

Опис заходів з кіберзахисту для ОКІ / ОКП I та II категорій критичності

1. Функція «Управління» (ідентифікатор GV) стосується запровадження контролю за функціонуванням всього циклу управління ризиками, визначення стратегій, політик, ролей та обов'язків, проведення моніторингу щодо управління ризиками кібербезпеки:

у межах категорії «Організаційний контекст» (ідентифікатор GV.OC):

здійснюється розуміння місії (мети функціонування) та її врахування при управлінні ризиками кібербезпеки, описується місія (наприклад, через бачення продуктів та послуг, які надаватиме суб'єкт, маркетинг та стратегії надання послуг), структура та організаційні схеми забезпечення кібербезпеки, визначаються ризики кібербезпеки, які можуть перешкодити функціонуванню суб'єкта відповідно до його мети (ідентифікатор GV.OC-01);

визначаються підрозділи/посадові особи та їхні потреби/очікування від управління ризиками кібербезпеки (наприклад, очікування підвищення ефективності контролю та управління посадових осіб суб'єкта, дотримання правил кібергігієни співробітниками, оптимізація структури та бюджету суб'єкта), а також зовнішні заінтересовані сторони та їхні очікування щодо результатів управління ризиками кібербезпеки, наприклад, очікування клієнтів щодо дотримання конфіденційності, очікування відповідності законодавчих умов договірним умовам (ідентифікатор GV.OC-02);

відстежуються зміни законодавства щодо кіберзахисту та захисту інформації (наприклад, щодо захисту персональних даних, захисту інформації в системах, хмарних обчислень, імплементації норм актів законодавства ЄС та НАТО у сфері кібербезпеки) та дотримання партнерами договірних вимог, визначається стратегія управління ризиками кібербезпеки, узгоджується з правовими, нормативними та договірними вимогами та їх змінами (ідентифікатор GV.OC-03);

у межах категорії «Стратегія управління ризиками кібербезпеки» (ідентифікатор GV.RM):

визначаються та узгоджуються із заінтересованими сторонами цілі управління ризиками кібербезпеки, оновлюються/переглядаються з визначеною частотою короткострокові та довгострокові цілі з управління ризиками кібербезпеки, як частини річного стратегічного планування та в разі значних змін, встановлюються вимірні показники щодо досягнення цілей управління ризиками кібербезпеки (наприклад, управління якістю навчання користувачів, забезпечення захисту систем

управління виробничими процесами, управління вразливостями та оновленнями використовуваного програмного забезпечення, антивірусним захистом, управління ризиками кібербезпеки ланцюга постачання суб'єкту, його елементів та послуг), погоджуються з керівництвом цілі кібербезпеки щодо заходів з управління ризиками кібербезпеки, які використовуються у повсякденній діяльності (ідентифікатор GV.RM-01);

визначається допустимий для суб'єкта рівень ризику кібербезпеки, інформація про який доводиться до відома всіх співробітників та заінтересованих сторін і підтримується в актуальному стані. Визначається належний рівень ризику кібербезпеки, який відповідає очікуванням. Інформація про готовність суб'єкта приймати такий рівень ризику кібербезпеки зазначається у розділі про допустимий рівень ризику. Інформація про готовність суб'єкта до прийняття ризиків кібербезпеки доводиться до відома співробітників та заінтересованих сторін. Встановлюється періодичність уточнення інформації про допустимий рівень ризику кібербезпеки (ідентифікатор GV.RM-02);

діяльність з управління ризиками кібербезпеки та досягнення її цілей об'єднується з іншими ризиками (наприклад, фінансовими, операційними, регуляторними, репутаційними, безпековими), менеджери з управління ризиками кібербезпеки залучаються до планування управління ризиками суб'єкта. Встановлюються критерії для передачі ризиків кібербезпеки на більш високий рівень управління ризиками суб'єкта (ідентифікатор GV.RM-03);

у межах категорії «Ролі, обов'язки та повноваження» (ідентифікатор GV.RR):

визначається посадова особа, яка звітує про ризики кібербезпеки, підтримання культури усвідомлення ризиків, відповідає за її вдосконалення, узгоджує з керівництвом їхні ролі та обов'язки щодо розробки, впровадження та оцінювання виконання стратегії кібербезпеки. Утворюється підрозділ з кіберзахисту, призначається керівник з кіберзахисту або відповідальна особа, до завдань якого належить проведення заходів з управління ризиками кібербезпеки та перевірок щодо розуміння співробітниками своїх повноважень, налагодження координації між особами, відповідальними за управління ризиками кібербезпеки (ідентифікатор GV.RR-01);

забезпечується комунікація, розуміння та дотримання ролей і повноважень щодо управління ризиками, визначаються у політиці та затверджуються ролі та обов'язки з управління ризиками кібербезпеки, включається до посадових обов'язків та доводиться до відома співробітників обов'язковість виконання вимог з кібербезпеки. Затверджуються показники продуктивності для співробітників, які виконують обов'язки з управління ризиками кібербезпеки, проводиться періодичний аналіз продуктивності для її покращення, визначаються обов'язки з кібербезпеки в межах операцій, функцій управління ризиками кібербезпеки та функцій внутрішнього аудиту (ідентифікатор GV.RR-02);

визначаються необхідні ресурси відповідно до стратегії управління ризиками кібербезпеки, ролей, відповідальності та політик, забезпечуються періодичні перевірки щодо наявності необхідних повноважень і розподілу ресурсів (людських, технічних), що відповідають заходам протидії ризику кібербезпеки (ідентифікатор GV.RR-03);

у межах категорії «Політика» (ідентифікатор GV.PO):

створюється, затверджується та поширюється політика управління ризиками кібербезпеки, яка є зрозумілою та враховує цілі, очікування та спрямування керівництва суб'єкта, проводиться періодичний перегляд політики та допоміжних послуг (сервісів) кібербезпеки для їх узгодження з цілями та пріоритетами стратегії управління ризиками кібербезпеки, а також з керівництвом політики кібербезпеки на високому рівні. Доводяться положення політики до відома всіх співробітників під час першого прийому на роботу, щорічно та у разі внесення оновлень до неї (ідентифікатор GV.PO-01);

у межах категорії «Контроль» (ідентифікатор GV.OV):

забезпечується врахування результатів стратегії управління ризиками кібербезпеки для вдосконалення та коригування її напрямів, проводиться аналіз – наскільки стратегія та результати аудиту системи управління ризиками допомогли керівникам приймати рішення та досягати цілей суб'єкта, а також, чи потребує коригування чинна стратегія управління ризиками кібербезпеки щодо усунення чинників, які перешкоджають ефективному функціонуванню суб'єкта та впровадженню інновацій в ньому (ідентифікатор GV.OV-01);

у межах категорії «Управління ризиками ланцюга постачання» (ідентифікатор GV.SC):

розроблюється стратегія, яка відображає цілі програми управління ризиками кібербезпеки ланцюга постачання, включаючи план, політики та процедури, які керують впровадженням і вдосконаленням цієї програми. Політика та процедури доводяться до відома заінтересованих сторін, забезпечується узгодженість між функціями, що сприяють управлінню ризиками кібербезпеки ланцюга постачання, наприклад: кібербезпека, безпека ІТ, юридичний, кадровий та інженерний аспекти (ідентифікатор GV.SC-01);

здійснюється внутрішня та зовнішня координація ролей з кібербезпеки при їх виконанні постачальниками товарів, робіт, послуг, користувачами та партнерами суб'єкта. Визначаються ролі/посадові особи, які відповідають за планування, забезпечення ресурсами та управління ризиками кібербезпеки ланцюга постачання, затверджуються у політиці ролі управління ризиками кібербезпеки ланцюга постачання та відповідальність за них. Створюється матриця відповідальності для визначення посадової особи (групи осіб), відповідальної за виконання заходів з управління ризиками кібербезпеки ланцюга постачання, а також встановлюються механізми проведення консультацій та інформування такої посадової особи (групи осіб). У посадових інструкціях визначаються обов'язки та показники

результативності щодо управління ризиками кібербезпеки ланцюга постачання, проводиться їх періодичне вимірювання, щоб визначити та покращити продуктивність. Розробляється завдання та встановлюється відповідальність для постачальників, користувачів і партнерів щодо допустимих ризиків кібербезпеки ланцюга постачання, які впроваджені в політику суб'єкта та застосовуються у відповідних договорах з постачальниками. Третя сторона повідомляється про ролі та обов'язки з управління ризиками кібербезпеки в ланцюгу постачання, встановлюються правила та протоколи обміну інформацією та звітування між суб'єктом та постачальником (ідентифікатор GV.SC-02);

забезпечується інтеграція управління ризиками ланцюга постачання у сфері кібербезпеки в процеси управління ризиками кібербезпеки суб'єкта, оцінки ризиків та їх вдосконалення, узгоджуються питання кібербезпеки з управлінням ризиками кібербезпеки суб'єкта. Утворюються зведені набори заходів управління ризиками кібербезпеки та управління ризиками кібербезпеки ланцюга постачання. Управління ризиками кібербезпеки ланцюга постачання інтегрується в процеси вдосконалення, доводиться до відома керівництва суб'єкта інформація про ризики кібербезпеки ланцюга постачання та враховуються на рівні управління ризиками суб'єкта (ідентифікатор GV.SC-03);

визначаються вимоги безпеки для постачальників, продуктів і послуг (зокрема, щодо тестування та доведення безпеки продуктів і послуг, що постачаються, протягом їх всього життєвого циклу) відповідно до рівня критичності та потенційного впливу компрометації продуктів та послуг, які ними постачаються. Включаються до договору всі вимоги до кібербезпеки та ланцюга постачання, обов'язкові для виконання третіми сторонами, а також встановлюються механізми перевірки дотримання цих вимог, визначаються правила та протоколи обміну інформацією між суб'єктом, постачальником та субпідрядником. Передбачається, що управління ризиками кібербезпеки щодо включення вимог з безпеки в договір базується на критичності потенційних наслідків у випадку компрометації поставок, визначаються вимоги до безпеки в договорах про рівень обслуговування (SLA) для моніторингу постачальників на предмет прийнятної продуктивності безпеки протягом усього життєвого циклу відносин з постачальниками (у контрактах від постачальників вимагається: розкривати функції, функціональні можливості та вразливості їхніх продуктів і послуг протягом усього терміну служби продукту або терміну обслуговування, надавати та підтримувати актуальний інвентар компонентів для критичних продуктів, зокрема, перелік програмного або апаратного забезпечення). У межах захисту від внутрішніх загроз перевіряються співробітники, у контрактах та інших договорах вказуються права та обов'язки суб'єкта, постачальників та ланцюгів постачання щодо потенційних ризиків кібербезпеки (ідентифікатор GV.SC-05);

забезпечується залучення відповідних постачальників товарів, робіт, послуг та інших третіх сторін до діяльності щодо планування, реагування на кіберінциденти,

кібератаки, кіберзагрози та відновлення після них. Визначаються та використовуються правила та протоколи звітування про заходи реагування на кіберінциденти, кібератаки або кіберзагрози та відновлення, а також статус між суб'єктом та його постачальниками. Визначаються та затверджуються ролі та відповідальність суб'єкта та його постачальників щодо реагування на кіберінциденти, кібератаки або кіберзагрози. Залучаються критичні постачальники до тренувань та симуляцій, визначаються та координуються методи комунікацій та протоколи взаємодії, проводиться спільний розгляд отриманого досвіду. Визначається та забезпечується координація способів кризових комунікацій та протоколів між суб'єктом та критичними постачальниками, проводяться спільні дослідження отриманих результатів навчань з критичними постачальникам (ідентифікатор GV.SC-08);

2. Функція «Ідентифікація» (ідентифікатор ID) забезпечує оцінку реальних і потенційних ризиків кібербезпеки для запобігання та нейтралізації кіберзагроз:

у межах категорії «Управління активами» (ідентифікатор ID.AM):

проводиться інвентаризація для всіх типів обладнання суб'єкта, включаючи пристрої, що взаємодіють між собою за допомогою мережі зв'язку, запроваджується постійний моніторинг суб'єкта кіберзахисту для виявлення нового обладнання та автоматична реєстрація проведених оновлень (ідентифікатор ID.AM-01);

проводиться інвентаризація для всіх типів програмного забезпечення, послуг і систем, якими керує суб'єкт, ідентифікується та документується програмне забезпечення та послуги, у тому числі з відкритим вихідним кодом, користувацькі програми, служби API та хмарні послуги, запроваджується постійний моніторинг всіх платформ, включаючи віртуальні машини, на предмет наявності оновлень для них (ідентифікатор ID.AM-02);

забезпечується підтримка використання авторизованих мережових з'єднань, базових ліній зв'язку та потоків даних у дротових та бездротових мережах суб'єкта, проводиться інвентаризація електронних комунікацій, які їх використовують, між суб'єктом та зовнішніми сторонами, розроблюється структурна схема інформаційних потоків, яка відображає інфраструктуру взаємодії між основними компонентами. У документації, з прив'язкою до кожного порту мережі, протоколу та служби визначається, що вони типово використовуються для авторизованих систем (ідентифікатор ID.AM-03);

забезпечується періодичне проведення інвентаризації послуг, що надаються постачальниками товарів/робіт, ідентифікуються та документуються всі послуги, у тому числі послуги хмарних сервісів IaaS, PaaS SaaS, та інші зовнішні служби додатків. Оновлюються інвентаризаційні дані при використанні нової зовнішньої служби або послуги, щоб забезпечити адекватний моніторинг управління ризиками кібербезпеки (ідентифікатор ID.AM-04);

встановлюються критерії пріоритетів та проводиться розподіл активів за пріоритетністю, враховуючи їх класифікацію, критичність, ресурси, вплив на

суб'єкта, застосовуються критерії для кожного активу та переглядаються періодично або у разі значних змін суб'єкта (ідентифікатор ID.AM-05);

забезпечується управління системами, апаратним та програмним забезпеченням, послугами та даними протягом усього їх життєвого циклу. Виявляється нелегальне використання інформаційних технологій, надлишкових систем, апаратного забезпечення, програмного забезпечення та послуг, які збільшують поверхню атаки суб'єкта, налаштовуються та захищаються системи, апаратне забезпечення, програмне забезпечення та послуги перед їх використанням, оновлюються дані інвентаризації щодо систем, апаратного забезпечення, програмного забезпечення та послуг при їх переміщенні або передачі в межах суб'єкта. Забезпечується безпечне знищення збережених даних відповідно до політики збереження даних суб'єкта, використовуючи передбачений метод знищення, безпечно очищуються сховища даних, коли апаратне забезпечення виводиться з експлуатації, списується, замінюється або відправляється на ремонт чи заміну, визначаються методи знищення паперу, носіїв зберігання та інших фізичних форм зберігання даних (ідентифікатор ID.AM-08);

у межах категорії «Оцінка ризиків кібербезпеки» (ідентифікатор ID.RA):

запроваджується використання технології управління вразливостями для виявлення не налаштованого та неправильно налаштованого програмного забезпечення, проводиться оцінювання архітектури мережі та системи на предмет слабких місць у проектуванні та під час впровадження, які впливають на кібербезпеку. Переглядається, аналізується або тестується програмне забезпечення, розроблене суб'єктом, щоб виявити вразливості в проектуванні, кодуванні та налаштуваннях за замовчуванням, оцінюються об'єкти, що містять критичні обчислювальні активи, на предмет фізичних вразливостей та питань стійкості. Проводиться моніторинг джерел розвідки кіберзагроз для отримання інформації про нові вразливості в продуктах і послугах, переглядаються процеси та процедури на предмет слабких місць, які можуть бути використані для впливу на кібербезпеку (ідентифікатор ID.RA-01);

забезпечується отримання інформації про кіберзагрози та вразливості з платформи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози, з репозиторію інформації про кіберінциденти, інших офіційних джерел. Налаштовуються інструменти та технології кібербезпеки з можливостями виявлення або реагування для безпечного надання та отримання зворотного зв'язку про кіберзагрози. Отримуються консультації від авторитетних третіх сторін щодо поточних суб'єктів загроз та їхньої тактики, методів і процедур. Проводиться моніторинг джерела інформації про кіберзагрози для отримання інформації про типи вразливостей, які можуть мати новітні технології (ідентифікатор ID.RA-02);

визначаються та документуються внутрішні та зовнішні кіберзагрози, використовується кіберрозвідка для підтримки обізнаності про типи загрозливих акторів, які можуть націлюватися на суб'єкт, та їх тактику, методи і процедури.

Виконується пошук загроз для виявлення ознак загрозових акторів у середовищі, реалізуються процеси для ідентифікації внутрішніх суб'єктів загроз (ідентифікатор ID.RA-03);

визначаються та документуються потенційні наслідки та вірогідні загрози, пов'язані з експлуатацією кіберзагроз і вразливостей, забезпечується координованість дій керівників суб'єкта та фахівців з управління ризиками кібербезпеки, щоб оцінити ймовірність і вплив сценаріїв ризиків і зареєструвати їх у реєстрах ризиків. Визначається та обраховується потенційний вплив несанкціонованого доступу до комунікацій суб'єкта, систем і даних, які обробляються цими системами, розглядається потенційний вплив каскадних відмов у взаємопов'язаних системах, враховується потенційний вплив каскадних збоїв для операційних систем (ідентифікатор ID.RA-04);

визначаються заходи реагування на ризики кібербезпеки та встановлюється їх пріоритетність, забезпечується їх відслідковування та комунікацію щодо них. Застосовуються критерії плану управління вразливостями для прийняття, передачі, пом'якшення або уникнення ризику кібербезпеки, або вибору компенсаційних заходів для пом'якшення ризику, проводиться відстеження удосконалення процесів реагування на ризики кібербезпеки (наприклад, за затвердженим планом, який містить основні етапи реагування на ризики, забезпечується ведення реєстру ризиків, надається детальний звіт про реагування). Використовуються результати оцінки ризиків кібербезпеки для прийняття рішення про реагування на ризик і виконання відповідних дій, у пріоритетному порядку інформуються заінтересовані сторони про заплановані заходи реагування на ризик кібербезпеки (ідентифікатор ID.RA-06);

визначаються процеси отримання, аналізу та реагування на опубліковані повідомлення про виявлені вразливості, здійснюється обмін інформацією про вразливості між суб'єктом, постачальниками відповідно до правил і протоколів, визначених у контрактах. Запроваджуються обов'язки щодо перевірки виконання процедур обробки, аналізу впливу та реагування на загрози кібербезпеці, уразливості або розкриття кіберінцидентів постачальниками, клієнтами, партнерами та Адміністрацією Держспецзв'язку, іншими уповноваженими державними організаціями з кібербезпеки (ідентифікатор ID.RA-08);

проводиться перевірка автентичності і цілісності обладнання та програмного забезпечення до їх придбання та використання (ідентифікатор ID.RA-09);

у межах категорії «Удосконалення» (ідентифікатор ID.IM):

визначаються напрями удосконалення за результатами проведеного оцінювання стану кіберзахисту, проводиться самооцінка критично важливих служб, враховуючи поточні загрози та відомі техніки, тактики та процедури. Забезпечується зовнішнє оцінювання/незалежний аудит ефективності програми кібербезпеки суб'єкта, за результатами цих заходів визначаються сфери, які потребують покращення, здійснюється оцінювання відповідності суб'єкта

встановленим для нього/обраних ним вимог з кібербезпеки за допомогою автоматизованих засобів (ідентифікатор ID.IM-01);

розробляється, затверджується, доводиться до відома співробітників, переглядається та удосконалюється план реагування на кіберінциденти, кібератаки, кіберзагрози відповідно до Національного плану реагування на кіберінциденти, кібератаки та кіберзагрози, затвердженого постановою Кабінету Міністрів України від 26 листопада 2025 року № 1533, внутрішні політики кібербезпеки, план кіберзахисту та інші регламентуючі документи. Розробляється план дій у надзвичайних ситуаціях для реагування та відновлення після несприятливих подій, які можуть перешкоджати діяльності (наприклад: викривати конфіденційну інформацію або іншим чином загрожувати місії та функціонуванню суб'єкта), заповнюється інформація щодо контактних осіб та комунікаційних схем, процесів обробки загальних сценаріїв, а також критеріїв для визначення пріоритетів, ескалації та підвищення рівня щодо усіх планів дій у надзвичайних ситуаціях. Створюється план управління вразливостями для визначення та оцінювання всіх типів вразливостей для їх пріоритизації, тестування та внесення до плану реагування на ризики кібербезпеки, план кіберзахисту з урахуванням управління ризиками кібербезпеки (включаючи внесені до них зміни), інформація зазначених планів доводиться до відома відповідальних за їх виконання посадових осіб та заінтересованих сторін. Затверджується, щороку переглядається та, за потреби, оновлюється план кіберзахисту (ідентифікатор ID.IM-04);

3. Функція «Забезпечення захисту» (ідентифікатор PR) забезпечує розроблення та впровадження методів, засобів, процедур кіберзахисту, спрямованих на підтримку сталого та надійного функціонування об'єктів кіберзахисту, удосконалення систем реагування на кіберінциденти, кібератаки, кіберзагрози з урахуванням необхідності забезпечення пропорційності можливостей таких систем реальним і потенційним ризикам кібербезпеки:

у межах категорії «Управління ідентифікацією, автентифікація та контроль доступу» (ідентифікатор PR.AA):

забезпечується керування обліковими даними для авторизованих користувачів, служб і апаратного забезпечення, відстежуються та переглядаються запити на отримання або на розширення існуючих прав доступу для співробітників, підрядників та інших осіб, надається дозвіл за потреби та за погодженням з власниками системи або даних. Видаються, управляються та відкликаються криптографічні сертифікати та ідентифікаційні токени, криптографічні ключі та інші облікові дані, обирається унікальний ідентифікатор для кожного пристрою, забезпечується фізичне маркування авторизованого обладнання ідентифікатором для цілей інвентаризації та обслуговування (ідентифікатор PR.AA-01);

забезпечується автентифікація користувачів, служб та апаратного забезпечення, упроваджується та використовується багатофакторна автентифікація, обмежується мінімальна довжина паролів, PIN-кодів і подібних автентифікаторів,

проводиться періодична повторна автентифікація користувачів, служб і апаратного забезпечення на основі ризику кібербезпеки (наприклад, в архітектурах нульової довіри). Забезпечується доступ уповноважених співробітників до облікових даних під час надзвичайних ситуацій (ідентифікатор PR.AA-03);

визначаються в політиці дозволи доступу, повноваження та авторизації, дотримуючись принципів найменших привілеїв і розподілу обов'язків, керуються ними, застосовуються та переглядаються ці дозволи. Забезпечується перегляд привілеїв логічного та фізичного доступу періодично та щоразу, коли змінюється роль або відбувається звільнення співробітника, або скасовують привілеї, які більше не потрібні. Для прийняття рішення щодо надання доступу до запитуваного ресурсу враховуються атрибути запитувача (наприклад, геолокація, день/час, стан захищеності обладнання, з якого здійснюється доступ, кінцева точка), надаються мінімально необхідні права та привілеї (наприклад, архітектура нульової довіри), проводиться періодичний перегляд привілеїв, пов'язаних з критично важливими функціями діяльності суб'єкта, щоб підтвердити належний розподіл обов'язків (ідентифікатор PR.AA-05);

здійснюється управління та моніторинг фізичного доступу до активів відповідно до ризику кібербезпеки, залучаються співробітники охорони, застосовуються камери спостереження, замки на вході, системи сигналізації та інші технічні засоби контролю перебування та обмеження доступу. Запроваджуються додаткові заходи фізичної безпеки для приміщень, в яких розміщуються активи високого рівня критичності, фізичний супровід відвідувачів у приміщеннях з активами, критичними для її функціонування (ідентифікатор PR.AA-06);

у межах категорії «Обізнаність і навчання з питань кіберзахисту» (ідентифікатор PR.AT):

систематично проводяться інструктажі та тренінги з кібергігієни, а також забезпечуються обізнаність і навченість співробітників таким чином, що вони мали знання та навички для виконання основних завдань щодо ризиків кібербезпеки. Проводяться навчання та тренінги для працівників, підрядників, партнерів, постачальників та інших визначених користувачів непублічних ресурсів суб'єкта для їх обізнаності щодо базових принципів кібербезпеки. Запроваджуються навчання щодо розпізнавання та протидії спробам застосування методів соціальної інженерії та поширених атак, дотримання прийнятних політик безпеки та базових принципів кібергігієни (наприклад, виправлення програмного забезпечення, вибір паролів, захист облікових даних), а також інформування про атаки та підозрілу активність. Доводиться до відома співробітників суб'єкта інформація про наслідки порушення політики кібербезпеки як для окремих користувачів, так і для суб'єкта в цілому, проводиться періодичне оцінювання або перевірка розуміння користувачами основних практик кібербезпеки, встановлюються вимоги щодо щорічного підвищення кваліфікації для покращення існуючих та впровадження нових практик з кібербезпеки (ідентифікатор PR.AT-01);

забезпечується обізнаність і навченість співробітників, які безпосередньо виконують завдання з кібербезпеки, кіберзахисту таким чином, що вони мали знання та навички для виконання встановлених завдань щодо ризиків кібербезпеки. Визначаються посади, які мають доступ до важливих даних суб'єкта, обіймання яких вимагає проходження додаткового навчання з питань кібербезпеки (співробітники з фізичної безпеки, кібербезпеки, фінансовий сектор, керівництво вищого рівня). Проводяться тренінги, навчання та перевіряється рольова обізнаність щодо кібербезпеки для співробітників, які виконують спеціалізовані ролі, а також підрядників, партнерів, постачальників та інших третіх осіб. Запроваджується періодичне оцінювання користувачів щодо розуміння практик кібербезпеки відповідно до їхніх спеціалізованих ролей, встановлюються вимоги стосовно щорічного підвищення кваліфікації для покращення існуючих та впровадження нових практик кібербезпеки (ідентифікатор PR.AT-02);

у межах категорії «Безпека даних» (ідентифікатор PR.DS):

забезпечується конфіденційність, цілісність і доступність даних, що зберігаються в обладнанні систем суб'єкта, запроваджується шифрування, цифрові підписи та криптографічні хеші для захисту конфіденційності та цілісності збережених даних у файлах, базах даних, образах дисків віртуальних машин, образах контейнерів та інших ресурсах. Використовується повне шифрування дисків для захисту даних, що зберігаються на кінцевих пристроях користувачів, та підтвердження цілісності програмного забезпечення шляхом перевірки цифрових підписів. Обмежується використання знімних носіїв для запобігання витоку даних, а знімні носії, що містять незашифровану конфіденційну інформацію, фізично зберігаються у закритих сейфах або файлових шафах (ідентифікатор PR.DS-01);

забезпечується конфіденційність, цілісність і доступність даних, що передаються, застосовується шифрування, цифрові підписи та криптографічні хеші для захисту конфіденційності та цілісності при використанні мережових комунікацій, здійснюється автоматичне шифрування або блокування вихідних електронних листів та інших комунікацій, що містять чутливі дані, залежно від класифікації таких даних. Блокується доступ до особистої електронної пошти, сервісів обміну файлами, зберігання файлів та інших особистих додатків і сервісів комунікації з організаційних систем і мереж, забезпечується запобігання повторному використанню чутливих даних з продуктивних середовищ (наприклад, записи клієнтів) у інженерних, тестових та інших непродуктивних середовищах (ідентифікатор PR.DS-02);

забезпечується конфіденційність, цілісність і доступність даних, що використовуються, до яких є доступ та які обробляються і регулярно оновлюються застосунками, користувачами або пристроями суб'єкта, здійснюється видалення даних, які мають залишитися конфіденційними (наприклад, з процесорів і пам'яті), коли вони не потрібні, забезпечується захист даних від інших користувачів та процесів тієї ж платформи (ідентифікатор PR.DS-10);

забезпечується створення, захист, підтримка та тестування резервних копій даних. Безперервно здійснюється резервне копіювання критичних даних у режимі, наближеному до реального часу, резервне копіювання інших даних проводиться за встановленими графіками, тестування резервних копій та відновлення для всіх типів джерел даних здійснюється принаймні щороку, запроваджується безпечне зберігання визначених резервних копій офлайн та поза межами суб'єкта, у територіально різних місцях, з обмеженням доступу до інформації про геолокацію місць зберігання (ідентифікатор PR.DS-11);

у межах категорії «Безпека платформ» (ідентифікатор PR.PS):

встановлюються та застосовуються методи керування конфігурацією. Встановлюються, тестуються, розгортаються та підтримуються захищені базові конфігурації, які забезпечують виконання політик кібербезпеки суб'єкта та надають лише необхідні можливості (принцип максимально обмеженої функціональності), переглядаються всі налаштування конфігурацій за замовчуванням, які можуть потенційно вплинути на кібербезпеку при встановленні або оновленні програмного забезпечення. Проводиться моніторинг виконуваного програмного забезпечення на предмет виявлення його відхилень від схвалених базових конфігурацій (ідентифікатор PR.PS-01);

створюються записи журналів подій, доступних для постійного моніторингу, налаштовуються всі операційні системи, додатки та сервіси (включаючи хмарні ресурси) для генерації записів у журнали подій. Налаштовуються генератори журналів для безпечного обміну їхніми журналами із системами та службами інфраструктури реєстрації суб'єкта, генератори записів журналів подій – для запису даних, необхідних для архітектури з нульовою довірою (ідентифікатор PR.PS-04);

забороняється встановлення та виконання несанкціонованого програмного забезпечення, перевіряється джерело походження та цілісність нового програмного забезпечення перед його встановленням, налаштовуються платформи на використання лише затверджених служб DNS, які блокують доступ до відомих шкідливих доменів, та на встановлення лише програмного забезпечення, схваленого суб'єктом, налаштовуються платформи для інсталяції лише затвердженого суб'єктом програмного забезпечення (ідентифікатор PR.PS-05);

у межах категорії «Стійкість технологічної інфраструктури» (ідентифікатор PR.IR):

забезпечується захист мережі та середовища від неавторизованого логічного доступу та використання, підтримується логічна сегментація мережі суб'єкта та хмарних платформ відповідно до меж довіри та типів платформ (наприклад, мобільні, гості), дозволяються необхідні комунікації лише між сегментами. Забезпечується логічна сегментація мережі суб'єкта від зовнішніх мереж, з дозволом лише необхідних комунікацій для входу в мережі суб'єкта із зовнішніх мереж. Упроваджується архітектура нульової довіри для забезпечення принципу мінімальних привілеїв під час доступу до ресурсів системи, перевіряється

кібербезпека кінцевих точок перед тим, як їм надано доступ і використання виробничих ресурсів (ідентифікатор PR.IR-01);

реалізуються механізми для досягнення вимог стійкості в нормальних і несприятливих ситуаціях, із запобіганням використання єдиних точок відмови у системах та інфраструктурі. Забезпечується балансування навантаження для збільшення потужності та підвищення надійності, використовуються компоненти з високою доступністю (резервне зберігання, джерела живлення) для підвищення надійності системи (ідентифікатор PR.IR-03);

4. Функція «Виявлення» (ідентифікатор DE) забезпечує проведення ідентифікації, збору та обробки кіберінцидентів, кібератак та кіберзагроз:

у межах категорії «Безперервний моніторинг» (ідентифікатор DE.CM):

проводиться постійний моніторинг мереж і мережевих служб для виявлення потенційно несприятливих подій, забезпечується відстеження мережевих служб (наприклад, DNS, BGP тощо) на наявність небажаних подій, дротових та бездротових мереж – на наявність підключень із неавторизованих кінцевих точок, та моніторинг засобів – на наявність несанкціонованих або шахрайських бездротових мереж. Проводиться порівняльний аналіз фактичних мережевих потоків з базовими лініями, щоб виявити відхилення, та моніторинг мережевих комунікацій – для виявлення змін у положеннях безпеки з метою нульової довіри (ідентифікатор DE.CM-01);

проводиться постійний моніторинг діяльності співробітників і використання ними технологій для виявлення потенційно несприятливих подій, забезпечується використання програмного забезпечення для аналітики поведінки з метою виявлення аномальної активності користувачів, щоб пом'якшити внутрішні загрози. Забезпечується відстеження журналів логічних систем контролю доступу, щоб знайти незвичайні шаблони доступу та невдалі спроби доступу, відстежуються на постійній основі технології обману, включаючи облікові записи користувачів, для будь-якого використання (ідентифікатор DE.CM-03);

проводиться постійний моніторинг діяльності і послуг зовнішнього постачальника товарів, робіт, послуг для виявлення потенційно несприятливих подій, забезпечується відстеження віддаленого та локального адміністрування і технічного обслуговування, які зовнішні постачальники виконують у системах суб'єкта. Забезпечується моніторинг активності надавачів хмарних послуг, постачальників послуг інтернету та інших постачальників послуг на наявність відхилень від очікуваної поведінки (ідентифікатор DE.CM-06);

проводиться постійний моніторинг використання комп'ютерного обладнання та програмного забезпечення, середовища їх виконання та даних для виявлення потенційно несприятливих подій, забезпечується моніторинг електронної пошти, інтернету, обміну файлами, служб спільної роботи та інших поширених векторів атак для виявлення зловмисного програмного забезпечення, фішингу, витоку та крадіжки даних та інших небажаних подій. Забезпечується відстеження спроб

автентифікації, щоб виявити атаки на облікові дані та неавторизоване повторне використання облікових даних, а також відстеження конфігурації програмного забезпечення на наявність відхилень від базових рівнів безпеки. Забезпечується контроль апаратного та програмного забезпечення на наявність ознак втручання, на кінцевих точках забезпечується використання технологій виявлення проблем забезпечення кібербезпеки (наприклад, відсутність патчів, зараження зловмисним програмним забезпеченням, несанкціоноване програмне забезпечення) з метою перенаправлення кінцевих точок в середовище відновлення до надання авторизованого доступу (ідентифікатор DE.CM-09);

у межах категорії «Аналіз несприятливих подій» (ідентифікатор DE.AE):

впроваджується періодичне проведення аналізу потенційно несприятливих подій – система управління інформацією та подіями безпеки або інші інструменти для постійного моніторингу подій у журналі на наявність відомої зловмисної та підозрілої активності. Використовується актуальна інформація про кіберзагрози в інструментах аналізу журналів, щоб підвищити точність виявлення та охарактеризувати суб'єкти загрози, їхні методи та показники компрометації, забезпечується регулярне проведення (вручну) перевірки подій журналу для технологій, які не можна належним чином контролювати за допомогою автоматизації, використовуються інструменти аналізу журналів для створення звітів про свої висновки (ідентифікатор DE.AE-02);

забезпечується передавання інформації про несприятливі події до уповноважених суб'єктів з використанням відповідного інструментарію, використовується спеціалізоване програмне забезпечення для створення та передачі сповіщень до центрів безпеки, служб реагування на кіберінциденти, кібератаки або кіберзагрози та інструментів реагування, забезпечується у будь-який час доступ служб реагування на кіберінциденти, кібератаки або кіберзагрози, а інших уповноважених співробітників – до результатів аналізу журналу. Забезпечується автоматичне створення та призначення сигналів у системі оповіщення, коли виникають певні типи несприятливих подій, та ручне створення і призначення сигналів у системі оповіщення суб'єкта, коли технічний співробітник виявляє ознаки компрометації (ідентифікатор DE.AE-06);

забезпечується збирання, виявлення та аналіз інформації про кіберзагрози та іншої контекстної інформації, а також безпечне надання інформації про кіберзагрози технологіям виявлення, процесам і співробітникам. Забезпечується безпечне надання інформації від інвентаризації активів до технологій виявлення процесів і співробітників, а також швидке отримання та швидкий аналіз інформації про вразливості технологічної інфраструктури від постачальників, третіх сторін і сторонніх консультантів із безпеки (ідентифікатор DE.AE-07);

5. Функція «Реагування» (ідентифікатор RS) забезпечує запобігання кіберінцидентам, кібератакам і кіберзагрозам, належне інформування про них, запобігання негативним наслідкам, їх мінімізація та усунення:

у межах категорії «Управління кіберінцидентами» (ідентифікатор RS.MA):

упроваджується виконання плану реагування на кіберінциденти, кібератаки, кіберзагрози в координації з відповідними третіми сторонами одразу після оголошення кіберінциденту, забезпечується автоматичне виявлення кіберінцидентів, залучається допомога з реагування на кіберінциденти, кібератаки або кіберзагрози на основі аутсорсингу. Призначається керівник з реагування на кожний кіберінцидент, ініціюється виконання додаткових планів кібербезпеки, якщо це необхідно для підтримки реагування на кіберінциденти, кібератаки, кіберзагрози, наприклад, забезпечується безперервне функціонування та аварійне відновлення (ідентифікатор RS.MA-01);

упроваджується таксономія та пріоритизація кіберінцидентів, проводиться аналіз і класифікація кіберінцидентів на основі їх таксономії (наприклад, порушення даних, програми вимагачі, DDoS, компрометація облікового запису). Визначається пріоритетність кіберінцидентів на основі їх масштабу, ймовірного впливу та критичного часу, вибирається стратегія реагування на кіберінциденти, кібератаки або кіберзагрози для активних кіберінцидентів, збалансовується необхідність швидкого відновлення після кіберінциденту з необхідністю спостерігати за зловмисником або проводити більш ретельне розслідування (ідентифікатор RS.MA-03);

у межах категорії «Аналіз кіберінциденту» (ідентифікатор RS.AN):

запроваджується проведення аналізу для встановлення того, що відбулося під час кіберінциденту, та які джерела виникнення кіберінциденту, визначається послідовність подій, що відбулися під час кіберінциденту, та які активи і ресурси були залучені до кожної події; аналізуються вразливості, загрози та суб'єкти загроз, які прямо чи опосередковано залучені до кіберінциденту. Аналізується сам кіберінцидент, щоб знайти основні системні причини, перевіряються будь-які технології шахрайства у кіберпросторі, щоб отримати додаткову інформацію про поведінку зловмисників (ідентифікатор RS.AN-03);

запроваджується запис дій, які виконуються під час розслідування кіберінциденту, та забезпечується цілісність і збереження таких записів, неможливість перезапису дій кожного спеціаліста з реагування на кіберінциденти, кібератаки або кіберзагрози та інших осіб (наприклад, системних адміністраторів, інженерів з кібербезпеки), які виконують завдання з реагування на кіберінциденти. Забезпечується участь особи, яка веде розслідування виникнення кіберінциденту, документує деталі кіберінциденту і несе відповідальність за збереження цілісності документації та джерел задокументованої інформації (ідентифікатор RS.AN-06);

запроваджується здійснення збору, забезпечується цілісність та збереження даних про кіберінциденти та метаданих (наприклад, джерело даних, дата/час збору) на основі процедур поводження та зберігання доказів (ідентифікатор RS.AN-07);

у межах категорії «Звітування про реагування на кіберінциденти, кібератаки, кіберзагрози та комунікація» (ідентифікатор RS.CO):

запроваджується сповіщення внутрішніх і зовнішніх заінтересованих сторін про кіберінциденти, кібератаки, кіберзагрози, дотримуються визначеної процедури оповіщення після виявлення кіберінциденту з порушенням даних, включаючи сповіщення постраждалих клієнтів. Повідомляються ділові партнери і клієнти про кіберінциденти відповідно до вимог контракту, правоохоронні органи та уповноважені органи – про кіберінциденти на основі затверджених критеріїв плану реагування на кіберінциденти, кібератаки, кіберзагрози (ідентифікатор RS.CO-02);

запроваджується надання інформації визначеним внутрішнім і зовнішнім заінтересованим сторонам, забезпечується безпечний обмін інформацією про кіберінциденти, кібератаки, кіберзагрози відповідно до планів кіберзахисту та договорів про обмін інформацією, добровільно поширюється інформація (з видаленням усіх конфіденційних даних) серед центрів обміну та аналізу інформації про спостережувані тактики, техніки та процедури зловмисників. Сповіщається керівництво про випадки зловмисної внутрішньої діяльності, забезпечується їх інформування про статус великих кіберінцидентів та дотримуються визначених у контрактах правил і протоколів щодо обміну інформацією про кіберінциденти між суб'єктом та його постачальниками, забезпечується координація методів комунікації в кризових ситуаціях між суб'єктом та його критично важливими постачальниками (ідентифікатор RS.CO-03);

у межах категорії «Пом'якшення кіберінциденту» (ідентифікатор RS.MI):

забезпечується локалізація кіберінцидентів та автоматичне виконання дій стримування за допомогою технологічних рішень (наприклад, антивірусне програмне забезпечення) та інших технологій (наприклад, операційні системи, пристрої мережевої інфраструктури), які мають функції забезпечення кібербезпеки, надається дозвіл службам реагування на кіберінциденти, кібератаки, кіберзагрози вручну вибирати та виконувати дії стримування, а також третій стороні (наприклад, постачальнику послуг інтернету, постачальнику послуг управління безпекою) – виконувати дії зі стримування від імені суб'єкта. Забезпечується автоматичне перенесення скомпрометованих кінцевих точок у віртуальну локальну мережу (VLAN) для відновлення (ідентифікатор RS.MI-01);

забезпечується ліквідація кіберінцидентів, автоматичне виконання завдань стримування за допомогою впроваджених технологій кіберзахисту та інших технологій, які мають такі функції (наприклад, операційні системи, мережа пристроїв інфраструктури), надається дозвіл службам реагування на кіберінциденти, кібератаки, кіберзагрози вручну вибирати та виконувати дії зі стримування кіберінциденту та дозвіл третій стороні (наприклад, постачальнику послуг управління безпекою) – виконувати дії зі стримування від імені суб'єкта (ідентифікатор RS.MI-02);

6. Функція «Відновлення» (ідентифікатор RC) забезпечує поновлення штатного режиму функціонування об'єктів кіберзахисту після кіберінциденту, кібератаки, відновлення інформації та відомостей у разі їх пошкодження або

видалення, створення умов для проведення розслідування кібератаки та кіберінциденту:

у межах категорії «Виконання плану відновлення після кіберінциденту» (ідентифікатор RC.RP):

забезпечується виконання передбачених планом реагування на кіберінциденти, кібератаки або кіберзагрози заходів щодо відновлення, під час або одразу після їх ініціалізації в ході реагування на кіберінциденти, кібератаки, кіберзагрози, ознайомлюються всі особи, які відповідають за відновлення, про плани відновлення та повноваження, необхідні для виконання кожного з аспекту планів (ідентифікатор RC.RP-01);

забезпечується відбір, визначення обсягу, пріоритетність і виконання заходів з відновлення, обираються дії з відновлення на основі критеріїв, визначених у плані реагування на кіберінциденти, кібератаки та кіберзагрози, і доступних ресурсів, змінюються обрані дії з відновлення на основі переоцінки потреб суб'єкта і ресурсів (ідентифікатор RC.RP-02);

перевіряється цілісність резервних копій та інших ресурсів, які підлягають відновленню, перед їх використанням для відновлення, а також відновлені активи на наявність ознак компрометації, пошкодження файлів та інших питань цілісності активів (ідентифікатор RC.RP-03);

перевіряється робочий стан та цілісність відновлених активів, систем та служб перед їх штатним використанням, а також правильність і адекватність дій з відновлення, вжитих перед запуском відновленої системи в режимі онлайн (ідентифікатор RC.RP-05);

у межах категорії «Комунікація з відновлення після кіберінциденту» (ідентифікатор RC.CO):

забезпечується інформування визначених внутрішніх і зовнішніх заінтересованих сторін про заходи з відновлення та прогрес у відновленні операційних спроможностей. Забезпечується безпечний обмін інформацією про відновлення, включаючи хід відновлення, відповідно до планів реагування на кіберінциденти, кібератаки та кіберзагрози та договорів про обмін інформацією, регулярне інформування керівництва вищого рівня про стан відновлення та хід відновлення для великих кіберінцидентів. Дотримуються правил і протоколів, визначених у контрактах між суб'єктом та його постачальниками, щодо обміну інформацією про кіберінциденти, координується кризова комунікація між суб'єктом та його критично важливими постачальниками (ідентифікатор RC.CO-03);

запроваджується інформування суспільства про відновлення після кіберінциденту, кібератаки, використовуючи затверджені методи та повідомлення відповідно до Порядку публічного інформування або звітування про реагування на кіберінциденти, кібератаки, усунення їх наслідків, затвердженого постановою Кабінету Міністрів України від 26 листопада 2025 року № 1533. Забезпечується інформування про кіберінциденти, кібератаки та кіберзагрози безперервно в

режимі, наближеному до реального часу, з використанням платформи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози та механізму «єдиного вікна» для інформування, дотримуються загальних правил обміну інформацією про кіберінциденти, кібератаки, кіберзагрози (протокол TLP), здійснюється публічне інформування про кіберінциденти, кібератаки від середнього рівня критичності і вище; описуються кроки, які вживалися для відновлення після кіберінциденту та запобігання його повторенню (ідентифікатор RC.CO-04).
