Додаток
до Методичних рекомендацій щодо підвищення рівня кіберзахисту систем електронного документообігу
(пункт 4 розділу III)

СИСТЕМА
заходів кіберзахисту до систем електронного документообігу

1. Клас заходів кіберзахисту ID – Ідентифікація ризиків кібербезпеки

1.1. Категорія заходів кіберзахисту ID.AM – Управління активами

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: НД ТЗІ 3.6-006-21 – CM-8,PM-5. Довідкові посилання: NIST SP 800-53 Rev. 5 – CM-8, PM-5.	В організації проводиться ідентифікація та інвентаризація компонентів СЕД, здійснюється їх реєстрація та документування відповідно до затвердженої та прийнятої процедури.
ID.AM-2. Програмне забезпечення, що використовуються ОКІ для надання життєво важливих послуг та функцій, ідентифіковано та задокументовано.	Нормативні посилання: НД ТЗІ 3.6-006-21 – CM-8, PM-5. Довідкові посилання: NIST SP 800-53 Rev. 5 – CM-8, PM-5.	Програмне забезпечення, що використовується для забезпечення функціонування СЕД та її компонентів, ідентифіковано та задокументовано.
ID.AM-3. Електронні комунікації та потоки даних ОКІ ідентифіковано та задокументовано.	Нормативні посилання: НД ТЗІ 3.6-006-21 – C-4, CA-3, CA-9, PL-8. Довідкові посилання: NIST SP 800-53 Rev. 5 – AC-4, CA-3, CA-9, PL-8.	Проводиться інвентаризація електронних комунікацій та управління потоком даних всередині СЕД та між іншими СЕД, які пов’язані між собою з використанням безпечного та авторизованого з’єднання. Розроблено структурну схему інформаційних потоків, яка відображає інформаційну взаємодію між основним СЕД та іншими. Визначено з прив’язкою до кожного елемента схеми інформаційних потоків, категорії інформації та рівні доступу до неї. Вся інформація задокументована та внесена в політику безпеки та

Продовження додатка

1	2	3
		приватності.
ID.AM-4. Зовнішні інформаційні та інформаційно-комунікаційні системи, промислові системи, які взаємодіють з інформаційно-комунікаційними та іншими системами ОКІ, обліковано.	Нормативні посилання: НД ТЗІ 3.6-006-21 – AC-20, SA-9. Довідкові посилання: NIST SP 800-53 Rev. 5 – AC-20, SA-9.	Зовнішні інформаційні та інформаційно-комунікаційні системи та служби організації, які експлуатують СЕД та/або які підтримують функціонування СЕД, слід віднести до певного каталогу.
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: НД ТЗІ 3.6-006-21 – CP-2, RA-2, RA-9, SC-6. Довідкові посилання: NIST SP 800-53 Rev. 5 – CP-2, RA-2, RA-9, SC-6.	Організація класифікує свої активи, враховуючи їх критичність в процесах СЕД. Відповідно до цього організація розробляє план реагування (реагування на кіберінциденти та забезпечення безперервності роботи) та план відновлення (відновлення функціонування після кіберінциденту та відновлення після аварії).
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: НД ТЗІ 3.6-006-21 – CP-2, PS-7, PM-11 Довідкові посилання: NIST S,P 800-53 Rev. 5 – CP-2, PS-7, PM-11.	Визначаються та описуються всі обов’язки та відповідальність штатного персоналу та персоналу партнерів організації, пов’язаних із забезпеченням кіберзахисту СЕД. Затверджується та доводиться до відома персоналу політика інформаційної безпеки/кібербезпеки. У планах реагування та відновлення визначаються ролі персоналу та забезпечується ознайомлення персоналу з цими планами. Упроваджуються програми підвищення обізнаності/навчання працівників з питань забезпечення кіберзахисту СЕД.

Продовження додатка

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

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: НД ТЗІ 3.6-006-21 – CP-2, SA-12. Довідкові посилання: NIST SP 800-53 Rev. 5 – CP-2, SA-12.	Організація ідентифікує та класифікує постачальників у відповідних ланцюгах постачання системи, компоненту системи або системної служби. В угодах з постачальниками можуть бути визначені вимоги з обробки ризиків, які пов'язані з безпекою постачання, послуги моніторяться, 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: НД ТЗІ 3.6-006-21 – PM-8. Довідкові посилання: NIST SP 800-53 Rev. 5 – PM-8.	Організація визначає завдання, які мають виконуватися в рамках впровадження заходів із забезпечення інформаційної безпеки та приватності при розробці документів у СЕД. План захисту організації та ключових ресурсів оновлено відповідно до визначених завдань.
ID.BE-3. Пріоритетність цілей, завдань і заходів щодо забезпечення кібербезпеки, надання життєво важливих послуг та функцій встановлено та повідомлено.	Нормативні посилання: НД ТЗІ 3.6-006-21 – PM-11, RA-9. Довідкові посилання: NIST SP 800-53 Rev. 5 – PM-11, RA-9.	Організація визначає пріоритети цілей, завдань і заходів щодо уніфікованих технологічних процедур службового діловодства.
ID.BE-4. Залежності та найважливіші процеси для забезпечення надання життєво важливих послуг та функцій встановлено.	Нормативні посилання: НД ТЗІ 3.6-006-21 – CP-8, PE-9, PE-11, PM-8, RA-9; Довідкові посилання: NIST SP 800-53 Rev. 5 – CP-8, PE-9, PE-11, PM-8, RA-9.	Організація здійснює ідентифікацію та реєстрацію критично важливих активів, необхідних для забезпечення електронного документообігу. Реєстрація містить принаймні таку інформацію: електронні комунікаційні мережі та інформаційні системи, що забезпечують електронний

Продовження додатка

1	2	3
		документообіг та інші функції, які потребують захисту від відмови джерела живлення або інших збоїв, спричинених аномаліями в службах підтримки; електронні комунікаційні мережі, що забезпечують електронний документообіг та потребують захисту від фальсифікації та перехоплення; планування потенціалу та моніторинг електронних комунікаційних мереж, інформаційних систем, що забезпечують електронний документообіг та інші функції, яке 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: НД ТЗІ 3.6-006-21 – CP-2, CP-11, SA-8, RA-9. Довідкові посилання: NIST SP 800-53 Rev. 5 – CP-2, CP-11, SA-8, RA-9.	Організація ідентифікує та визначає відповідні вимоги для забезпечення стійкості електронного документообігу та інших функцій СЕД. Альтернативні протоколи зв'язку розгорнуто за планом забезпечення безперервної роботи та відновлення функціонування.

1.3. Категорія заходів кіберзахисту ID.GV – Управління безпекою

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: НД ТЗІ 3.6-006-21 – 1 засоби контролю всіх серій. Довідкові посилання: 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. Політика має містити заходи з: управління доступом; підвищення обізнаності та

Продовження додатка

1	2	3
		навчання для користувачів СЕД; аудиту та підзвітності; оцінювання, акредитації та моніторингу безпеки та приватності; управління конфігурацією; планування безперервної роботи; ідентифікації та автентифікації користувачів системи, як в середині організації так і ззовні; індивідуальної участі (мета, сфера застосування, ролі, обов'язки, відповідальність керівництва, координація між підрозділами, система контролю відповідності); реагування на інциденти; технічного обслуговування системи; захисту носіїв інформації; авторизації приватності; фізичного захисту та захисту робочого середовища; планування безпеки та приватності; розроблення концепції інформаційної безпеки; кадрової безпеки; оцінювання ризику; придбання системи та послуг; захисту системи та електронних комунікацій; цілісності інформації; кіберзахисту в СЕД.
ID.GV-2. Обов'язки щодо забезпечення кібербезпеки ОКІ скоординовано та узгоджено з обов'язками персоналу ОКІ та із зовнішніми партнерами.	Нормативні посилання: НД ТЗІ 3.6-006-21 – PM-1, PM-2, PS-7. Довідкові посилання: NIST SP 800-53 Rev. 5 – PM-1, PM-2, PS-7.	В організації визначаються усі обов'язки, пов'язані із забезпеченням інформаційної безпеки/кібербезпеки СЕД. Призначається старша посадова особа служби інформаційної безпеки при експлуатації СЕД. Вимоги щодо безпеки персоналу встановлено відповідно до ролей та обов'язків, які вони виконують. У разі потреби до виконання робіт із забезпечення кіберзахисту можуть залучатися зовнішні організації, що мають ліцензії на відповідний вид діяльності у сфері

Продовження додатка

1	2	3
		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: НД ТЗІ 3.6-006-21 – 1 засоби контролю всіх серій. Довідкові посилання: NIST SP 800-53 Rev. 5 – 1 засоби контролю всіх серій.	Організація узагальнює та виконує нормативно-правові вимоги щодо забезпечення кіберзахисту СЕД, дотримуючись національних та європейських норм, політики та процедури індивідуальної участі та кадрової безпеки, 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: НД ТЗІ 3.6-006-21 – PM-3, PM-7, PM-9, PM-10, PM-11, SA-2. Довідкові посилання: NIST SP 800-53 Rev. 5 – PM-3, PM-7, PM-9, PM-10, PM-11, SA-2.	Організація забезпечує управління станом безпеки та приватності в СЕД. Визначаються необхідні ресурси, проводиться оцінка ризиків. Для проведення аналізу ризиків складаються переліки суттєвих загроз, вразливостей, через які загрози можуть бути реалізовано, описуються методи та способи обробки ризиків.

1.4. Категорія заходів кіберзахисту ID.RA – Оцінка ризиків

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: 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: 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.	Організація проводить безперервний моніторинг стану безпеки та приватності в програмному забезпеченні СЕД різноманітними тестовими методами. Застосовуються методи тестування на проникнення та сканування на наявність вразливостей. Усі відомі вразливості та дефекти були виявлені, оцінюються в організації, ідентифіковані та

Продовження додатка

1	2	3
		задокументовані, 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: НД ТЗІ 3.6-006-21 – PM-15, PM-16, SI-5. Довідкові посилання: 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 внаслідок проведення технічного розслідування кіберінцидентів/кібератак.
ID.RA-3. Загрози кібербезпеки (модель загроз) як внутрішні, так і зовнішні визначено й задокументовано.	Нормативні посилання: НД ТЗІ 3.6-006-21 – RA-3, SI-5, PM-12, PM-16. Довідкові посилання: NIST SP 800-53 Rev. 5 – RA-3, SI-5, PM-12, PM-16.	Відповідно до стратегії (політики) управління ризиками організація визначає та документує можливі загрози для СЕД, які можуть бути реалізовані через ідентифіковані вразливості в її активах, та забезпечує поінформованість щодо них.
ID.RA-4. Потенційні наслідки (рівень шкоди), які можуть завдати загрози внаслідок їх реалізації на безперервне надання життєво важливих послуг та функцій та ймовірності їх реалізації, визначено.	Нормативні посилання: НД ТЗІ 3.6-006-21 – RA-2, RA-3, PM-9, PM-11. Довідкові посилання: NIST SP 800-53 Rev. 5 – RA-2, RA-3, PM-9, PM-11.	Виконується кількісна або якісна оцінка збитків, що можуть бути нанесені СЕД та її компонентам 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 СЕД та її компонентами внаслідок реалізації загрози.
ID.RA-5. Для визначення ризику застосовуються дані щодо загроз, вразливостей, їх ймовірностей та рівня шкоди, які використано для визначення ризику кібербезпеки.	Нормативні посилання: НД ТЗІ 3.6-006-21 – RA-2,RA-3, PM-16. Довідкові посилання: NIST SP 800-53 Rev. 5 – RA-2, RA-3, PM-16.	Організація визначає у методології управління ризиками критерії для визначення ймовірності та впливу ризику на СЕД та її компоненти, а також на інформацію, яка в ній обробляється. Вразливість та загрози враховуються під час процесу ідентифікації ризиків.

Продовження додатка

1	2	3
ID.RA-6. Заходи реагування на ризик кібербезпеки визначено та їх пріоритетність встановлено.	Нормативні посилання: НД ТЗІ 3.6-006-21 – PM-4, PM-9. Довідкові посилання: NIST SP 800-53 Rev. 5 – PM-4, PM-9.	На підставі визначеної методології управління ризиками організація впроваджує заходи реагування на ризики кібербезпеки в СЕД, які ідентифіковані та рівні яких розраховано з урахуванням їх пріоритетності.

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

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: НД ТЗІ 3.6-006-21 – PM-9. Довідкові посилання: NIST SP 800-53 Rev. 5 – PM-9.	Стратегію управління ризиками розроблено та реалізовано в масштабах організації.
ID.RM-2. Допустимий рівень ризику кібербезпеки визначено та чітко виражено.	Нормативні посилання: НД ТЗІ 3.6-006-21 – PM-9. Довідкові посилання: NIST SP 800-53 Rev. 5 – PM-9.	Організація формулює в методології управління ризиками свій підхід до обробки ризиків кібербезпеки в СЕД 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: НД ТЗІ 3.6-006-21 – PM-8, PM-9, PM-11, RA-9. Довідкові посилання: NIST SP 800-53 Rev. 5 – PM-8, PM-9, RA-9.	Організація визначає порядок обробки ризиків: інформаційної/кібербезпеки для організаційних операцій та активів, фізичних осіб, інших організацій та партнерів, пов’язаних з експлуатацією та використанням СЕД, забезпечення приватності та ланцюга постачання. План захисту організації та ключових ресурсів службового діловодства в СЕД оновлено відповідно до визначених завдань.

Продовження додатка

1.6. Категорія заходів кіберзахисту ID.SC – Управління ризиками системи 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: НД ТЗІ 3.6-006-21 – SA-9, SA-12, PM-9. Довідкові посилання: NIST SP 800-53 Rev. 5 – SA-9, SA-12, PM-9.	Організація проводить аудит постачальників товарів і послуг, зовнішніх системних послуг, які надаються організацією в рамках забезпечення електронного документообігу, 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 відповідно до політики управління ризиками кібербезпеки з урахуванням ризиків, притаманних системі постачання.	Нормативні посилання: НД ТЗІ 3.6-006-21 – RA-2, RA-3, RA-9, SA-12, SA-15, PM-9. Довідкові посилання: NIST SP 800-53 Rev. 5 – RA-2, RA-3, RA-9, SA-12, SA-15, PM-9	Організація забезпечує ідентифікацію та класифікацію постачальників компонентів і послуг для СЕД та схем інших адміністративних й ділових процесів. Організація класифікує своїх постачальників за: доступом до конфіденційної інформації; можливим впливом на ланцюг поставок; компонентами і послугами, що надаються. Ця інформація врахована та внесена до Стратегії управління ризиками.
ID.SC-3. Постачальники товарів і послуг та партнери відповідно до договору можуть впроваджувати заходи, спрямовані на досягнення мети політики інформаційної безпеки/кібербезпеки ОКІ та плану управління ризиками постачання.	Нормативні посилання: НД ТЗІ 3.6-006-21 – A-9, SA-11, SA-12, PM-9. Довідкові посилання: NIST SP 800-53 Rev. 5 – SA-9, SA-11, SA-12, PM-9.	У випадку укладення договору із постачальниками зовнішніх онлайн сервісів та служб електронного документообігу, а також інших компонентів і послуг для СЕД у ньому можуть бути прямо вказані вимоги із забезпечення належного рівня надання цих послуг, у тому числі взаємні обов’язки із кіберзахисту СЕД та його компонентів, до яких постачальник може отримати

Продовження додатка

1	2	3
		доступ (обробка, зберігання, взаємодія). Здійснюється періодичний контроль виконання постачальником своїх зобов'язань, проводяться огляди результатів аудитів, або інші еквівалентні перевірки постачальників. Організація розробляє та проваджує план з оцінювання забезпечення безпеки та приватності розробником СЕД.
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: НД ТЗІ 3.6-006-21 – AU-2, AU-6, AU-12, AU- 16, PS-7, SA-9, SA-12. Довідкові посилання: 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 внутрішніх та зовнішніх постачальників компонентів і послуг, які надаються в рамках забезпечення функціонування СЕД, партнерів та проводить аудит, щоб встановити повноту надання послуг та виконання ними договірних зобов'язань в повному обсязі.
ID.SC-5. З постачальниками проводиться планування і тестування реагування за відповідними політиками реагування на кіберінциденти та відновлення стану кібербезпеки.	Нормативні посилання: НД ТЗІ 3.6-006-21 – CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9. Довідкові посилання: NIST SP 800-53 Rev. 5 – CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9.	Організація забезпечує проведення з розробником та постачальником СЕД планування та тестування заходів із реагування на кіберінциденти для забезпечення безперервної роботи та відновлення функціонування СЕД. Плани реагування існують і регулярно тестуються та покращуються.

2. Клас заходів кіберзахисту PR – Кіберзахист

2.1. Категорія заходів кіберзахисту PR.AC – Управління ідентифікацією, автентифікацією та контроль 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	Нормативні посилання: НД ТЗІ 3.6-006-21 – AC-1, AC-2, IA-1, IA-2,	Організація забезпечує ідентифікацію та автентифікацію

Продовження додатка

1	2	3
користувачів, адміністраторів та процесів призначаються, верифікуються, адмініструються, відкликаються (скасовуються) та перевіряються.	ІА-3, ІА-4, ІА-5, ІА-6, ІА-7, ІА-8, ІА-9, ІА-10, ІА-11. Довідкові посилання: 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.	користувачів СЕД та процесів, які вони виконують. Організація визначає типи системних облікових записів, які дозволені для використання в СЕД у рамках забезпечення підтримки цілей, завдань, функцій і процесів організації. Організація передбачає ідентифікацію та автентифікацію авторизованих користувачів СЕД, адміністраторів та процесів перед встановленням локального та дистанційного підключення.
PR.AC-2. Фізичний доступ до ОКІІ захищений та управляється.	Нормативні посилання: НД ТЗІ 3.6-006-21 – PE-2, PE-3, PE-4, PE5, PE-6, PE-8. Довідкові посилання: NIST SP 800-53 Rev. 5 – PE-2, PE-3, PE-4, PE-5, PE-6, PE-8.	Організація охороняє та керує фізичним доступом до своїх об'єктів та інфраструктури, що підтримують її електронні комунікаційні мережі та інформаційні системи. Цей контроль застосовується до всіх співробітників та відвідувачів, «чутливих» зон, у яких доступ обмежений, або до «чутливих» районів, в яких обробляється конфіденційна інформація та розміщені електронні комунікаційні мережі або інформаційні системи. Організація забезпечує введення та затвердження переліку осіб, які мають право авторизованого доступу до об’єкта, де перебуває СЕД. Організація забезпечує авторизацію фізичного доступу до сервісних модулів та інструментальних засобів СЕД та ведення журналу контролю такого доступу до електронної комунікаційної мережі, в якій розгорнуто СЕД.
PR.AC-3. Здійснюється контроль та управління віддаленим доступом.	Нормативні посилання: НД ТЗІ 3.6-006-21 – AC-1, AC-17, AC-19, AC-20, SC-15. Довідкові посилання:	Організація встановлює обмеження на використання та розробляє вимоги до конфігурації/підключення до платформи СЕД.

Продовження додатка

1	2	3
	NIST SP 800-53 Rev. 5 – AC-1, AC-17, AC-19, AC-20, SC-15.	Організація має політику віддаленого доступу, яка передбачає всі види доступу, в тому числі й мобільного, безпроводового. Віддалена активація спільних обчислювальних пристроїв (хмар) та застосунків заборонена.
PR.AC-4. Права доступу встановлено із застосуванням принципів мінімальних привілеїв та розподілу обов'язків.	Нормативні посилання: НД ТЗІ 3.6-006-21 – AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24. Довідкові посилання: 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. Пов’язані атрибути безпеки та приватності мають створюватися і зберігатися разом з інформацією на серверах СЕД. Рішення щодо управління доступом застосовано до кожного запиту щодо виконання доступу до модулів та бізнес-процесів СЕД.
PR.AC-5. Цілісність електронної комунікаційної мережі захищено (наприклад, сегментація мережі).	Нормативні посилання: НД ТЗІ 3.6-006-21 – AC-4, AC-10, SC-7. Довідкові посилання: NIST SP 800-53 Rev. 5 – AC-4, AC-10, SC-7.	Цілісність електронної комунікаційної мережі з розгорнутою СЕД захищена за допомогою поділу та сегментації мережі. Підключення до зовнішніх мереж або систем здійснюється тільки через керовані інтерфейси, що складаються з пристроїв захисту периметра, які розташовані відповідно до архітектури безпеки та приватності організації.
PR.AC-6. Ідентичність особи підтверджується і прив’язується до облікових даних та затверджується під час взаємодії.	Нормативні посилання: 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: 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.	Організація забезпечує процес реєстрації і відміни такої реєстрації всіх користувачів організації з можливістю надання відповідних прав доступу. Особи перед отримання дозволу на доступ до СЕД перевірено, список доступу, в якому закріплений перелік персоналу або ролей, оновлюється. Користувачі або процеси, що не належать організації, в якій розгорнуто СЕД, які діють від імені користувачів, унікально ідентифіковано та автентифіковано.

Продовження додатка

1	2	3
PR.AC-7. Автентифікація користувачів, адміністраторів, пристроїв та інших активів проводиться (наприклад методами однофакторної, багатофакторної автентифікації) відповідно до встановленого ризику порушення безпеки.	Нормативні посилання: 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. Довідкові посилання: 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.	Організація проводить ідентифікацію та автентифікацію користувачів або процесів, які діють від імені користувачів, здійснює управління системними автентифікаторами. Системні автентифікатори управляються. Механізми автентифікації в СЕД визначаються та оновлюються з метою забезпечення цілісності та конфіденційності інформації.

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

Таблиця 8 – Заходи кіберзахисту категорії PR.AT

Заходи кіберзахисту		
захід кіберзахисту	нормативні та додаткові посилання	опис
PR.AT-1. Усі співробітники ОКІ обізнані та пройшли підготовку з питань кібербезпеки.	Нормативні посилання: НД ТЗІ 3.6-006-21– AT-2, PM-13. Довідкові посилання: NIST SP 800-53 Rev. 5 – AT-2, PM-13.	Організація формує та затверджує програму розвитку та вдосконалення спеціалістів з питань забезпечення безпеки та приватності. Організація забезпечує проходження співробітниками СЕД базових тренінгів з підвищення обізнаності у сфері забезпечення безпеки та приватності для користувачів СЕД (включно з менеджерами, керівниками компаній і підрядниками).
PR.AT-2. Користувачі (адміністратори) з перевагами доступу розуміють свої обов’язки з питань кібербезпеки.	Нормативні посилання: НД ТЗІ 3.6-006-21 – AT-3, PM-13. Довідкові посилання: NIST SP 800-53 Rev. 5 – AT-3, PM-13.	Користувачі (адміністратори), яким надано привілеї доступу до СЕД, ретельно вивчають свої обов'язки з питань кібербезпеки. Навчання користувачів (адміністраторів) проводиться на основі ролей в СЕД. Користувачам надання доступу до СЕД або допуску до виконання обов’язків в організації здійснюється тільки після проходження навчання.
PR.AT-3. Партнери	Нормативні посилання:	Партнери організації знають та

Продовження додатка

організації розуміють свої обов'язки з питань кібербезпеки.	НД ТЗІ 3.6-006-21 – PS-7, SA-9, SA-16. Довідкові посилання: NIST SP 800-53 Rev. 5 – PS-7, SA-9, SA-16.	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 користування та забезпечення належного функціонування СЕД.
PR.AT-4. Керівництво ОКІ розуміє свої обов'язки з питань кібербезпеки.	Нормативні посилання: НД ТЗІ 3.6-006-21 – AT-3, PM-13. Довідкові посилання: NIST SP 800-53 Rev. 5 – AT-3, PM-13.	Керівництво організації забезпечує проведення навчання працівників з питань забезпечення безпеки та приватності відповідно до їх ролей.
PR.AT-5. Персонал із забезпечення фізичної та інформаційної безпеки розуміє свої обов'язки.	Нормативні посилання: НД ТЗІ 3.6-006-21 – AT-3, IR-2, PM-13. Довідкові посилання: NIST SP 800-53 Rev. 5 – AT-3, IR-2, PM-13.	Визначаються та призначаються всі обов'язки, пов'язані із забезпеченням фізичної та інформаційної безпеки. Персонал має належну кваліфікацію щодо реагування на кіберінциденти в СЕД відповідно до призначених ролей та обов'язків, на постійній основі проводиться підвищення кваліфікації, кожен розуміє межі своїх повноважень.

2.3. Категорія заходів кіберзахисту PR.DS – Безпека даних

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: НД ТЗІ 3.6-006-21 – MP-8, SC-12, SC-28. Довідкові посилання: NIST SP 800-53 Rev. 5 – MP-8, SC-12, SC-28.	В електронних комунікаційних мережах та СЕД забезпечується конфіденційність, цілісність та доступність даних організації. Криптографічні механізми для запобігання несанкціоновану розкриттю та модифікації даних впроваджено.
PR.DS-2. Дані, що передаються, захищено.	Нормативні посилання: НД ТЗІ 3.6-006-21 – SC-8, SC-11, SC-12.	Організація забезпечує захист даних, що передаються.

Продовження додатка

1	2	3
	НД ТЗІ 3.7-001-99 – п. 6.4.2. Довідкові посилання: NIST SP 800-53 Rev. 5 – SC-8, SC-11, SC-12.	Організація встановлює та забезпечує управління криптографічними ключами для криптографічних засобів, які використовуються в СЕД.
PR.DS-3. Управління активами здійснюється з дотриманням правил видалення, передачі та розміщення.	Нормативні посилання: НД ТЗІ 3.6-006-21 – CM-8, MP-6, PE-16. Довідкові посилання: NIST SP 800-53 Rev. 5 – CM-8, MP-6, PE-16.	В організації встановлені процеси авторизації, моніторингу та контролю за документами в СЕД. Впроваджуються механізми безпечного видалення, передачі та утилізації інформації на серверах та носіях СЕД зі стійкістю та цілісністю, що відповідає категорії безпеки або рівню секретності інформації.
PR.DS-4. Необхідні спроможності для забезпечення доступності активів створено та підтримуються.	Нормативні посилання: НД ТЗІ 3.6-006-21 – AU-4, CP-2, SC-5. Довідкові посилання: NIST SP 800-53 Rev. 5 – AU-4, CP-2, SC-5.	Спроможність СЕД контролюється задля забезпечення доступності активів. Організація забезпечує відповідний рівень захисту доступності документів у СЕД з метою мінімізації наслідків атак та подій (DoS), які призведуть до відмови в обслуговуванні СЕД.
PR.DS-5. Захист від витоку даних впроваджено.	Нормативні посилання: НД ТЗІ 3.6-006-21 – C-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4. Довідкові посилання: 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 забезпечує захист СЕД, передачу даних та інформації відповідно до національних політик і процедур захисту від несанкціонованих витоків даних. Організація впроваджує захист від витоку інформації шляхом випромінювання електромагнітних сигналів. Організація проводить аналіз схем, відповідно до яких здійснюються комунікації в СЕД, з метою визначення таких схем комунікацій, які володіють потенційними можливостями для реалізації прихованих каналів. Організація впроваджує криптографічні засоби та визначає тип криптографічного захисту для кожного сервісного модуля СЕД. Організація забезпечує контроль та управління зв’язком на зовнішньому периметрі системи та

Продовження додатка

1	2	3
		на ключових внутрішніх периметрах всередині СЕД.
PR.DS-6. Механізми перевірки цілісності використовуються для верифікації програмного забезпечення, програмно-апаратних засобів та цілісності інформації.	Нормативні посилання: 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 забезпечує впровадження інструментів перевірки цілісності для виявлення несанкціонованих змін програмного забезпечення СЕД. Ці заходи контролю призначені для виявлення несанкціонованого втручання або непередбачених помилок, викликаних неправомірним використанням. Забезпечується перевірка атрибутів безпеки та приватності пов'язаних з інформацією, яка передається між системами та компонентами СЕД.
PR.DS-7. Середовища розробки та тестування відокремлені від виробничого середовища.	Нормативні посилання: НД ТЗІ 3.6-006-21 – CM-2. Довідкові посилання: NIST SP 800-53 Rev. 5 – CM-2.	Організація забезпечує розподіл середовищ розробки та тестування СЕД від розгорнутої платформи СЕД.
PR.DS-8. Механізми перевірки цілісності використовуються для перевірки цілісності обладнання	Нормативні посилання: НД ТЗІ 3.6-006-21 – SA-10, SI-7. Довідкові посилання: NIST SP 800-53 Rev. 5 – SA-10, SI-7.	Організація забезпечує цілісність обладнання, запроваджуючи періодичні перевірки та перевірки виробником самого обладнання або сертифікованим постачальником цього самого обладнання для виявлення несанкціонованих змін в сервісних модулях та службах СЕД.

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

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	Нормативні посилання: НД ТЗІ 3.6-006-21 – CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10. Довідкові посилання:	Організація встановлює та підтримує базову конфігурацію в СЕД на робочих місцях організації, на серверах та у мобільних пристроях користувачів.

Продовження додатка

1	2	3
створена й підтримується.	NIST SP 800-53 Rev. 5 – CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10.	Організація визначає та забезпечує застосування фізичних і логічних обмежень доступу, пов'язаних зі змінами в СЕД. Організація розробляє та реалізує План управління конфігурацією СЕД.
PR.IP-2. Життєвий цикл розробки, експлуатації та управління системами (SDLC) впроваджено.	Нормативні посилання: 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: 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 визначає ролі та обов'язки щодо забезпечення безпеки та приватності інформації протягом усього життєвого циклу розробки СЕД. Організація розробляє та забезпечує виконання плану оцінювання безпеки та приватності, проводить тестування й оцінювання системних компонентів або системних служб СЕД на всіх етапах проєктування та життєвого циклу розробки системи. Організація вимагає від розробника СЕД, системних компонентів СЕД або системних служб дотримання вимог існуючої та затвердженої документації щодо забезпечення безпеки та приватності. Організація разом із розробником СЕД, системних компонентів СЕД або системних служб створюють проєкт та архітектуру безпеки.
PR.IP-3. Процеси (заходи) управління змінами конфігурації впроваджено.	Нормативні посилання: НД ТЗІ 3.6-006-21 – CM-3, CM-4, SA-10. Довідкові посилання: NIST SP 800-53 Rev. 5 – CM-3, CM-4, SA-10.	Організація запроваджує процес управління конфігурацією під час розробки, проєктування, реалізації та експлуатації СЕД, його системних компонентів або служб. Організація проводить моніторинг і аналіз дій, пов'язаних зі змінами конфігурації СЕД та її сервісних модулів.
PR.IP-4. Резервне копіювання інформації проводиться, підтримується та періодично тестується.	Нормативні посилання: НД ТЗІ 3.6-006-21 – CP-4, CP-6, CP-9. Довідкові посилання: NIST SP 800-53 Rev. 5 –	Організація має політику резервного копіювання системної інформації на системному рівні, що міститься в СЕД та забезпечує відновлення резервних копій, якщо

Продовження додатка

1	2	3
	CP-4, CP-6, CP-9.	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: НД ТЗІ 3.6-006-21 – PE-10, PE-12, PE-13, PE-14, PE-15, PE-18. Довідкові посилання: 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 операційного середовища СЕД та обладнання від природних катастроф, відключення електроенергії, пожежі та повені.
PR.IP-6. Дані знищуються відповідно до політики безпеки.	Нормативні посилання: НД ТЗІ 3.6-006-21 – MP-6. Довідкові посилання: NIST SP 800-53 Rev. 5 – MP-6.	Організація забезпечує очищення системних носіїв з СУБД, web-серверами, e-mail-серверами перед утилізацією, випуском за межі організаційного контролю або перед повторним використанням. Використовуються механізми очищення зі стійкістю та цілісністю, що відповідає категорії безпеки або рівню секретності інформації, яка зберігається в СЕД.
PR.IP-7. Процеси кіберзахисту постійно вдосконалюються.	Нормативні посилання: НД ТЗІ 3.6-006-21 – CA-2, CA-7, CP-2, IR-8, PL-2, PM-6. Довідкові посилання: NIST SP 800-53 Rev. 5 – CA-2, CA-7, CP-2, IR-8, PL-2, PM-6.	Організація розробляє, відстежує та звітує про результати вимірювань показників продуктивності забезпечення безпеки інформації та приватності на основі плану захисту інформації та персональних даних для СЕД
PR.IP-8. Інформація про ефективність технологій захисту розподіляється	Нормативні посилання: НД ТЗІ 3.6-006-21 – AC-21, CA-7, SI-4. Довідкові посилання: NIST SP 800-53 Rev. 5 – AC-21, CA-7, SI-4.	Організація забезпечує спрощений обмін інформацією, надаючи змогу авторизованим користувачам визначати чи відповідають повноваження на доступ, що призначені партнерам для обміну інформацією, обмеженням доступу та повноваженням для забезпечення приватності щодо інформації.
PR.IP-9. Плани реагування (реагування на кіберінциденти та забезпечення безперервності бізнесу) і плани відновлення	Нормативні посилання: НД ТЗІ 3.6-006-21 – CP-2, CP-7, CP-12, CP- 13, IR-7, IR-8, IR-9, PE-17. Довідкові посилання: NIST SP 800-53 Rev. 5 –	План забезпечення безперервної роботи та відновлення функціонування компонентів СЕД та план реагування на інциденти розроблені та регулярно оновлюються. Застосовано альтернативні

Продовження додатка

1	2	3
(відновлення після кіберінциденту та відновлення після аварії) наявні та управляються.	CP-2, CP-7, CP-12, CP- 13, IR-7, IR-8, IR-9, PE-17.	механізми безпеки, коли основні засоби реалізації функцій безпеки в СЕД недоступні або скомпрометовані.
PR.IP-10. Плани реагування та відновлення тестуються.	Нормативні посилання: НД ТЗІ 3.6-006-21 – CP-4, IR-3, PM-14. Довідкові посилання: NIST SP 800-53 Rev.4 – CP-4, IR-3, PM-14.	Організація забезпечує розроблення, підтримання на постійній основі та виконання організаційних планів щодо проведення тестування безпеки та приватності, навчання та моніторингу діяльності, пов'язаної з електронним документообігом організації.
PR.IP-11: Кібербезпека внесена до практики роботи з персоналом (наприклад, деініціалізація, перевірка персоналу)	Нормативні посилання: 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: NIST SP 800-53 Rev. 5 – PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21.	Політика кадрової безпеки організації, в якій розгорнута СЕД, розроблена, задокументована та поширена серед співробітників. Організаційні заходи для практики роботи з персоналом СЕД такі, як перевірка, звільнення, переведення, укладання контрактів тощо, переглядаються відповідно до встановлених вимог. Формальний процес санкцій для осіб організації, які не дотримуються встановлених правил і процедур інформаційної безпеки застосовано та юридично узгоджено.
PR.IP-12. План управління вразливостями розроблено й впроваджено.	Нормативні посилання: НД ТЗІ 3.6-006-21 – RA-3, RA-5, SI-2. Довідкові посилання: NIST SP 800-53 Rev. 5 – RA-3, RA-5, SI-2.	В організації розроблено та впроваджено план управління вразливостями для СЕД. Сканування вразливостей в СЕД та інстальованих сервісних модулях та інструментальних засобах здійснюється на систематичній основі, виявлені дефекти виправлено. Оновлення програмного забезпечення СЕД та оновлення вбудованого програмного забезпечення в межах випуску оновлень інстальовано.

2.5. Категорія заходів кіберзахисту PR.MA – Технічне обслуговування

Таблиця 11 – Заходи кіберзахисту категорії PR.MA

Заходи кіберзахисту

Продовження додатка

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: НД ТЗІ 3.6-006-21 – MA-2, MA-3, MA-5. Довідкові посилання: NIST SP 800-53 Rev. 5 – MA-2, MA-3, MA-5.	Організація регулярно планує, документує та переглядає записи з технічного обслуговування, ремонту або заміни компонентів СЕД відповідно до організаційних вимог її розробника. Проводиться моніторинг усіх заходів з технічного обслуговування СЕД, незалежно від того, виконуються вони на місці або віддалено, а також чи обслуговуються системи або системні компоненти на місці чи переміщуються в інше місце. Процедуру авторизації технічного персоналу встановлено, перелік авторизованих організацій технічного обслуговування або персоналу сформовано.
PR.MA-2. Дистанційне обслуговування активів ОКІ схвалено, задокументовано та виконується в спосіб, що унеможливлює несанкціонований доступ.	Нормативні посилання: НД ТЗІ 3.6-006-21 – MA-4. Довідкові посилання: NIST SP 800-53 Rev. 5 – MA-4.	Організація дозволяє використання віддалених засобів технічного обслуговування в СЕД та діагностики відповідно до організаційної політики. Облік віддалених дій з обслуговування та діагностики сервісних модулів та інструментальних засобів СЕД ведеться.

2.6. Категорія заходів кіберзахисту PR.PT – Технології кіберзахисту

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: НД ТЗІ 3.6-006-21 – AU Клас. Довідкові посилання: NIST SP 800-53 Rev. 5 – AU Family.	Записи аудиту (журналів подій) на рівні серверних додатків СЕД визначаються, документуються, впроваджуються та регулярно переглядаються відповідно до політик, правил, процедур з безпеки. СЕД генерує записи аудиту, що

Продовження додатка

1	2	3
		містять інформацію, яка встановлює: який тип події стався, коли відбулася подія, де відбулася подія, джерело події, результат події та ідентифікатор будь-яких осіб або суб'єктів, пов'язаних з подією.
PR.PT-2. Змінні носії захищено, а їх використання обмежено відповідно до правил, процедур з безпеки.	Нормативні посилання: НД ТЗІ 3.6-006-21 – MP-2, MP-3, MP-4, MP- 5, MP-7, MP-8. Довідкові посилання: NIST SP 800-53 Rev. 5 – MP-2, MP-3, MP-4, MP- 5, MP-7, MP-8.	Доступ до локального сховища даних СЕД, серверів баз даних, e-mail-сервераів, web-серверів обмежено відповідно до функцій, які виконують адміністратори та користувачі для підтримання роботи СЕД. На носіях інформації маркування, що вказують на обмеження поширення та обробки, а також застереження нанесено. Системні носії з розгорнутою платформою СЕД захищено до того часу, як носії знищуються або очищаються, з використанням затвердженого обладнання, методів та процедур.
PR.PT-3. Контроль доступу до систем і активів здійснюється із застосуванням принципу мінімальних привілеїв.	Нормативні посилання: НД ТЗІ 3.6-006-21 – AC-3, CM-7. Довідкові посилання: NIST SP 800-53 Rev. 5 – AC-3, CM-7.	Повноваження для логічного доступу до інформації та ресурсів СЕД застосовано й затверджено відповідно до чинної політики безпеки та приватності. Використання визначених організацією функцій, портів, протоколів та/або служб на серверах СЕД заборонено або обмежено.
PR.PT-4. Електронні комунікаційні мережі та мережі управління захищено.	Нормативні посилання: 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: 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,	Альтернативні електронні СЕД впроваджено, коли основні можливості зв'язку недоступні на основному місці локації або розташовані на альтернативному майданчику для роботи чи зберігання. Авторизувати віддалений та/або безпроводовий доступ до СЕД, перш ніж будуть дозволені такі підключення. Поділ СЕД за функціональною архітектурою на сервісні модулі та системні компоненти, які

Продовження додатка

1	2	3
	SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43.	розміщені в окремих фізичних доменах або середовищах на основі технології віртуальних мереж.
PR.PT-5. Упровадження механізмів на ОКІ для досягнення вимог до стійкості у разі надзвичайних ситуацій та інцидентів у кіберпросторі.	Нормативні посилання: НД ТЗІ 3.6-006-21– CP-7, CP-8, CP-11, CP-13, PL8, SA-14, SC-6. Довідкові посилання: NIST SP 800-53 Rev. 5 – CP-7, CP-8, CP-11, CP-13, PL8, SA-14, SC-6.	Організація визначає альтернативні протоколи зв'язку та альтернативний майданчик для роботи та забезпечує доступними для роботи інформацією, обладнанням та приладами, що необхідні для передачі та відновлення роботи. Укладено контракти протягом встановленого організацією періоду часу для передачі та відновлення роботи. Організація впроваджує на альтернативному майданчику роботи заходи захисту, еквівалентні тим, що впровадженні на основному майданчику. Визначаються правила належного розподілу додаткових ресурсів СЕД, які необхідні для досягнення стійкості.

3. Клас заходів кіберзахисту DE – Виявлення кіберінцидентів

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

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 3.6-006-21 – AC-4, CA-3, CM-2, SI- 4. Довідкові посилання: NIST SP 800-53 Rev. 5 – AC-4, CA-3, CM-2, SI- 4.	Організація забезпечує, щоб для управління потоком інформації всередині СЕД та між пов’язаними зовнішніми системами застосовувалися затверджені повноваження. Мережеві операції за допомогою платформи СЕД здійснюються на структурованій основі кваліфікованим персоналом, забезпечується захист цілісності, конфіденційності та доступності інформації.

Продовження додатка

1	2	3
		Перегляд та оновлення базових налаштувань здійснюються з визначеним періодом, за потреби та при встановленні нових або оновленні існуючих компонентів СЕД.
DE.AE-2. Існує практика аналізу виявлених подій	Нормативні посилання: НД ТЗІ 3.6-006-21 – AU-6, CA-7, IR-4, SI-4. Довідкові посилання: NIST SP 800-53 Rev. 5 – AU-6, CA-7, IR-4, SI-4.	Організація впроваджує практику перегляду та оновлення записів системного аудиту для виявлення та аналізу подій, класифікації кіберінцидентів, кібератак з метою розуміння цілей і методів атак та причин виникнення кіберінцидентів. Стратегію безперервного моніторингу безпеки та приватності розроблено.
DE.AE-3. Дані про події збираються та корелюються з кількох джерел та датчиків.	Нормативні посилання: НД ТЗІ 3.6-006-21 – AU-6, CA-7, IR-4, IR-5, IR-8, SI-4. Довідкові посилання: 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 дозволяє проводити огляд, аудит, аналізувати та звітувати стосовно зміни рівня ризику на основі інформації від правоохоронних органів, розвідувальної інформації або від інших достовірних джерел інформації, налаштовано в рамках СЕД. Кіберінциденти, які пливають на безпеку та приватність, відстежуються та документуються.
DE.AE-4. Існує процес визначення можливих впливів кіберінцидентів.	Нормативні посилання: НД ТЗІ 3.6-006-21 – CP-2, IR-4, RA-3, SI-4. Довідкові посилання: NIST SP 800-53 Rev. 5 – CP-2, IR-4, RA-3, SI 4.	Організація на основі моніторингу та оцінювання ризику розробляє План забезпечення безперервної роботи та відновлення функціонування СЕД та її функціональних компонентів.
DE.AE-5. Пороги оповіщення про кіберінциденти встановлено.	Нормативні посилання: НД ТЗІ 3.6-006-21 – IR-4, IR-5, IR-8. Довідкові посилання: NIST SP 800-53 Rev. 5 – IR-4, IR-5, IR-8.	Організація забезпечує оновлення Плану реагування на інциденти в разі системних та організаційних змін або проблем в СЕД, що виникають при реалізації, виконанні чи тестуванні. Адміністратори безпеки СЕД повідомляються у разі зміни плану реагування на інциденти.

Продовження додатка

3.2. Категорія заходів кіберзахисту DE.CM – Безперервний моніторинг 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: НД ТЗІ 3.6-006-21 – AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4. Довідкові посилання: NIST SP 800-53 Rev. 5 – AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4.	Процес моніторингу в СЕД інтегровано в існуючий процес управління заходами кіберзахисту організації. Організація визначає авторизованих користувачів СЕД, членство в групі та ролі, а також надає дозволи доступу. Типи подій в СЕД, що перевіряються, повинні перевірятися окремими компонентами системи.
DE.CM-2. Фізичне середовище відстежується для виявлення потенційних кіберінцидентів.	Нормативні посилання: НД ТЗІ 3.6-006-21 – CA-7, PE-3, PE-6, PE-20. Довідкові посилання: NIST SP 800-53 Rev. 5 – CA-7, PE-3, PE-6, PE-20.	Організація забезпечує авторизацію фізичного доступу до ресурсів СЕД. Журнали контролю фізичного доступу для локального сховища документів формуються на основі безперервного моніторингу. Моніторинг фізичного доступу до об’єкта, де розгорнуто СЕД, проводиться. Журнали фізичного доступу переглядаються на предмет наявності потенційних ознак подій. Моніторинг та відстеження змін місця розташування та переміщення документів здійснюються в зоні контрольованого ядра розгорнутої СЕД.
DE.CM-3. Активність персоналу відстежується для виявлення потенційних кіберінцидентів.	Нормативні посилання: НД ТЗІ 3.6-006-21 – AC-2,AU-12, AU- 13, CA-7, CM-10, CM-11. Довідкові посилання: NIST SP 800-53 Rev. 5 – AC-2, AU-12, AU- 13, CA-7, CM-10, CM-11.	Персоналом визначаються відкриті джерела інформації та/або інформаційні сайти для отримання свідчень про несанкціоноване розкриття корпоративної інформації. Організація контролює та документує використання технології однорангового обміну файлами в СЕД.

Продовження додатка

1	2	3
		Застосовуються правила (політики) встановлення програмного забезпечення СЕД.
DE.CM-4. Шкідливий код виявляється.	Нормативні посилання: НД ТЗІ 3.6-006-21 – SI-3, SI-8. Довідкові посилання: NIST SP 800-53 Rev. 5 – SI-3, SI-8.	Організація впроваджує механізми захисту від шкідливого коду на основі електронного підпису документів на вході та виході системи для виявлення та знищення шкідливого коду. Проводиться періодичне сканування СЕД. Впроваджуються механізми захисту від спаму в СЕД у точках входу та виходу системи, щоб виявляти та протидіяти небажаним повідомленням.
DE.CM-5. Несанкціонований програмний продукт виявлено.	Нормативні посилання: НД ТЗІ 3.6-006-21 – SC-18, SI-4, SC-44. Довідкові посилання: NIST SP 800-53 Rev. 5 – SC-18, SI-4, SC-44.	Організація впроваджує екрановані камери у вигляді демілітаризованої зони в СЕД. Встановлюються обмеження на використання та рекомендації щодо впровадження прийнятних мобільних кодів і технологій мобільного коду. Впроваджуються та проводяться заходи щодо авторизації, відслідковування та контролю використання мобільного коду всередині СЕД.
DE.CM-6. Активність зовнішнього постачальника товарів і послуг відстежується з метою виявлення потенційних кіберінцидентів.	Нормативні посилання: НД ТЗІ 3.6-006-21 – CA-7, PS-7, SA-4, SA-9, SI-4. Довідкові посилання: NIST SP 800-53 Rev. 5 – CA-7, PS-7, SA-4, SA-9, SI-4.	Організація формує та вносить вимоги до стійкості механізму, до забезпечення безпеки та приватності, до документації з безпеки та приватності, до захисту документації з безпеки та приватності при закупівлі СЕД, її системного компонента або системної служби у контрагента. Здійснюється контроль за виявленням несанкціонованого доступу до електронних комунікаційних мереж СЕД при застосуванні зовнішнього документообігу.
DE.CM-7. Моніторинг неавторизованого персоналу, з'єднань, пристроїв і програмного забезпечення проводиться на постійній основі.	Нормативні посилання: НД ТЗІ 3.6-006-21 – AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4. Довідкові посилання:	Організація стежить за доступом співробітників до електронних комунікаційних мереж та СЕД, пристроїв та процесів.

Продовження додатка

1	2	3
	NIST SP 800-53 Rev. 5 – AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4.	
DE.CM-8. Сканування вразливостей виконується.	Нормативні посилання: НД ТЗІ 3.6-006-21 – RA-5. Довідкові посилання: NIST SP 800-53 Rev. 5 – RA-5.	Організація застосовує інструменти та методи сканування вразливості в СЕД, які полегшують сумісність між інструментами, автоматизують частини процесу управління вразливостями, використовуючи існуючі стандарти. Аналізуються звіти про сканування вразливостей СЕД та результати контрольних оцінювань. Використовуються інструменти сканування вразливостей СЕД, які дають можливість легко оновлювати вразливості, що були просканові.

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

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: НД ТЗІ 3.6-006-21 – CA-2, CA-7, PM-14. Довідкові посилання: NIST SP 800-53 Rev. 5 – CA-2, CA-7, PM-14.	В організації визначено обов’язки щодо тестування та моніторингу ризиків в СЕД, забезпечується введення звітності щодо них. Розробляються та перевіряються плани тестування, навчання та моніторингу для узгодженості з організаційною стратегією управління ризиками та загальноорганізаційними пріоритетами дій щодо реагування на ризик в СЕД.
DE.DP-2. Заходи виявлення кіберінцидентів відповідають всім застосованим вимогам.	Нормативні посилання: НД ТЗІ 3.6-006-21 – AC-25, CA-2, CA-7, PM-14, SI-4, SR-9. Довідкові посилання: NIST SP 800-53 Rev. 5 – C-25, CA-2, CA-7,	Організація впроваджує програму захисту від несанкціонованого доступу для СЕД, системного компонента, сервісних модулів або системної служби.

Продовження додатка

1	2	3
	SA-18, SI-4, PM-14.	
DE.DP-3. Процеси виявлення кіберінцидентів протестовані.	Нормативні посилання: НД ТЗІ 3.6-006-21 – CA-2, CA-7, PE-3, PM-14, SI-3, SI-4. Довідкові посилання: NIST SP 800-53 Rev. 5 – CA-2, CA-7, PE-3, PM-14, SI-3, SI-4.	Організація проводить випробування і перевірку ефективності процесів документообігу. Забезпечується періодичне сканування СЕД із частотою не менше одного разу на місяць та постійне сканування файлів із зовнішних джерел у реальному часі.
DE.DP-4. Інформацію про виявлені кіберінциденти повідомлено партнерам організації.	Нормативні посилання: НД ТЗІ 3.6-006-21 – AU-6, CA-2, CA-7, RA-5, SI-4. Довідкові посилання: NIST SP 800-53 Rev. 5 – AU-6, CA-2, CA-7, RA-5, SI-4.	Організація забезпечує перегляд та аналіз записів системного аудиту в СЕД для виявлення кіберінцидентів та інформування контрагентів та партнерів організації.
DE.DP-5. Процеси виявлення кіберінцидентів постійно вдосконалюються.	Нормативні посилання: НД ТЗІ 3.6-006-21 – CA-2, CA-7, PL-2, PM-14, RA-5, SI-4. Довідкові посилання: NIST SP 800-53 Rev. 5 – CA-2, CA-7, PL-2, RA-5, SI-4, PM-14.	Організація переглядає план захисту інформації та персональних даних в СЕД з певною частотою та оновлює зміни, які відбулися в СЕД й у робочому середовищі. План захисту інформації та персональних даних у СЕД переглядається та оновлюється відповідно до проблем, виявлених у ході реалізації або оцінювання заходів безпеки та приватності.

4. Клас заходів кіберзахисту RS – Реагування на кіберінциденти

4.1. Категорія заходів кіберзахисту RS.RP – Планування реагування

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: НД ТЗІ 3.6-006-21 – CP-2, CP-10, IR-4, IR- 8. Довідкові посилання: NIST SP 800-53 Rev. 5 – CP-2, CP-10, IR-4, IR- 8.	Негайне виконання плану реагування на кіберінциденти, що сталися з документами в СЕД під час або після подій. При зборі даних щодо подій, що сталися з документами в СЕД та аналізі подій (кіберінцидентів),

Продовження додатка

1	2	3
		забезпечується збереженість і цілісність даних.

4.2. Категорія заходів кіберзахисту RS.CO – Комунікації.

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: НД ТЗІ 3.6-006-21 – CP-2, CP-3, IR-3, IR-8. Довідкові посилання: NIST SP 800-53 Rev. 5 – CP-2, CP-3, IR-3, IR-8.	Організація забезпечує навчання користувачів СЕД щодо забезпечення безперервної роботи відповідно до визначених ролей та обов'язків. Під час реагування на кіберінциденти залучаються усі співробітники організації.
RS.CO-2. Факти про кіберінциденти задокументовані та повідомляються відповідно до встановлених критерій.	Нормативні посилання: НД ТЗІ 3.6-006-21 – AU-6, IR-6, IR-8. Довідкові посилання: NIST SP 800-53 Rev. 5 – AU-6, IR-6, IR-8.	Організація вимагає від персоналу негайного інформування про підозрілі інциденти з безпеки та приватності відповідно до спроможностей організації реагувати на інциденти впродовж визначеного організацією періоду часу
RS.CO-3. Здійснюється обмін інформацією про кіберінциденти відповідно до планів реагування.	Нормативні посилання: НД ТЗІ 3.6-006-21 – CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4. Довідкові посилання: NIST SP 800-53 Rev. 5 – CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4.	Організація здійснює обмін інформацією про кіберінциденти відповідно до планів реагування на кіберінциденти з партнерами та контрагентами організації, в якій експлуатується СЕД.
RS.CO-4. Координація з партнерами організації проводиться відповідно до планів реагування.	Нормативні посилання: 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.	Організація виконує план координації з партнерами при забезпеченні безперервної роботи та відновленні функціонування, а також при реагуванні на кіберінциденти в СЕД.
RS.CO-5. З метою досягнення ширшої ситуативної обізнаності щодо стану кібербезпеки здійснюється обмін інформацією із основними	Нормативні посилання: НД ТЗІ 3.6-006-21 – PM-15, SI-5. Довідкові посилання: NIST SP 800-53 Rev. 5 – PM-15, SI-5.	Організація створює контакти між обраними групами та асоціаціями зі спільнотами безпеки та приватності для підтримки ознайомленості з рекомендованими практиками

Продовження додатка

суб'єктами національної системи кібербезпеки та зовнішніми партнерами організації.		безпеки та приватності, техніками та технологіями. Здійснюється обмін інформацією з основними суб'єктами національної системи кібербезпеки та зовнішніми контрагентами при проведенні безперервного моніторингу СЕД.

4.3. Категорія заходів кіберзахисту RS.AN – Аналіз

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: НД ТЗІ 3.6-006-21 – AU-6, CA-7, IR-4, IR-5, PE-6, SI-4. Довідкові посилання: 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 кіберінциденту усвідомлено.	Нормативні посилання: НД ТЗІ 3.6-006-21 – CP-2, IR-4. Довідкові посилання: NIST SP 800-53 Rev. 5 – CP-2, IR-4.	Організація впроваджує в СЕД можливості оброки інцидентів безпеки та приватності відповідно до плану реагування на інциденти, включно з етапами підготовки, виявленням і аналізом, стримуванням, ліквідацією та відновленням.
RS.AN-3. Експертиза проводиться.	Нормативні посилання: НД ТЗІ 3.6-006-21 – AU-7, IR-4. Довідкові посилання: NIST SP 800-53 Rev. 5 – AU-7, IR-4.	Організація забезпечує та реалізовує можливості скорочення записів аудиторських перевірок СЕД і звітів до рівня, який підтримує перевірку, аналіз і звітність аудиту щодо розслідування інцидентів безпеки, а також не змінює оригінальний вміст або час упорядкування записів аудиту.
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 –	Організація забезпечує, щоб класифікація кіберінцидентів проводилася відповідно до плану реагування на кіберінциденти. Збір електронних доказів кіберінцидентів, що сталися в СЕД організації, забезпечено.

Продовження додатка

1	2	3
	4.3.4.5.6; NIST SP 800-53 Rev. 5 – CP-2, IR-4, IR-5, IR-8.	
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 в СЕД. 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, групами та асоціаціями з безпеки, які мають великий досвід роботи з документообігом.

4.4. Категорія заходів кіберзахисту RS.MI – Мінімізація наслідків

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: НД ТЗІ 3.6-006-21 – IR-4. Довідкові посилання: NIST SP 800-53 Rev. 5 – IR-4.	Організація забезпечує, щоб інтенсивність, обсяг і результати діяльності з обробки кіберінцидентів можна було порівняти та передбачити у всій організації з розгорнутою СЕД.
RS.MI-2. Наслідки кіберінцидентів мінімізовано.	Нормативні посилання: НД ТЗІ 3.6-006-21 – IR-4. Довідкові посилання: NIST SP 800-53 Rev. 5 – IR-4.	Організація координує діяльність з обробки кіберінцидентів в СЕД із заходами із забезпечення безперервності функціонування.
RS.MI-3. Вперше виявлені вразливості усунено або задокументовано як прийняті ризики.	Нормативні посилання: 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.	Організація проводить оцінювання ризику, включно з вірогідністю й величиною шкоди від несанкціонованого доступу, використання, розголошення, руйнування, модифікації або знищення СЕД, інформації, яку ця система обробляє, зберігає та

Продовження додатка

		передає, а також будь-якої пов'язаної інформації. Вперше виявлені вразливості усуваються або документуються як прийняті ризики.

4.5. Категорія заходів кіберзахисту RS.IM – Удосконалення

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: 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.	Організація враховує отриманий досвід у планах реагування на кіберінциденти в СЕД.
RS.IM-2. Плани реагування оновлено.	Нормативні посилання: 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.	Організація оновлює план реагування на інциденти та план забезпечення безперервної роботи і відновлення функціонування СЕД.

5. Клас заходів кіберзахисту RC – Відновлення стану кібербезпеки

5.1. Категорія заходів кіберзахисту RC.RP – Планування відновлення

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: НД ТЗІ 3.6-006-21 – CP-10, IR-4, IR-8. Довідкові посилання: NIST SP 800-53 Rev. 5 – CP-10, IR-4, IR-8.	Організація розробляє та виконує план дій стосовно забезпечення безперервної роботи та відновлення функціонування СЕД, він виконується під час або після виникнення кіберінцидентів у СЕД.

Продовження додатка

5.2. Категорія заходів кіберзахисту RC.IM – Удосконалення

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 досвід попередніх кіберінцидентів враховувався в плані дій щодо забезпечення безперервної роботи та відновлення функціонування СЕД.
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.	Організація забезпечує оновлення Плану дій щодо забезпечення безперервної роботи та відновлення функціонування СЕД.

5.3. Категорія заходів кіберзахисту RC.CO – Комунікації

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 організований 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. Інформування користувачів СЕД та її клієнтів здійснюється таким чином, щоб звести до мінімуму потенційний вплив на репутацію організації та довіру.
RC.CO-2. Репутація 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

Продовження додатка

1	2	3
		функціонування електронних комунікаційних мереж та СЕД. 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 відновлення після кіберінцидентів відповідно до плану дій щодо забезпечення безперервної роботи та відновлення функціонування СЕД. Організація забезпечує інформування внутрішніх і зовнішніх партнерів організації про серйозні кіберінциденти.