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 12 жовтня 2021 року № 616)

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 3.7-001-99 – 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.	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	Нормативні посилання:	Програмне забезпечення, що використовуються для

Продовження додатка 1

1	2	3
використовуються ОКІ для надання життєво важливих послуг та функцій, ідентифіковано та задокументовано.	ДСТУ ISO/IEC 27001:2013 А.8.1.1, А.8.1.2; 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 3.7-001-99 – 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.	забезпечення роботи ОКІІ ОКІ, які забезпечують надання життєво важливих послуг та виконання життєво важливих функцій, повинні бути ідентифіковані та задокументовані.
ID.AM-3. Телекомунікації та потоки даних ОКІ ідентифіковано та задокументовано.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – А.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 3.7-001-99 – 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 телекомунікацій 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 телекомунікаційну інфраструктуру та існуючі потоки даних.
ID.AM-4. Зовнішні інформаційні та інформаційно-телекомунікаційні системи, промислові системи, які взаємодіють з інформаційно-телекомунікаційними	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – А.11.2.6; Загальні вимоги – пп. 5, 7, 52; НД ТЗІ 2.5-004-99 – п. 9.7; 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;	Інформаційні та інформаційно-телекомунікаційні системи, які взаємодіють з ОКІІ ОКІ (в тому числі, які розташовані, або можуть використовуватись за межами ОКІ), слід віднести до певного каталогу. Необхідно забезпечити безпечну роботу обладнання, яке може санкціоновано

Продовження додатка 1

1	2	3
та іншими системами ОКІ обліковано.	NIST SP 800-53 Rev. 5 – AC-20, SA-9.	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 – А.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 3.7-001-99 – 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.	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 – А.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 3.7-001-99 – 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 – A.15.1.3, A.15.2.1, A.15.2.2; Загальні вимоги – п. 7. 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. 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 визначити ідентифікувати та категорізувати власні ОКІІ.
ID.BE-3. Пріоритетність цілей, завдань і заходів щодо забезпечення кібербезпеки надання життєво важливих послуг та функцій встановлено та повідомлено.	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. 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.	На ОКІ визначаються пріоритети цілей, завдань і заходів щодо забезпечення кібербезпеки ОКІІ, що забезпечують надання життєво важливих послуг та 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 3.7-001-99 – п. 6.3; НД ТЗІ 3.7-003-05 – п. 6.1.3.	Організація забезпечує ідентифікацію та реєстрацію критично важливих активів, необхідних для надання життєво важливих послуг та функцій.

1	2	3
	Довідкові посилання: NIST SP 800-53 Rev. 5 – CP-8, PE-9, PE-11, PM-8, SA-14.	Реєстрація містить принаймні таку інформацію: телекомунікаційні 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; телекомунікаційні мережі, які підтримують важливі послуги та потребують захисту від фальсифікації та перехоплення; планування потенціалу та моніторинг телекомунікаційних 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 3.7-003-05 – п. 6.1.3. Довідкові посилання: COBIT 5 – DSS04.02; NIST SP 800-53 Rev. 5 – CP-2, CP-11, SA-14.	Організація ідентифікує та визначає відповідні вимоги для забезпечення стійкості надання критично важливих послуг та функцій.

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)	Нормативні посилання:	Організація: визначає політику інформаціної/

Продовження додатка 1

1	2	3
кібербезпеки ОКІ встановлено та задокументовано.	ДСТУ ISO/IEC 27001:2013 – А.5.1.1; Загальні вимоги – пп. 1, 2, 4, 7, 8; НД ТЗІ 1.4-001-2000 – п. Д5; НД ТЗІ 2.5-004-99 – п. 6, 7, 8, 9; НД ТЗІ 3.7-001-99 – п. 6.4.1; НД ТЗІ 1.1-002-99 – п. 6.2; 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.	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 1.4-001-2000 – п. 6; НД ТЗІ 2.5-004-99 – п. 9.4; НД ТЗІ 3.7-001-99 – п. 6.4.1; НД ТЗІ 1.1-002-99 – п. 7.2.4. Довідкові посилання: COBIT 5 – APO13.12; IEC 62443-2-1:2015 – 4.3.2.3.3; NIST SP 800-53 Rev. 5 – PM-1, 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 політики та процедур організації всім персоналом. ОКІ може взаємодіяти з державними органами, установами та підприємствами, 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	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 3.7-001-99 – п. 6.4.1.	Організація узагальнює та виконує нормативно-правові та нормативні вимоги щодо кібербезпеки, дотримуючись національних та європейських норм, в тому числі

Продовження додатка 1

1	2	3
захисту недоторканості особистого життя (приватності), усвідомлено та управління ними здійснюється.	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 (окрім PM-1).	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 3.7-001-99 – 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-9, PM-11.	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 1.4-001-2000 – п. Д1.2, Д4, Д5.6.2.4; НД ТЗІ 1.1-002-99 – п. 6.1, 6.5. 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;	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.

Продовження додатка 1

1	2	3
	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.	
ID.RA-2. Інформацію про загрози безпеки та вразливості отримано з форумів обміну інформацією та офіційних джерел.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – А.6.1.4; Загальні вимоги – п. 5, 6. 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 обновлюваної 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 задокументовано.	Нормативні посилання: Загальні вимоги – п. 4, 5; НД ТЗІ 1.4-001-2000 – п. Д4.2.3, Д4.3, Д4.4; НД ТЗІ 1.1-002-99 – п. 6.1, 6.4, 6.5; 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.	Відповідно до стратегії (політики) управління ризиками організація визначає та задокументує можливі загрози, які 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 1.4-001-2000 – п. Д5.6.2.4; НД ТЗІ 1.1-002-99 – п. 6.1, 6.5; 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	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – А.12.6.1; Загальні вимоги – п. 4, 5; НД ТЗІ 1.4-001-2000 – п. Д5.6.2;	Організація визначає у методології управління ризиками, які є критерії для визначення ймовірності та впливу ризику. Ці критерії

1	2	3
ймовірностей та рівня шкоди використано для визначення ризику кібербезпеки.	НД ТЗІ 1.1-002-99 – п. 6.1 6.5; 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.	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. 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. 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

Продовження додатка 1

1	2	3
		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. 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 відповідному сектору критичної інфраструктури.	Нормативні посилання: Загальні вимоги – п. 4, 5; НД ТЗІ 1.4-001-2000 – п. Д4. 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.

1.6. 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. 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)	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.15.2.1, A.15.2.2;	Постачальники товарів і послуг для ОКІ ідентифікується.

Продовження додатка 1

1	2	3
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.	Загальні вимоги – п. 4, 5; НД ТЗІ 1.4-001-2000 – п. Д7.1. 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.	Організація класифікує своїх постачальників за: доступом до конфіденційної інформації; можливим впливом на ланцюг поставок; товарами і послугами, що надаються.
ID.SC-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.	Нормативні посилання: 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. 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.	У випадку укладення 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. З постачальниками здійснюється планування та тестування реагування за відповідними політиками реагування на кіберінциденти та відновлення стану кібербезпеки.	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. Довідкові посилання: 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.	Організація визначає, які постачальники братимуть участь у опрацюванні заходів реагування та планах відновлення, щоб забезпечити їх участь у запланованих навчаннях з 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 1.4-001-2000 – п. Д5.7; НД ТЗІ 2.5-004-99 – п.8.1; НД ТЗІ 3.7-001-99 – п. 6.4.1; НД ТЗІ 1.1-002-99 – п. 7.2, 7.2.2. 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 Family.	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 захищений та управляється.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – 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 1.4-001-2000 – п. Д5.7; НД ТЗІ 3.7-001-99 – п. 6.4.1; НД ТЗІ 1.1-002-99 – п. 7.2, 7.2.2, 7.2.3. Довідкові посилання: COBIT 5 – DSS01.04, DSS05.05; IEC 62443-2-1:2015 - 4.3.3.3.2,	Організація охороняє та керує фізичним доступом до своїх об'єктів та інфраструктури, що підтримують її телекомунікаційні 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 телекомунікаційні мережі або інформаційні системи.

Продовження додатка 1

1	2	3
	4.3.3.3.8; NIST SP 800-53 Rev. 5 – PE-2, PE-3, PE-4, PE5, PE-6, PE-9.	
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 1.4-001-2000 – п. Д5.7; НД ТЗІ 2.5-004-99 – п. 8.1, 9.8; НД ТЗІ 1.1-002-99 – п. 7.2, 7.2.2, 7.2.3; 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 телекомунікаційних мереж та інформаційних систем. Віддалений доступ включає всі види доступу до мережевих або інформаційних систем через зовнішні телекомунікаційні 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 1.4-001-2000 – п. Д5.7; НД ТЗІ 2.5-004-99 – п.8.1; НД ТЗІ 1.1-002-99 – п. 7.2, 7.2.2, 7.2.3. 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.	Доступ надається на основі принципів мінімальних привілеїв і поділу обов'язків. Принципи мінімальних привілеїв свідчать, що доступ до телекомунікаційних 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 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 телекомунікаційної	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 –	Цілісність телекомунікаційної мережі захищена за допомогою

Продовження додатка 1

1	2	3
мережі захищено (наприклад, сегментація мережі).	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 3.7-001-99 – 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.	поділу і сегментації мережі. Проєктування телекомунікаційної 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. 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 3.7-001-99 – 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.

Продовження додатка 1

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 обізнані та пройшли підготовку з питань кібербезпеки.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – А.7.2.2; Загальні вимоги – п. 1, 2, 9; НД ТЗІ 1.4-001-2000 – п. 8.3; НД ТЗІ 1.1-002-99 – п. 7.2.4. Довідкові посилання: COBIT 5 – APO07.03, BAI05.07; IEC 62443-2-1:2015 – 4.3.2.4.2; NIST SP 800-53 Rev. 5 – AT-2, PM-13.	Організація формує план дій для навчання працівників з питань 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. 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 – AT-3, PM-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. 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.	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. Довідкові посилання: IEC 62443-2-1:2015 – 4.3.2.4.2; COBIT 5 – APO07.03; NIST SP 800-53 Rev. 5 – AT-3, PM-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 назначаються всі обов’язки, пов’язані із забезпеченням

1	2	3
фізичної та інформаційної безпеки розуміє свої обов'язки.	А.6.1.1, А.7.2.2; Загальні вимоги – п. 2; НД ТЗІ 2.5-004-99 – п. 9.4. 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 здійснюється підвищення кваліфікації та 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 – А.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. 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 –SC-28.	В телекомунікаційних 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 – А.8.2.3, А.13.1.1, А.13.2.1, А.13.2.3, А.14.1.2, А.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 3.7-001-99 – п. 6.4.2. Довідкові посилання: COBIT 5 – APO01.06, DSS06.06; IEC 62443-3-3:2016 – SR 3.1, SR 3.8, SR 4.1, SR 4.2; NIST SP 800-53 Rev. 5 – SC-8.	Організація забезпечує захист даних, що передаються.
PR.DS-3. Управління активами здійснюється з	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – А.8.2.3, А.8.3.1, А.8.3.2, А.8.3.3, А.11.2.7;	В організації встановлені правила безпечного видалення, передачі та утилізації

Продовження додатка 1

1	2	3
дотриманням правил видалення, передачі та розміщення.	Загальні вимоги – п. 19, 20; НД ТЗІ 2.5-004-99 – 7.3, 8.1. 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.	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. 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 телекомунікаційної 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 3.7-001-99 – 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.	Організація запроваджує контроль безпеки на периметрах телекомунікаційної мережі та інформаційних систем, ОКІІ для виявлення несанкціонованих витоків даних.
PR.DS-6. Механізми перевірки цілісності	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.12.2.1,	Організація використовує механізми перевірки для

Продовження додатка 1

1	2	3
використовуються для верифікації програмного забезпечення, програмно-апаратних засобів та цілісності інформації.	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. 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 – SI-7.	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. 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.

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-телекомунікаційних 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 2.5-004-99 – п. 10.1; НД ТЗІ 1.1-002-99 – п. 7.4. 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,	Організація встановлює базову конфігурацію інформаційно-телекомунікаційних систем/систем управління виробничими процесами. Базова конфігурація передбачає: програмне забезпечення, встановлене на робочих станціях; персональне обладнання, ноутбуки, принтери та кінцеве обладнання; сервери та елементи

Продовження додатка 1

1	2	3
	CM-4, CM-5, CM-6, CM-7, CM-9, SA-10.	телекомунікаційної мережі; конфігурацію та параметри у відповідності до встановлених правил (політик); відповідність запланованій топології телекомунікаційної 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 2.5-004-99 – п. 10.3; НД ТЗІ 3.7-001-99 – п. 6.4; НД ТЗІ 1.1-002-99 – п. 7.4. Довідкові посилання: COBIT 5 – APO13.01; IEC 62443-2-1:2015 – 4.3.4.3.3; NIST SP 800-53 Rev. 5 – SA-3, SA-4, SA-8, SA10, SA-11, SA-12, SA-15, SA-17, PL-8.	Організація застосовує обґрунтовані інженерні принципи захисту інформації щодо специфікації, проєктування, розробки, впровадження та зміни телекомунікаційних 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; Загальні вимоги – п. 10; НД ТЗІ 2.5-004-99 – п. 10.3, 10.6; НД ТЗІ 3.7-001-99 – п. 6.7; НД ТЗІ 1.1-002-99 – п. 7.4. 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.	Організація запроваджує процес управління змінами конфігурації.
PR.IP-4. Резервне копіювання інформації проводиться, підтримується та періодично	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. Довідкові посилання:	Організація має політику резервного копіювання та забезпечує відновлення резервних копій, якщо це необхідно. Копії регулярно тестуються та перевіряються

Продовження додатка 1

1	2	3
тестується.	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.	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. 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 телекомунікаційних 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. 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 відповідно до їх класифікації і конфіденційності.
PR.IP-7. Процеси кіберзахисту постійно вдосконалюються.	Нормативні посилання: НД ТЗІ 1.4-001-2000 – п. 8.2. 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. 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; Загальні вимоги – п. 74; НД ТЗІ 1.4-001-2000 – п. Д5.8, Д.5.6.2. 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, IR-8.	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.

Продовження додатка 1

1	2	3
PR.IP-9. Плани реагування та відновлення тестуються.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.17.1.3; Загальні вимоги – п.39. 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, PM-14.	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.
PR.IP-10. План управління вразливостями розроблено й впроваджено.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.12.6.1, A.18.2.2. Довідкові посилання: NIST SP 800-53 Rev. 5 – RA-3, RA-5, SI-2.	В організації (на ОКІ) розроблено та впровадженно план управління вразливостями для телекомунікаційних 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-телекомунікаційних 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 – A.11.1.2, A.11.2.4, A.11.2.5; Загальні вимоги – п. 10, 39; НД ТЗІ 1.4-001-2000 – п. Д5.6.5. Довідкові посилання: COBIT 5 – BAI09.03; IEC 62443-2-1:2015 – 4.3.3.3.7; NIST SP 800-53 Rev. 5 – MA-2, MA-3, MA-5.	Організація регулярно та за розкладом виконує технічне обслуговування своїх критичних активів. Технічне обслуговування реєструється та проводиться під наглядом уповноваженого персоналу з належними технічними знаннями.
PR.MA-2. Дистанційне обслуговування активів ОКІ схвалено, задокументовано та виконується в спосіб, що унеможливлює	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.11.2.4, A.15.1.1, A.15.2.1; Загальні вимоги – п. 36. Довідкові посилання: COBIT 5 – DSS05.04;	Віддалене обслуговування систем і телекомунікаційних мереж підлягає реєстрації та виконується безпечно, щоб уникнути несанкціонованого доступу.

Продовження додатка 1

1	2	3
несанкціонований доступ.	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.	

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. 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.	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. 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-4, MP-5, MP-7.	Організація запроваджує політики (процедури), що забезпечують застосування правил використання знімнних носіїв інформації, враховуючи застосовану політику класифікації інформації.
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. 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,	Організація впроваджує принцип мінімальних привілеїв, налаштовуючи системи на забезпечення лише життєво важливих послуг та функцій.

Продовження додатка 1

1	2	3
	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.	
PR.PT-4. Телекомунікаційні 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. 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.	Телекомунікаційні мережі та мережі управління регулюють передачу інформації і шляхи, які можуть бути відкриті всередині систем і між ними. По відношенню до них реалізовані заходи захисту.
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. 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.

Продовження додатка 1

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. 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. 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, SI4.	Організація впроваджує практику виявлення, аналізу подій, класифікації кіберінцидентів, кібератак з метою розуміння цілей і методів атак та причин виникнення кіберінцидентів. Можуть впроваджуватись рішення на кшталт SIEM, які: підтримують процес виявлення, аналізу і обробки кіберінцидентів (кібератак).
DE.AE-3. Дані про кіберінциденти агрегуються та корелюються з декількох джерел і датчиків.	Нормативні посилання: НД ТЗІ 2.5-004-99 – п. 6.44; НД ТЗІ 1.4-001-2000 – п. А.1. Довідкові посилання: IEC 62443-3-3:2016 – SR 6.1; NIST SP 800-53 Rev. 5 – AU-6, CA-7, IR-4, IR5, IR-8, SI-4.	Організація впроваджує технологічні та процесні механізми, що дозволяють збирати і зіставляти кіберінциденти, які виявляються в телекомунікаційних 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	Нормативні посилання: Загальні вимоги – п.4. Довідкові посилання:	Організація проводить класифікацію та категоризацію кіберінцидентів і оцінює їх

1	2	3
кіберінцидентів.	COBIT 5 – APO12.06; NIST SP 800-53 Rev. 5 – CP-2, IR-4, RA-3, SI 4.	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. 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 та 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. Телекомунікаційна 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. 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 телекомунікаційні 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. Довідкові посилання: IEC 62443-2-1:2015 – 4.3.3.3.8; NIST SP 800-53 Rev. 5 – CA-7, PE-3, PE-6, PE20.	Компоненти об’єкта повинні забезпечити реєстрацію, збереження в електронних журналах та захист від модифікації інформації про події кібербезпеки.
DE.CM-3. Активність персоналу	Нормативні посилання: Загальні вимоги – п. 19;	Моніторинг діяльності співробітників інтегровано в

Продовження додатка 1

1	2	3
відстежується для виявлення потенційних кіберінцидентів.	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. ДСТУ ISO/IEC 27001:2013 – А.12.4.1. 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.	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 – А.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. Довідкові посилання: 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.	Організація впроваджує механізми, що дозволяють виявляти шкідливі коди в її телекомунікаційних мережах та інформаційних системах (в ОКІІ). По можливості, працює політика запобігання запуску таких 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. 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 телекомунікаційних 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. Довідкові посилання: COBIT 5 – APO07.06; NIST SP 800-53 Rev. 5 – CA-7, PS-7, SA-4, SA9, SI-4.	Здійснюється контроль за послугами, наданими зовнішніми постачальниками товарів і послуг, з метою виявлення несанкціонованого доступу до телекомунікаційних 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	Нормативні посилання: Загальні вимоги – п. 19; НД ТЗІ 1.4-001-2000 – п. Д1.1; НД ТЗІ 2.5-004-99 – п. 9. Довідкові посилання: NIST SP 800-53 Rev. 5 – AU-12,	Організація стежить за доступом співробітників до телекомунікаційних мереж та інформаційних систем (ОКІІ), пристроїв та процесів.

Продовження додатка 1

1	2	3
постійній основі.	CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4.	
DE.CM-8. Сканування вразливостей виконується	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.12.6.1; Загальні вимоги – п. 24; НД ТЗІ 1.4-001-2000 – п. Д1.1; НД ТЗІ 2.5-004-99 – п.9. Довідкові посилання: COBIT 5 – BAI03.10; IEC 62443-2-1:2015 – 4.2.3.1, 4.2.3.7; NIST SP 800-53 Rev. 5 – RA-5.	Організація здійснює процес управління вразливістю в тому числі, шляхом регулярного сканування вразливостей як автоматично, так і за запитом.

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. 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. Довідкові посилання: IEC 62443-2-1:2015 – 4.4.3.2; NIST SP 800-53 Rev. 5 – CA-2 CA-7, PM-14, SI-4.	Організація проводить моніторинг ефективності заходів виявлення кіберінцидентів та співставлення дій щодо виявлення з усіма вимогами.
DE.DP-3. Процеси виявлення	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 –	Організація проводить випробування і перевірку

Продовження додатка 1

1	2	3
кіберінцидентів протестовані.	A.14.2.8; НД ТЗІ 3.7-001-99 – п. 6.8; НД ТЗІ 1.4-001-2000 – п. Д1.1. Довідкові посилання: COBIT 5 – APO13.02; IEC 62443-2-1:2015 – 4.4.3.2; IEC 62443-3-3:2016 – SR 3.3; NIST SP 800-53 Rev. 5 – CA-2, CA-7, PE-3, PM-14, SI-3, SI-4.	ефективності процесів виявлення за планом, та, коли: відбулася суттєва зміна системи; нові прикладні програми розробляються у значних масштабах; в існуючу інфраструктуру додано нову систему; 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. 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. Довідкові посилання: COBIT 5 – APO11.06, DSS04.05; IEC 62443-2-1:2015 – 4.4.3.4; NIST SP 800-53 Rev. 4 – CA-2, CA-7, PL-2, RA-5, SI-4, PM-14.	Організації аналізує кіберінциденти, які відбуваються в їх телекомунікаційних 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. Довідкові посилання: COBIT 5 – BAI01.10; IEC 62443-2-1:2015 – 4.3.4.5.1; NIST SP 800-53 Rev. 5 – CP-2, CP-10, IR-4, IR- 8.	В організації (на ОКІ) розроблено план реагування на кіберінциденти. При зборі даних щодо події та аналізі подій (кіберінцидентів) забезпечується збереженість і цілісність доказів.

4.2. Категорія заходів кіберзахисту RS.CO – Комунікації.

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

Продовження додатка 1

1	2	3
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. Довідкові посилання: IEC 62443-2-1:2015 – 4.3.4.5.2; NIST SP 800-53 Rev. 5 – CA-2, CA-7, CP-2, IR4, IR-8, PE-6, RA-5, SI-4.	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.
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. 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. Довідкові посилання: 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; Довідкові посилання: COBIT 5 – DSS02.07;	Організація забезпечує, щоб кіберінциденти, які генеруються системами виявлення, розслідувалися, класифікувалися і розглядалися послідовним чином.

Продовження додатка 1

1	2	3
	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.	
RS.AN-2. Вплив кіберінциденту усвідомлено.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.16.1.6; Загальні вимоги – п. 22,23. 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.	У процесі класифікації кіберінцидентів організація оцінює їх наслідки для своїх активів та операцій і використовує отримані результати для визначення ступеня серйозності інцидентів.
RS.AN-3. Кіберінциденти класифіковано відповідно до планів реагування. Електронні докази збираються та фіксуються належним чином.	Нормативні посилання: ДСТУ ISO/IEC 27001:2013 – A.16.1.4. 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-4. Створено процеси для отримання, аналізу та реагування на чинники уразливості, виявлені організацією з внутрішніх і зовнішніх джерел.	Нормативні посилання: Загальні вимоги – п. 10, 2Д, 7Д, 11Д; ДСТУ ISO/IEC 27001:2013 – A.6.1.2. Довідкові посилання: COBIT 5 – EDM03.02, DSS05.07; NIST SP 800-53 Rev. 5 SI-5, PM-15; CIS CSC 4, 19.	Запроваджується процес отримання інформації про фактори уразливості з внутрішніх або зовнішніх джерел. Кожен випадок аналізується, перевіряється виконується за процедурою розгляду кіберінцидентів у сфері безпеки, якщо тільки він не є хибним.

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.	Організація визначає процеси та процедури для забезпечення ефективного стримування інцидентів у сфері безпеки.

Продовження додатка 1

1	2	3
	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.	
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. 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. 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. Довідкові посилання: COBIT 5 – BAI01.13; IEC 62443-2-1:2015 – 4.3.4.5.10, 4.4.3.4;	Організація вивчає минулі кіберінциденти після того, як вони будуть врегульовані для того, щоб врахувати досвід. Аналізується вся інформація, яка відома про кіберінцидент, визначивши, що добре спрацювало і що необхідно поліпшити у процесі розгляду кіберінцидентів,

Продовження додатка 1

1	2	3
	NIST SP 800-53 Rev. 5 – CP-2, IR-4, IR-8.	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; 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. Довідкові посилання: COBIT 5 – DSS02.05, DSS03.04; NIST SP 800-53 Rev. 5 CP-10, IR-4, IR-8.	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.
RC.IM-2. Плани відновлення оновлено.	Нормативні посилання: постанова № 518 – п. 4. 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.

5.2. Категорія заходів кіберзахисту RC.IM – Удосконалення.

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

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. 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.

5.3. Категорія заходів кіберзахисту RC.CO – Комунікації.

Заходи з відновлення координуються з внутрішніми та зовнішніми партнерами організації, такими як координаційні центри, оператори, провайдери телекомунікацій, власники атакуючих систем, інші групи реагування на інциденти, пов'язані з інформаційною та/або кібербезпекою (CSIRT), постачальники, 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.
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 телекомунікаційних 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. Довідкові посилання: NIST SP 800-53 Rev. 5 – CP-2, IR-4.	Організація забезпечує інформування внутрішніх і зовнішніх партнерів організації про серйозні кіберінциденти.