання: COBIT 5 DSS05.02, APO13.01; IEC 62443-3-3:2016 - SR 2.3; NIST SP 800-53 Rev. 5 – MP-2, MP-3, MP-4, MP- 5, MP-7, MP-8.	
PR.PT-3. Контроль доступу до систем і активів здійснюється із застосуванням принципу мінімальних привілеїв.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.9.1.2; Загальні вимоги – п. 11, 12 ,25 ,29; НД ТЗІ 2.5-004-99 – 6.1, 6.2, 9.2; НД ТЗІ 3.6-006-21 – AC-3, CM-7. Довідкові посилання: COBIT 5 – DSS05.02; IEC 62443-2-1:2015 – 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4; IEC 62443-3-3:2016 – SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7; NIST SP 800-53 Rev. 5 – AC-3, CM-7.	Організація впроваджує принцип мінімальних привілеїв, налаштовуючи системи на забезпечення лише життєво важливих послуг та функцій.
PR.PT-4. Електронні комунікаційні мережі та мережі управління захищено.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.13.1.1, A.13.2.1; Загальні вимоги – п. 24, 26 ,27, 28, 37. НД ТЗІ 2.5-004-99 – п. 6.5, 7.4; НД ТЗІ 3.6-006-21 – AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43. Довідкові посилання: COBIT 5 – DSS05.02, APO13.01; IEC 62443-3-3:2016 - SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6; NIST SP 800-53 Rev. 5 – AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-	Електронні комунікаційні мережі та мережі управління регулюють передачу інформації і шляхи, які можуть бути відкриті всередині систем і між ними. Щодо них реалізовані заходи захисту.

1	2	3
	25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43.	
PR.PT-5. Упровадження механізмів на ОКІ для досягнення вимог до стійкості у разі надзвичайних ситуацій та інцидентів у кіберпросторі.	Нормативні посилання: Загальні вимоги – п. 12, 38; НД ТЗІ 1.1-002-99 – п. 6.4; НД ТЗІ 2.5-004-99 – п. 8.2, А.3.2; НД ТЗІ 3.6-006-21– CP-7, CP-8, CP-11, CP-13, PL8, SA-14, SC-6. Довідкові посилання: ISO/IEC 27001:2013 – A.17.1.2, A.17.2.1; COBIT 5 – BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05; NIST SP 800-53 Rev. 5 – CP-7, CP-8, CP-11, CP-13, PL8, SA-14, SC-6.	Організація впроваджує необхідні механізми для забезпечення базової стійкості у всіх заздалегідь визначених функціональних станах - під навантаженням, у незвичних ситуаціях, під час відновлення, у нормальних умовах, під атакою. Правила належного розподілу додаткових ресурсів, які необхідні для досягнення стійкості, визначено.

3. Клас заходів кіберзахисту DE – Виявлення кіберінцидентів.

3.1. Категорія заходів кіберзахисту DE.AE – Аномалії та кіберінциденти.

Аномальну активність своєчасно виявлено, потенційний вплив кіберінцидентів усвідомлено.

Таблиця 13 – Підкатегорії заходів кіберзахисту категорії DE.AE

Заходи кіберзахисту		
Захід кіберзахисту	Нормативні та додаткові посилання	Опис
1	2	3
DE.AE-1. Еталони мережевих операцій та очікуваних потоків даних для користувачів і систем встановлені та управляються.	Нормативні посилання: НД ТЗІ 3.7-001-99 – п. 6.3; НД ТЗІ 3.6-006-21 – AC-4, CA-3, CM-2, SI- 4. Довідкові посилання: COBIT 5 – DSS03.01; IEC 62443-2-1:2015 – 4.4.3.3; NIST SP 800-53 Rev. 5 – AC-4, CA-3, CM-2, SI- 4.	Організація забезпечує, щоб мережеві операції здійснювалися на структурованій основі кваліфікованим персоналом і щоб були захищені цілісність, конфіденційність, доступність інформації. Для кожної інформаційної системи організація визначає, створює і підтримує довідкову модель очікуваної комунікації, незалежно від того, генерується вона користувачами або системами (як внутрішніми, так і зовнішніми).
DE.AE-2. Існує практика аналізу виявлених подій	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.16.1.1, A.16.1.4; Загальні вимоги – п.20; НД ТЗІ 3.6-006-21 – AU-6, CA-7,	Організація впроваджує практику виявлення, аналізу подій, класифікації кіберінцидентів, кібератак з метою розуміння цілей і методів

1	2	3
	IR-4, SI-4. Довідкові посилання: IEC 62443-2-1:2015 – 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8; IEC 62443-3-3:2016 – SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2; NIST SP 800-53 Rev. 5 – AU-6, CA-7, IR-4, SI-4.	атак та причин виникнення кіберінцидентів. Можуть впроваджуватися рішення, такі як SIEM, які підтримують процес виявлення, аналізу і обробки кіберінцидентів (кібератак).
DE.AE-3. Дані про події збираються та корелюються з кількох джерел та датчиків.	Нормативні посилання: НД ТЗІ 2.5-004-99 – п. 6.44; НД ТЗІ 1.4-001-2000 – п. А.1; НД ТЗІ 3.6-006-21 – AU-6, CA-7, IR-4, IR-5, IR-8, SI-4. Довідкові посилання: IEC 62443-3-3:2016 – SR 6.1; NIST SP 800-53 Rev. 5 – AU-6, CA-7, IR-4, IR-5, IR-8, SI-4.	Організація впроваджує технологічні та процесні механізми, що дозволяють збирати і зіставляти кіберінциденти, які виявляються в електронних комунікаційних мережах, інформаційних системах. Ці кіберінциденти співвідносяться між собою і по можливості збагачені додатковою аналітичною інформацією про зовнішні загрози.
DE.AE-4. Існує процес визначення можливих впливів кіберінцидентів.	Нормативні посилання: Загальні вимоги – п.4; НД ТЗІ 3.6-006-21 – CP-2, IR-4, RA-3, SI-4. Довідкові посилання: COBIT 5 – APO12.06; NIST SP 800-53 Rev. 5 – CP-2, IR-4, RA-3, SI 4.	Організація проводить класифікацію та категоризацію кіберінцидентів і оцінює їх можливий вплив на мережеві інформаційні системи (ОКІІ). Категоризація кіберінцидентів підтримує процес прийняття рішень про те, які дії виконувати для кожного типу.
DE.AE-5. Пороги оповіщення про кіберінциденти встановлено.	Нормативні посилання: Загальні вимоги – п.4; НД ТЗІ 1.4-001-2000 – п. Д1.1; НД ТЗІ 3.6-006-21 – IR-4, IR-5, IR-8. Довідкові посилання: COBIT 5 – APO12.06; IEC 62443-2-1:2015 – 4.2.3.10; NIST SP 800-53 Rev. 5 – IR-4, IR-5, IR-8.	На основі типізації та категоризації кіберінцидентів організація визначає критерії, завдяки яким приймається рішення щодо оповіщення про інцидент.

3.2. Категорія заходів кіберзахисту DE.CM – Безперервний моніторинг кібербезпеки.

Безпека інформаційних систем та активів ОКІІ відстежуються через дискретні інтервали для виявлення кіберінцидентів і перевірки ефективності заходів кібербезпеки.

Таблиця 14 – Підкатегорії заходів кіберзахисту категорії DE.CM

Заходи кіберзахисту		
Захід кіберзахисту	Нормативні та додаткові посилання	Опис
1	2	3
DE.CM-1. Електронна комунікаційна мережа (ОКІІ) відстежується для виявлення потенційних кіберінцидентів.	Нормативні посилання: Загальні вимоги – п. 4; НД ТЗІ 2.5-004-99 – п. 6.4, 9.1; НД ТЗІ 1.4-001-2000 – п. Д1.1; НД ТЗІ 3.6-006-21 – AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4. Довідкові посилання: COBIT 5 – DSS05.07; IEC 62443-3-3:2016 – SR 6.2; NIST SP 800-53 Rev. 5 – AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4.	Організація контролює свої електронні комунікаційні мережі та інформаційні системи. Процес моніторингу інтегровано в існуючий процес управління заходами кіберзахисту.
DE.CM-2. Фізичне середовище відстежується для виявлення потенційних кіберінцидентів.	Нормативні посилання: Загальні вимоги – п. 19, 28; НД ТЗІ 1.4-001-2000 – п. Д1.1; НД ТЗІ 2.5-004-99 – п. 6.4, 9.3; НД ТЗІ 3.6-006-21 – CA-7, PE-3, PE-6, PE-20. Довідкові посилання: IEC 62443-2-1:2015 – 4.3.3.3.8; NIST SP 800-53 Rev. 5 – CA-7, PE-3, PE-6, PE-20.	Компоненти об’єкта повинні забезпечити реєстрацію, збереження в електронних журналах та захист від модифікації інформації про події кібербезпеки.
DE.CM-3. Активність персоналу відстежується для виявлення потенційних кіберінцидентів.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.12.4.1; Загальні вимоги – п. 19; НД ТЗІ 1.4-001-2000 – п. Д1.1; НД ТЗІ 2.5-004-99 – п. 9.1, 9.2, 9.7, 9.8, 9.9; НД ТЗІ 3.6-006-21 – AC-2, AU-12, AU- 13, CA-7, CM-10, CM-11. Довідкові посилання: IEC 62443-3-3:2016 – SR 6.2; NIST SP 800-53 Rev. 5 – AC-2, AU-12, AU- 13, CA-7, CM-10, CM-11.	Моніторинг діяльності співробітників інтегровано в сферу управління подіями. Ця діяльність генерує достатню інформацію, що дозволяє оперативно вживати заходів у разі виникнення загрози кібербезпеці, яка виникає в результаті діяльності користувача.
DE.CM-4. Шкідливий код виявляється.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.12.2.1; Загальні вимоги – п. 24; НД ТЗІ 1.4-001-2000 – п. Д1.1; НД ТЗІ 2.5-004-99 – п. 6.4., 9.3; НД ТЗІ 3.6-006-21 – SI-3, SI-8. Довідкові посилання:	Організація впроваджує механізми, що дозволяють виявляти шкідливі коди в її електронних комунікаційних мережах та інформаційних системах (в ОКІІ). По можливості працює політика запобігання запуску таких

1	2	3
	COBIT 5 – DSS05.01; IEC 62443-2-1:2015 - 4.3.4.3.8; IEC 62443-3-3:2016 - SR 3.2; NIST SP 800-53 Rev. 5 – SI-3, SI-8.	кодів.
DE.CM-5. Несанкціонований програмний продукт виявлено.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – А.12.5.1; Загальні вимоги – п. 24; НД ТЗІ 1.4-001-2000 – п. Д1.1; НД ТЗІ 2.5-004-99 – п. 6.4; НД ТЗІ 3.6-006-21 – SC-18, SI-4, SC-44. Довідкові посилання: IEC 62443-3-3:2016 – SR 2.4; NIST SP 800-53 Rev. 5 – SC-18, SI-4, SC-44.	Організація виявляє несанкціоновані програми, що працюють у її електронних комунікаційних мережах та інформаційних системах (в ОКІІ).
DE.CM-6. Активність зовнішнього постачальника товарів і послуг відстежується з метою виявлення потенційних кіберінцидентів.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – А.14.2.7, А.15.2.1; Загальні вимоги – п. 7; НД ТЗІ 1.4-001-2000 – п. Д1.1; НД ТЗІ 3.6-006-21 – CA-7, PS-7, SA-4, SA-9, SI-4. Довідкові посилання: COBIT 5 – APO07.06; NIST SP 800-53 Rev. 5 – CA-7, PS-7, SA-4, SA-9, SI-4.	Здійснюється контроль за послугами, наданими зовнішніми постачальниками товарів і послуг, з метою виявлення несанкціонованого доступу до електронних комунікаційних мереж та інформаційних систем (ОКІІ), а також інших негативних подій кібербезпеки.
DE.CM-7. Моніторинг неавторизованого персоналу, з'єднань, пристроїв і програмного забезпечення здійснюється на постійній основі.	Нормативні посилання: Загальні вимоги – п. 19; НД ТЗІ 1.4-001-2000 – п. Д1.1; НД ТЗІ 2.5-004-99 – п. 9; НД ТЗІ 3.6-006-21 – AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4. Довідкові посилання: NIST SP 800-53 Rev. 5 – AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4.	Організація стежить за доступом співробітників до електронних комунікаційних мереж та інформаційних систем (ОКІІ), пристроїв та процесів.
DE.CM-8. Сканування вразливостей виконується	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – А.12.6.1; Загальні вимоги – п. 24; НД ТЗІ 1.4-001-2000 – п. Д1.1; НД ТЗІ 2.5-004-99 – п.9; НД ТЗІ 3.6-006-21 – RA-5. Довідкові посилання: COBIT 5 – BAI03.10; IEC 62443-2-1:2015 – 4.2.3.1, 4.2.3.7;	Організація здійснює процес управління вразливістю, в тому числі шляхом регулярного сканування вразливостей як автоматично, так і за запитом.

1	2	3
	NIST SP 800-53 Rev. 5 – RA-5.	

3.3. Категорія заходів кіберзахисту DE.DP – Процеси виявлення кіберінцидентів.

Процеси й процедури виявлення кіберінцидентів підтримуються й тестуються для забезпечення своєчасного та адекватного оповіщення про аномальні події кібербезпеки.

Таблиця 15 – Підкатегорії заходів кіберзахисту категорії DE.DP

Заходи кіберзахисту		
Захід кіберзахисту	Нормативні та додаткові посилання	Опис
1	2	3
DE.DP-1. Обов'язки щодо виявлення кіберінцидентів чітко визначено задля забезпечення звітності.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.6.1.1; Загальні вимоги – п. 8; НД ТЗІ 1.4-001-2000 – п. Д1.1; НД ТЗІ 2.5-004-99 – п. 9.4; НД ТЗІ 3.6-006-21 – CA-2, CA-7, PM-14. Довідкові посилання: COBIT 5 – DSS05.01; IEC 62443-2-1:2015 – 4.4.3.1; NIST SP 800-53 Rev. 5 – CA-2, CA-7, PM-14.	В організації визначено обов’язки щодо виявлення кіберінцидентів, забезпечується ведення звітності щодо них.
DE.DP-2. Заходи виявлення кіберінцидентів відповідають всім застосованим вимогам.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.18.1.4; НД ТЗІ 1.4-001-2000 – п. Д1.1; НД ТЗІ 3.6-006-21 – AC-25, CA-2, CA-7, SA-18, SI-4, PM-14. Довідкові посилання: IEC 62443-2-1:2015 – 4.4.3.2; NIST SP 800-53 Rev. 5 – AC-25, CA-2, CA-7, SA-18, SI-4, PM-14.	Організація проводить моніторинг ефективності заходів виявлення кіберінцидентів та зіставлення дій щодо виявлення з усіма вимогами.
DE.DP-3. Процеси виявлення кіберінцидентів протестовані.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.14.2.8; НД ТЗІ 1.4-001-2000 – п. Д1.1; НД ТЗІ 3.7-001-99 – п. 6.8; НД ТЗІ 3.6-006-21 – CA-2, CA-7, PE-3, PM-14, SI-3, SI-4 Довідкові посилання: COBIT 5 – APO13.02; IEC 62443-2-1:2015 – 4.4.3.2; IEC 62443-3-3:2016 – SR 3.3;	Організація проводить випробування і перевірку ефективності процесів виявлення за планом, та, коли: відбулася суттєва зміна системи; нові прикладні програми розробляються у значних масштабах; в існуючу інфраструктуру додано нову систему;

1	2	3
	NIST SP 800-53 Rev. 5 – CA-2, CA-7, PE-3, PM-14, SI-3, SI-4.	з'являється новий тип вразливості.
DE.DP-4. Інформацію про виявлені кіберінциденти повідомлено партнерів організації.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.16.1.2; Загальні вимоги – п. 23; НД ТЗІ 1.4-001-2000 – п. Д1.1; НД ТЗІ 3.6-006-21 – AU-6, CA-2, CA-7, RA-5, SI-4. Довідкові посилання: COBIT 5 – APO12.06; IEC 62443-2-1:2015 – 4.3.4.5.9; IEC 62443-3-3:2016 – SR 6.1; NIST SP 800-53 Rev. 5 – AU-6, CA-2, CA-7, RA-5, SI-4.	Організація розробляє комунікаційну стратегію (політику), згідно з якою забезпечує інформування партнерів організації про кіберінциденти у сфері безпеки. Стратегія (політика) підкріплюється комунікаційним планом, який може бути об'єднаний з іншими комунікаційними планами.
DE.DP-5. Процеси виявлення кіберінцидентів постійно вдосконалюються.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.16.1.6; НД ТЗІ 1.4-001-2000 – п. Д1.1; НД ТЗІ 3.6-006-21 – CA-2, CA-7, PL-2, RA-5, SI-4, PM-14. Довідкові посилання: COBIT 5 – APO11.06, DSS04.05; IEC 62443-2-1:2015 – 4.4.3.4; NIST SP 800-53 Rev. 5 – CA-2, CA-7, PL-2, RA-5, SI-4, PM-14.	Організації аналізує кіберінциденти, які відбуваються в їх електронних комунікаційних мережах та інформаційних системах (на ОКІІ), та шляхом визначення оперативних і/або процесних заходів, підвищує потенціал виявлення нових кіберінцидентів.

4. Клас заходів кіберзахисту RS – Реагування на кіберінциденти.

4.1. Категорія заходів кіберзахисту RS.RP – Планування реагування.

Процеси та процедури реагування на кіберінциденти виконуються та підтримуються з метою забезпечення своєчасного реагування на виявлені кіберінциденти.

Таблиця 16 – Підкатегорія заходів кіберзахисту категорії RS.RP

Заходи кіберзахисту		
Захід кіберзахисту	Нормативні та додаткові посилання	Опис
1	2	3
RS.RP-1. План реагування виконується під час або після події.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.16.1.5; НД ТЗІ 1.4-001-2000 – п. Д1.1; НД ТЗІ 3.6-006-21 – CP-2, CP-10, IR-4, IR-8. Довідкові посилання: COBIT 5 – BAI01.10; IEC 62443-2-1:2015 – 4.3.4.5.1;	В організації (на ОКІ) розроблено план реагування на кіберінциденти. При зборі даних щодо події та аналізі подій (кіберінцидентів) забезпечується збереженість і цілісність доказів.

1	2	3
	NIST SP 800-53 Rev. 5 – CP-2, CP-10, IR-4, IR-8.	

4.2. Категорія заходів кіберзахисту RS.CO – Комунікації.

Заходи з реагування координуються з внутрішніми та зовнішніми партнерами організації, такими як координаційні центри, постачальники електронних комунікаційних мереж та/або послуг, власники атакуючих систем, інші групи реагування на інциденти, пов'язані з інформаційною та/або кібербезпекою (CSIRT), тощо.

Таблиця 17 – Підкатегорії заходів кіберзахисту категорії RS.CO

Заходи кіберзахисту		
Захід кіберзахисту	Нормативні та додаткові посилання	Опис
1	2	3
RS.CO-1. Персонал знає свої обов'язки та порядок дій у ситуаціях, коли необхідне реагування на кіберінциденти.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.6.1.1, A.16.1.1; НД ТЗІ 1.4-001-2000 – п. 8, 9; НД ТЗІ 3.6-006-21 – CP-2, CP-3, IR-3, IR-8. Довідкові посилання: IEC 62443-2-1:2015 – 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4; NIST SP 800-53 Rev. 5 – CP-2, CP-3, IR-3, IR-8.	Під час реагування на кіберінциденти організація забезпечує, щоб усі співробітники залучалися до зазначеної роботи.
RS.CO-2. Факти про кіберінциденти задокументовано та повідомляються відповідно до встановлених критерій.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.6.1.3, A.16.1.2; Загальні вимоги – п. 19; НД ТЗІ 1.4-001-2000 – п. Д1.1; НД ТЗІ 3.6-006-21 – AU-6, IR-6, IR-8. Довідкові посилання: IEC 62443-2-1:2015 – 4.3.4.5.5; NIST SP 800-53 Rev. 5 – AU-6, IR-6, IR-8.	Організація створює і розповсюджує серед партнерів організації повідомлення про кіберінциденти та належної класифікації інцидентів з точки зору інформаційної безпеки.
RS.CO-3. Здійснюється обмін інформацією про кіберінциденти відповідно до планів реагування.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.16.1.2; Загальні вимоги – п. 7; НД ТЗІ 3.6-006-21 – CA-2, CA-7, CP-2, IR4, IR-8, PE-6, RA-5, SI-4. Довідкові посилання: IEC 62443-2-1:2015 – 4.3.4.5.2; NIST SP 800-53 Rev. 5 – CA-2, CA-7, CP-2, IR-4, IR-8, PE-6,	Організації використовує належні канали для поширення інформації про кіберінциденти у сфері безпеки серед партнерів організації. Це допоможе партнерам організації виявляти, стримувати і розв'язувати аналогічні проблеми, які можуть виникати в їх системах.

1	2	3
	RA-5, SI-4.	
RS.CO-4. Координація з партнерами організації проводиться відповідно до планів реагування.	Нормативні посилання: Загальні вимоги – п. 7; НД ТЗІ 1.4-001-2000 – п. 10.2; НД ТЗІ 3.6-006-21 – CP-2, IR-4, IR-8. Довідкові посилання: IEC 62443-2-1:2015 – 4.3.4.5.5; NIST SP 800-53 Rev. 5 – CP-2, IR-4, IR-8.	Організація виконує план координації при ескалації кіберінцидентів у сфері безпеки з урахуванням їх категоризації і важливості.
RS.CO-5. З метою досягнення ширшої ситуативної обізнаності щодо стану кібербезпеки здійснюється обмін інформацією із основними суб'єктами національної системи кібербезпеки та зовнішніми партнерами організації.	Нормативні посилання: Загальні вимоги – п. 7; НД ТЗІ 3.6-006-21 – PM-15, SI-5. Довідкові посилання: CIS CSC – 19 COBIT 5 – BAI08.04 NIST SP 800-53 Rev. 5 – PM-15, SI-5.	На етапі реагування на кіберінциденти організація визначає інформацію, якою вона буде ділитися із зовнішніми партнерами організації та основними суб'єктами національної системи кібербезпеки, для забезпечення більш широкої поінформованості про ситуацію у сфері кібербезпеки.

4.3. Категорія заходів кіберзахисту RS.AN – Аналіз.

Проводиться аналіз кіберінцидентів для забезпечення адекватних заходів реагування та підтримки відновлення.

Таблиця 18 – Підкатегорії заходів кіберзахисту категорії RS.AN

Заходи кіберзахисту		
Захід кіберзахисту	Нормативні та додаткові посилання	Опис
1	2	3
RS.AN-1. Повідомлення від систем виявлення кіберінцидентів досліджуються.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 A.12.4.1, A.12.4.3, A.16.1.5; Загальні вимоги – п. 22, 23; НД ТЗІ 3.6-006-21 – AU-6, CA-7, IR-4, IR-5, PE-6, SI-4. Довідкові посилання: COBIT 5 – DSS02.07; IEC 62443-2-1:2015 – 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8; IEC 62443-3-3:2016 – SR 6.1; NIST SP 800-53 Rev. 5 – AU-6, CA-7, IR-4, IR-5, PE-6, SI-4.	Організація забезпечує, щоб кіберінциденти, які генеруються системами виявлення, розслідувалися, класифікувалися і розглядалися послідовним чином.
RS.AN-2. Вплив	Нормативні посилання:	У процесі класифікації

1	2	3
кіберінциденту усвідомлено.	ДСТУ ISO/IEC 27001:2013 – A.16.1.6; Загальні вимоги – п. 22,23; НД ТЗІ 3.6-006-21 – CP-2, IR-4. Довідкові посилання: IEC 62443-2-1:2015 – 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8; NIST SP 800-53 Rev. 5 – CP-2, IR-4.	кіберінцидентів організація оцінює їх наслідки для своїх активів та операцій і використовує отримані результати для визначення ступеня серйозності інцидентів.
RS.AN-3. Експертиза проводиться	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.16.1.4; НД ТЗІ 3.6-006-21 – AU-7, IR-4. Довідкові посилання: COBIT 5 – APO12.06, DSS03.02, DSS05.07; ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR, 2.11, SR 2.12, SR 3.9, SR 6.1; NIST SP 800-53 Rev. 5 – AU-7, IR-4.	Організація надає необхідні ресурси для проведення експертизи під час процесу обробки кіберінциденту. Така експертиза допомагає виявити вразливості, а потім розробити способи їх пом'якшення.
RS.AN-4. Кіберінциденти класифіковано відповідно до планів реагування. Електронні докази збираються та фіксуються належним чином.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.16.1.4; НД ТЗІ 3.6-006-21 – CP-2, IR-4, IR-5, IR-8. Довідкові посилання: IEC 62443-2-1:2015 – 4.3.4.5.6; NIST SP 800-53 Rev. 5 – CP-2, IR-4, IR-5, IR-8.	Організація забезпечує, щоб класифікація кіберінцидентів проводилася відповідно плану дій у разі виявлення кіберінцидентів у сфері безпеки. Збір електронних доказів забезпечено.
RS.AN-5. Процеси для отримання, аналізу та реагування на вразливості, що розкриваються для організації з внутрішніх та зовнішніх джерел (наприклад, внутрішні тести, бюлетені з безпеки або дослідники проблем безпеки)	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.16.1.4; НД ТЗІ 3.6-006-21 – SI-5, PM-15. Довідкові посилання: COBIT 5 – APO12.06, DSS03.02, DSS05.07; ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR, 2.11, SR 2.12, SR 3.9, SR 6.1; NIST SP 800-53 Rev. 5 – SI-5, PM-15.	Організація впроваджує автоматизовані механізми з метою отримання, аналізу та реагування на вразливості. Організація проводить аналіз і перевірку інформаційних джерел, офіційних сайтів органів державної влади з метою отримання актуальної інформації щодо безпеки на національному рівні, забезпечує постійний контакт з провідними організаціями з безпеки, які мають великий досвід роботи з мінливими технологіями та загрозами.

4.4. Категорія заходів кіберзахисту RS.MI – Мінімізація наслідків.

Виконуються заходи з метою запобігання розширенню кіберінциденту,

мінімізації його наслідків та унеможливлення його повторення.

Таблиця 19 – Підкатегорії заходів кіберзахисту категорії RS.MI

Заходи кіберзахисту		
Захід кіберзахисту	Нормативні та додаткові посилання	Опис
1	2	3
RS.MI-1. Кіберінциденти стримано.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 A.16.1.5; Загальні вимоги – п. 4,7; НД ТЗІ 3.6-006-21 – IR-4. Довідкові посилання: IEC 62443-2-1:2015 – 4.3.4.5.6; IEC 62443-3-3:2016 – SR 5.1, SR 5.2, SR 5.4; NIST SP 800-53 Rev. 5 – IR-4.	Організація визначає процеси та процедури для забезпечення ефективного стримування інцидентів у сфері безпеки.
RS.MI-2. Наслідки кіберінцидентів мінімізовано.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.12.2.1, A.16.1.5; Загальні вимоги – п. 4,7; НД ТЗІ 3.6-006-21 – IR-4. Довідкові посилання: IEC 62443-2-1:2015 –4.3.4.5.6, 4.3.4.5.10; NIST SP 800-53 Rev. 5 – IR-4.	Організація визначає процеси та процедури для забезпечення ефективного пом'якшення наслідків кіберінцидентів у сфері безпеки.
RS.MI-3. Вперше виявлені вразливості усунено або задокументовано як прийняті ризики.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.12.6.1; Загальні вимоги – п.4,7; НД ТЗІ 1.4-001-2000 – п. Д4; НД ТЗІ 3.6-006-21 – CA-7, RA-3, RA-5. Довідкові посилання: NIST SP 800-53 Rev. 5 – CA-7, RA-3, RA-5.	Нововиявлені чинники уразливості оцінюються організацією з урахуванням масштабів можливих наслідків для діяльності (надання життєво важливих послуг, виконання життєво важливих функцій), визначених у процесі управління вразливістю. Організація визначає, яких заходів слід вжити у зв'язку з цими факторами вразливості зважаючи на політику управління ризиками.

4.5. Категорія заходів кіберзахисту RS.IM – Удосконалення.

Заходи з реагування вдосконалюються шляхом урахування досвіду з поточних або виконаних заходів виявлення/реагування.

Таблиця 20 – Підкатегорії заходів кіберзахисту категорії RS.IM

Заходи кіберзахисту		
Захід кіберзахисту	Нормативні та додаткові посилання	Опис
1	2	3
RS.IM-1. У планах реагування враховано отриманий досвід.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 –A.16.1.6; Загальні вимоги – п. 4; НД ТЗІ 1.4-001-2000 – п. Д5.6.5; НД ТЗІ 3.6-006-21 – CP-2, IR-4, IR-8. Довідкові посилання: COBIT 5 – BAI01.13; IEC 62443-2-1:2015 – 4.3.4.5.10, 4.4.3.4; NIST SP 800-53 Rev. 5 – CP-2, IR-4, IR-8.	Організація вивчає минулі кіберінциденти після того, як вони будуть врегульовані для того, щоб врахувати отриманий досвід. Аналізується вся інформація, яка відома про кіберінцидент, визначивши, що добре спрацювало і що необхідно покращити у процесі розгляду кіберінцидентів для того, щоб організація і її системи були більш стійкими до майбутніх інцидентів.
RS.IM-2. Плани реагування оновлено.	Нормативні посилання: Загальні вимоги – п. 4; НД ТЗІ 1.4-001-2000 – п. Д5.6.5; НД ТЗІ 3.6-006-21 – CP-2, IR-4, IR-8. Довідкові посилання: NIST SP 800-53 Rev. 5 – CP-2, IR-4, IR-8.	Плани реагування оновлюються з урахуванням внутрішніх змін після врегулювання кіберінцидентів.

5. Клас заходів кіберзахисту RC – Відновлення стану кібербезпеки.

5.1. Категорія заходів кіберзахисту RC.RP – Планування відновлення.

Процеси та процедури відновлення виконуються та підтримуються з метою своєчасного відновлення систем або активів, постраждалих від кіберінцидентів.

Таблиця 21 – Підкатегорії заходів кіберзахисту категорії RC.RP

Заходи кіберзахисту		
Захід кіберзахисту	Нормативні та додаткові посилання	Опис
1	2	3
RC.RP-1. План відновлення виконується під час або після кіберінцидентів.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.16.1.5; Загальні вимоги – п. 4; НД ТЗІ 1.4-001-2000 – п. Д5.6.5; НД ТЗІ 2.5-004-99 - п. 8.3, 8.4; НД ТЗІ 3.6-006-21 – CP-10, IR-4, IR-8. Довідкові посилання: COBIT 5 – DSS02.05, DSS03.04; NIST SP 800-53 Rev. 5 – CP-10,	Організація розробляє свій план ліквідації наслідків кіберінцидентів, для того щоб забезпечити належний розподіл ресурсів (людських і технічних) для врегулювання інцидентів. Процес ліквідації наслідків кіберінцидентів, забезпечує збереження і наявність активів, необхідних для проведення найважливіших видів діяльності.

1	2	3
	IR-4, IR-8.	

5.2. Категорія заходів кіберзахисту RC.IM – Удосконалення.

Процеси й планування відновлення удосконалюються шляхом урахування отриманого досвіду для реалізації майбутніх заходів.

Таблиця 22 – Підкатегорії заходів кіберзахисту категорії RC.RP

Заходи кіберзахисту		
Захід кіберзахисту	Нормативні та додаткові посилання	Опис
1	2	3
RC.IM-1. Плани відновлення враховують отриманий досвід.	Нормативні посилання: IEC 62443-2-1:2015 - 4.4.3.4; Загальні вимоги – п. 4; НД ТЗІ 1.4-001-2000 – п. Д5.6.5; НД ТЗІ 3.6-006-21 – CP-2, IR-4, IR-8. Довідкові посилання: COBIT 5 – BAI05.07; NIST SP 800-53 Rev. 5 – CP-2, IR-4, IR-8.	Організація забезпечує, щоб плани відновлення оновлювалися з урахуванням заходів, прийнятих на основі накопиченого досвіду.
RC.IM-2. Плани відновлення оновлено.	Нормативні посилання: Загальні вимоги – п. 4; НД ТЗІ 3.6-006-21 – CP-2, IR-4, IR-8. Довідкові посилання: COBIT 5 – BAI07.08; NIST SP 800-53 Rev. 5 – CP-2, IR-4, IR-8.	Плани відновлення у разі виникнення інцидентів оновлюються з урахуванням внутрішніх змін.

5.3. Категорія заходів кіберзахисту RC.CO – Комунікації.

Заходи з відновлення координуються з внутрішніми та зовнішніми партнерами організації, такими як координаційні центри, постачальники електронних комунікаційних мереж та/або послуг, власники атакуючих систем, інші групи реагування на інциденти, пов'язані з інформаційною та/або кібербезпекою (CSIRT), тощо.

Таблиця 23 – Підкатегорії заходів кіберзахисту категорії RC.CO

Заходи кіберзахисту		
Захід кіберзахисту	Нормативні та додаткові посилання	Опис
1	2	3
RC.CO-1. Процес зв'язків з громадськістю організовано та є керованим.	Нормативні посилання: Загальні вимоги – п. 7. Довідкові посилання: COBIT 5 – EDM03.02.	Організація повідомляє про те, що є актуальним у контексті кібербезпеки. Інформаційний надається організацією таким чином, щоб звести до мінімуму потенційний вплив на репутацію та довіру.

1	2	3
RC.CO-2. Репутацію після кіберінцидентів відновлюється.	Нормативні посилання: Загальні вимоги – п. 7. Довідкові посилання: COBIT 5 – MEA03.02.	Організація оглядає і коригує політику, принципи, стандарти, процедури і методологію для забезпечення безпечного функціонування електронних комунікаційних мереж та інформаційних систем на ОКІ. Одночасно робляться кроки на відновлення репутації.
RC.CO-3. Заходи з відновлення повідомлено внутрішнім та зовнішнім партнерам організації, а також керівництву.	Нормативні посилання: Загальні вимоги – п. 7; НД ТЗІ 3.6-006-21 – CP-2, IR-4. Довідкові посилання: NIST SP 800-53 Rev. 5 – CP-2, IR-4.	Організація забезпечує інформування внутрішніх і зовнішніх партнерів організації про серйозні кіберінциденти.

Директор Департаменту кіберзахисту
Адміністрації Держспецзв'язку
полковник Данило МЯЛКОВСЬКИЙ

Додаток 2
до Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури (пункт 4 розділу VII)

Методичні рекомендації щодо розробки поточного профілю кіберзахисту

Поточний профіль кіберзахисту розробляється з використанням класифікації заходів кіберзахисту. Розробку поточного профілю кіберзахисту ОКІІ може здійснювати особа, відповідальна за впровадження заходів захисту інформації на ОКІ. Профіль кіберзахисту рекомендується розробляти для кожного ОКІІ окремо.

Розробка поточного профілю кіберзахисту має на меті зіставлення вимог Рекомендацій з практикою захисту інформації, що впроваджена на ОКІ. В цьому випадку можна розглядати три типи організації.

Організація першого типу (далі – Організація 1) реалізує підхід із захисту інформації, що базується на власній практиці із захисту інформації.

Організація другого типу (далі – Організація 2) організація, яка будувала систему захисту інформації на основі вимог міжнародних, національних або галузевих стандартів.

Організація третього типу (далі – Організація 3) – заходи захисту взагалі не реалізовані.

Поточна практика захисту інформації, що наведена у таблиці, є узагальнюючою та призначена для ілюстрації концепції зіставлення. Рівень специфічності та деталізації необхідний для того, щоб профіль був корисним та унікальним для кожної організації.

Таблиця – Приклади поточного профілю кіберзахисту ОКІІ

Функція кібербезпеки	Категорія заходів кіберзахисту	Заходи кіберзахисту	Профіль кіберзахисту
			Поточна практика захисту інформації
1	2	3	4
Організація 1 Підхід на основі власних заходів захисту			
Кіберзахист (PR)	Управління ідентифікацією, автентифікацією та контроль доступу (PR.AC)	PR.AC-3: здійснюється контроль віддаленого доступу	Комутований доступ для здійснення технічного обслуговування персоналом постачальника надається у разі потреби та відключається, коли таке обслуговування завершується. Віддалений доступ дозволено лише через VPN. Діяльність під час надання віддаленого доступу записується та контролюється.

1	2	3	4
			Доступ до VPN надається виключно для визначених організацією пристроїв. Усі спроби несанкціонованого підключення до VPN реєструються. У разі звільнення працівника негайно скасовується його VPN-акаунт. Рівень упровадження – другий рівень – ризик-орієнтований.
Організація 2 Підхід, що базується на використанні вимог стандарту			
Кіберзахист (PR)	Управління ідентифікацією, автентифікацією та контроль доступу (PR.AC)	PR.AC-3: здійснюється контроль віддаленого доступу	У разі реалізованої СУІБ відповідно до ДСТУ ISO/IEC 27001. Контроль віддаленого доступу здійснюється відповідно до вимог ДСТУ ISO/IEC 27001: A.6.2.1 ; A.6.2.2 ; A.11.2.6; A.13.1.1; A.13.2.1. Рівень упровадження – другий рівень – ризик-орієнтований.
			У разі побудованої КСЗІ. Контроль віддаленого доступу реалізовано відповідно до вимог НД ТЗІ 2.5-004-99: ДР-2, ДС-1, НР-2, НИ-2, НО-2, НЦ-1, НТ- 2, НВ-1. Рівень гарантій – Г2. Рівень упровадження – третій рівень – повторюваний.
			У разі побудованої системи захисту інформації на основі галузевих стандартів. Система захисту інформації побудована відповідно до вимог міжнародного стандарту IEC 62443: IEC 62443-2-1:2015: 4.3.3.6.6. IEC 62443-3-3:2016: SR 1.13; SR 2.6. Рівень упровадження – другий рівень – ризик-орієнтований.

1	2	3	4
Організація 3 Підхід до опису відсутності заходів захисту			
Кіберзахист (PR)	Управління ідентифікацією, автентифікацією та контроль доступу (PR.AC)	PR.AC-3: здійснюється контроль віддаленого доступу	Не застосовується – віддалений доступ заборонено для активів і систем, що входять у сферу діяльності організації. Заходи кіберзахисту не впроваджувалися.

Додаток 3
до Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури (пункт 4 розділу VII)

Методичні рекомендації щодо розробки цільового профілю кіберзахисту

Створюючи цільовий профіль кіберзахисту, організація враховує:
вимоги нормативно-правових актів та нормативних документів;
сучасні практики захисту інформації;
сучасні практики управління ризиками;
поточне середовище ризику;
цілі діяльності та завдання;
організаційні обмеження.

У таблиці наведено приклад гіпотетичного цільового профілю кіберзахисту для конкретного результату заходів кіберзахисту підкатегорії (PR.AC-3) для трьох організацій, що використовують три різні підходи.

Організація 1 визначила, що чинна практика захисту, яку вона використовує для управління віддаленим доступом, є недостатньою для опрацювання ризиків кібербезпеки, тому потрібно впровадити додаткові заходи кіберзахисту. Організація 2 доходить до такого самого висновку та визначає додаткові вимоги стандартів безпеки, які хотіла б впровадити у себе. Організація 3 демонструє, що поточний профіль є ідентичним цільовому профілю кіберзахисту для визначених заходів кіберзахисту. Такі випадки відбудуться тоді, коли стандарти, інструменти, методи, що реалізуються організацією, достатньою мірою відповідають її вимогам кібербезпеки та управління ризиками.

Однак таке узгодження поточного профілю та цільового профілю кіберзахисту може тривати тільки протягом короткого періоду часу, оскільки вимоги організації до кібербезпеки та управління ризиками будуть розвиватися в міру її розвитку та виникнення нових ризиків. Наприклад, організація може визначити, що поточна практика більше не потрібна або недостатня, та виключити її з цільового профілю кіберзахисту.

При розробці цільового профілю кіберзахисту організації можуть використати ширший підхід – з урахуванням більш ефективних і дієвих підходів до управління ризиками у всій організації.

Окрім цільового профілю кіберзахисту, організація вибирає цільовий рівень упровадження заходів кіберзахисту, який застосовується до процесу управління ризиками в межах сфери своєї діяльності. Організація самостійно вибирає прийнятний для неї рівень («бажаний» стан) та визначає заходи кіберзахисту та заходи щодо управління ризиками, необхідні для досягнення цієї мети.

Використовуючи стандарти, інструменти, методи щодо управління кібербезпекою, організація відображає бажані результати у цільовому профілі кіберзахисту та цільовому рівні реалізації.

Таблиця – Приклади цільового профілю кіберзахисту ОКІІ

Функція кібербезпеки	Категорія заходів кіберзахисту	Заходи кіберзахисту	Профілі кіберзахисту	
			Поточний профіль кіберзахисту – поточна практика захисту інформації	Цільовий профіль кіберзахисту
1	2	3	4	5
Організація 1 Підхід на основі власних заходів захисту				
Кіберзахист (PR)	Управління ідентифікацією, автентифікацією та контроль доступу (PR.AC)	PR.AC-3: здійснюється контроль віддаленого доступу	Комутований доступ для здійснення технічного обслуговування персоналом постачальника надається у разі потреби та відключається, коли таке обслуговування завершується. Віддалений доступ дозволено лише через VPN. Діяльність під час надання віддаленого доступу записується та контролюється. Доступ до VPN надається виключно для визначених організацією пристроїв. Усі спроби несанкціонованого підключення до VPN реєструються. У разі звільнення працівника негайно скасовується його	Комутований доступ для здійснення технічного обслуговування персоналом постачальника надається у разі потреби та відключається, коли таке обслуговування завершується. Віддалений доступ дозволено лише через VPN. Діяльність під час надання віддаленого доступу записується та контролюється. Доступ до VPN надається виключно для визначених організацією пристроїв. Усі спроби несанкціонованого підключення до VPN реєструються. У разі звільнення працівника негайно скасовується його VPN-акаунт. Огляд авторизованого списку облікових записів VPN рекомендується здійснювати двічі на

Продовження додатка 3

1	2	3	4	5
			VPN-акаунт. Рівень упровадження – другий рівень – ризик-орієнтований.	рік.* Цільовий рівень упровадження – другий рівень – ризик-орієнтований.
Організація 2 Підхід, що базується на використанні вимог стандарту				
Кіберзахист (PR)	Управління ідентифікацією, автентифікацією та контроль доступу (PR.AC)	PR.AC-3: здійснюється контроль віддаленого доступу	У разі реалізованої СУІБ відповідно до ДСТУ ISO/IEC 27001. Контроль віддаленого доступу здійснюється відповідно до вимог ДСТУ ISO/IEC 27001: A.6.2.1; A.6.2.2; A.11.2.; A.13.1.1; A.13.2.1. Рівень упровадження – другий рівень – ризик-орієнтований.	У разі реалізованої СУІБ відповідно до ДСТУ ISO/IEC 27001. Контроль віддаленого доступу рекомендується здійснювати відповідно до вимог ДСТУ ISO/IEC 27001: A.6.2.; A.6.2.; A.11.2.6; A.13.1.1; A.13.2.1. A.13.2.2;* A.13.2.3;* A.13.2.4;* A.14.2.8;* A.15*. Рівень впровадження – третій рівень – повторюваний.
			У разі побудованої КСЗІ. Контроль віддаленого доступу реалізовано відповідно до вимог НД ТЗІ 2.5-004-99: ДР-2, ДС-1, НР-2, НИ-2, НО-2, НЦ-1, НТ-2, НВ-1. Рівень гарантій – Г2. Рівень упровадження – третій рівень – повторюваний.	У разі побудованої КСЗІ. Контроль віддаленого доступу рекомендується реалізовувати відповідно до вимог НД ТЗІ 2.5-004-99: ДР-3,* ДС-1, ДЗ-1;* НР-2, НИ-2, НК-1;* НО-2, НЦ-2, НТ-2,* НВ-1. Рівень гарантій – Г3. Цільовий рівень упровадження – третій рівень – повторюваний.

Продовження додатка 3

1	2	3	4	5
			У разі побудованої системи захисту інформації на основі галузевих стандартів. Контроль віддаленого доступу реалізовано відповідно до вимог міжнародного стандарту: IEC 62443-2-1:2015: 4.3.3.6.6. IEC 62443-3-3:2016: SR 1.13; SR 2.6. Рівень упровадження – другий рівень – ризик-орієнтований.	У разі побудованої системи захисту інформації на основі галузевих стандартів. Контроль віддаленого доступу рекомендується реалізовувати відповідно до вимог міжнародного стандарту: IEC 62443-2-1:2015: 4.3.3.6.4* 4.3.3.6.6. 4.3.3.6.7* IEC 62443-3-3:2016: SR 1.13; SR 2.6; SR 1.13 (1).* Цільовий рівень упровадження – другий рівень – ризик-орієнтований.
Організація 3 Підхід до опису відсутності заходів захисту				
Кіберзахист (PR)	Управління ідентифікацією, автентифікацією та контроль доступу (PR.AC)	PR.AC-3: здійснюється контроль віддаленого доступу	Не застосовується – віддалений доступ заборонено для активів і систем, що входять у сферу діяльності організації.	Не застосовується – віддалений доступ заборонено для активів і систем, що входять у сферу діяльності організації.

Примітка

* Організація визначила необхідність впровадження додаткових практик, які вона хоче впровадити для успішного досягнення результату на основі аналізу поточного середовища ризику, цілей і завдань діяльності у сфері надання основних послуг.

Продовження додатка 4
до Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури (пункт 1 розділу VIII)

Методичні рекомендації щодо аналізу поточного та цільового профілю кіберзахисту

На етапі визначення, аналізу та пріоритизації недоліків організація оцінює свій поточний профіль кіберзахисту і рівень його впровадження порівняно з цільовим профілем кіберзахисту і цільовим рівнем впровадження та виявляє будь-які потенційні ризики.

Під час здійснення порівняння виникає розрив у вимогах, тобто в цільовому профілі кіберзахисту на рівні цільового впровадження є бажаний результат для категорії або підкатегорії заходів кіберзахисту, який у цей час не відповідає чинним підходам із забезпечення кібербезпеки та управління ризиками.

Після виявлення розривів як у профілі, так і на рівні впровадження організація вивчає потенційні наслідки нездатності розв’язати такі проблеми. На цьому етапі організації рекомендується визначити пріоритет усунення виявлених розривів. Пріоритизація розривів повинна здійснюватися на основі вивчення вимог нормативно-правових актів та нормативних документів, чинних практик управління ризиками, поточного середовища ризику безпеки, цілей діяльності, а також будь-яких інших організаційних обмежень або міркувань.

Як тільки кожному розриву присвоюється пріоритет усунення, організація визначає потенційні зусилля щодо усунення розриву і виконує аналіз витрат та вигод для кожного варіанта. Колонка «Розрив» у Таблиці наводить додаткові вимоги, які організація може вибрати задля усунення розриву.

Таблиця – Аналіз поточного та цільового профілю кіберзахисту ОКІІ

Функція кібер-безпеки	Категорія заходів кібер-захисту	Заходи кіберзахисту	Профілі кіберзахисту		
			Поточний профіль кіберзахисту - поточна практика захисту інформації	Цільовий профіль кіберзахисту	Розрив
1	2	3	4	5	6
Організація 1 Підхід на основі власних заходів захисту					
Кібер-захист (PR)	Управління ідентифікацією, автентифікацією та контроль	PR.AC-3: здійснюється контроль віддаленого доступу	Комутований доступ для здійснення технічного обслуговування персоналом постачальника	Комутований доступ для здійснення технічного обслуговування персоналом постачальника	Додаткові вимоги: огляд авторизо-ваного списку

1	2	3	4	5	6
	доступу (PR.AC)		надається у разі потреби та відключається, коли таке обслуговування завершується. Віддалений доступ дозволено лише через VPN. Діяльність під час надання віддаленого доступу записується та контролюється. Доступ до VPN надається виключно для визначених організацією пристроїв. Усі спроби несанкціонованого підключення до VPN реєструються. У разі звільнення працівника негайно скасовується його VPN-акаунт. Рівень упровадження – другий рівень – ризик-орієнтований.	надається у разі потреби та відключається, коли таке обслуговування завершується. Віддалений доступ дозволено лише через VPN. Діяльність під час надання віддаленого доступу записується та контролюється. Доступ до VPN надається виключно для визначених організацією пристроїв. Усі спроби несанкціонованого підключення до VPN реєструються. У разі звільнення працівника негайно скасовується його VPN-акаунт. Огляд авторизованого списку облікових записів VPN рекомендується здійснювати двічі на рік. Цільовий рівень упровадження – другий рівень – ризик-орієнтований.	облікових записів VPN може здійснюватися двічі на рік.

1	2	3	4	5	6
Організація 2 Підхід, що базується на використанні вимог стандарту					
Кібер-захист (PR)	Управління іденти-фікацією, автенти-фікацією та контроль доступу (PR.AC)	PR.AC-3: здійснюється контроль віддаленого доступу	У разі реалізованої СУІБ відповідно до ДСТУ ISO/IEC 27001. Контроль віддаленого доступу здійснюється відповідно до вимог ДСТУ ISO/IEC 27001: A.6.2.1; A.6.2.2; A.11.2.6; A.13.1.1; A.13.2.1. Рівень впровадження – другий рівень – ризик-орієнтований.	У разі реалізованої СУІБ відповідно до ДСТУ ISO/IEC 27001. Контроль віддаленого доступу рекомендується здійснювати відповідно до вимог ДСТУ ISO/IEC 27001: A.6.2.1; A.6.2.2; A.11.2.6; A.13.1.1; A.13.2.1; A.13.2.2; A.13.2.3; A.13.2.4; A.14.2.8; A.15.1. Цільовий рівень впровадження – третій рівень – повторюваний.	Додаткові вимоги: ДСТУ ISO/IEC 27001: A.13.2.2; A.13.2.3; A.13.2.4; A.14.2.8; A.15.1. Цільовий рівень впровадж-ня – третій рівень – повторю-ваний
			У разі побудованої КСЗІ. Контроль віддаленого доступу реалізовано відповідно до вимог НД ТЗІ 2.5-004-99: ДР-2, ДС-1, НР-2, НИ-2, НО-2, НЦ-1, НТ-2, НВ-1. Рівень гарантій – Г2. Рівень впровадження – третій рівень – повторюваний.	У разі побудованої КСЗІ. Контроль віддаленого доступу рекомендується реалізовувати відповідно до вимог НД ТЗІ 2.5-004-99: ДР-3, ДС-1, ДЗ-1; НР-2, НИ-2, НК-1; НО-2, НЦ-2, НТ-2, НВ-1. Рівень гарантій – Г3.	Додаткові вимоги: ДР-3, ДЗ-1, НК-1, НЦ-2. Рівень гарантій – Г3.

1	2	3	4	5	6
				Цільовий рівень впровадження – третій рівень – повторюваний	
			У разі побудованої системи захисту на основі галузевих стандартів. Контроль віддаленого доступу реалізовано відповідно до вимог міжнародного стандарту: IEC 62443-2-1:2015: 4.3.3.6.6. IEC 62443-3-3:2016: SR 1.13; SR 2.6. Рівень впровадження – другий рівень – ризик-орієнтований.	У разі побудованої системи захисту на основі галузевих стандартів. Контроль віддаленого доступу рекомендується реалізовувати відповідно до вимог міжнародного стандарту: IEC 62443-2-1:2015: 4.3.3.6.4; 4.3.3.6.6; 4.3.3.6.7. IEC 62443-3-3:2016: SR 1.13; SR 2.6; SR 1.13 (1). Цільовий рівень впровадження – другий рівень – ризик-орієнтований.	Додаткові вимоги: IEC 62443-2-1:2015: 4.3.3.6.4; 4.3.3.6.7 IEC 62443-3-3:2016: SR 1.13 (1).
Організація 3 Підхід до опису відсутності заходів захисту					
Кібер-захист (PR)	Управління ідентифікацією, автентифікацією та контроль доступу (PR.AC)	PR.AC-3: здійснюється контроль віддаленого доступу	Не застосовується – віддалений доступ заборонено для активів і систем, що входять у сферу діяльності організації.	Не застосовується - віддалений доступ заборонено для активів і систем, що входять у сферу діяльності організації.	Немає