ЗАТВЕРДЖЕНО
Наказ Адміністрації Державної служби спеціального зв’язку та захисту інформації України
___ _____ 2026 року № ___

Базові заходи з кіберзахисту

І. Загальні положення

1. Ці Базові заходи з кіберзахисту розроблено відповідно до пункту 2 Загальних вимог з кіберзахисту об’єктів критичної інфраструктури, затверджених постановою Кабінету Міністрів України від 19 червня 2019 року № 518 (в редакції постанови Кабінету Міністрів України від 13 листопада 2025 року № 1470), абзацу четвертого пункту 26 Мінімальних вимог до захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем, затверджених постановою Кабінету Міністрів України від 29 березня 2006 року № 373 (в редакції постанови Кабінету Міністрів України від 26 листопада 2025 року № 1531), та з метою належного здійснення організаційних і технічних заходів з кіберзахисту з урахуванням результатів управління ризиками кібербезпеки.

2. Ці Базові заходи з кіберзахисту розроблено на основі Каталогу заходів з кіберзахисту з урахуванням документа NIST Cybersecurity Framework (CSF) 2.0, виданого у 2024 році Національним інститутом стандартів та технології Сполучених Штатів Америки (National Institute of Standards and Technology), та визначають мінімально необхідну взаємопов’язану сукупність організаційних та технічних заходів з кіберзахисту.

3. Дія цих Базових заходів з кіберзахисту поширюється на органи державної влади, інші державні органи, органи місцевого самоврядування, державні підприємства, установи та організації, які є власниками або розпорядниками інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем (далі – системи), в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, операторів критичної інфраструктури та власників або розпорядників об’єктів критичної інформаційної інфраструктури (далі – суб’єкти) відповідно до Загальних вимог з кіберзахисту об’єктів критичної інфраструктури, затверджених постановою Кабінету Міністрів України від 19 червня 2019 року № 518 (в редакції постанови Кабінету Міністрів України від 13 листопада 2025 року № 1470), Мінімальних вимог до захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем, затверджених постановою Кабінету Міністрів України

від 29 березня 2006 року № 373 (в редакції постанови Кабінету Міністрів України від 26 листопада 2025 року № 1531).

4. Базові заходи з кіберзахисту, наведені в розділах II-V, є обов'язковими для здійснення суб'єктами відповідно до абзацу другого пункту 3 Загальних вимог з кіберзахисту об'єктів критичної інфраструктури, затверджених постановою Кабінету Міністрів України від 19 червня 2019 року № 518 (в редакції постанови Кабінету Міністрів України від 13 листопада 2025 року № 1470), абзацу другого пункту 25 Мінімальних вимог до захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем, затверджених постановою Кабінету Міністрів України від 29 березня 2006 року № 373 (в редакції постанови Кабінету Міністрів України від 26 листопада 2025 року № 1531).

5. Терміни вживаються у значеннях, наведених у Законах України «Про основні засади кібербезпеки України», «Про захист інформації в інформаційно-комунікаційних системах», «Про критичну інфраструктуру», «Про електронні комунікації», «Про Державну службу спеціального зв'язку та захисту інформації України», Положенні про організаційно-технічну модель кіберзахисту, затвердженому постановою Кабінету Міністрів України від 29 грудня 2021 року № 1426, Загальних вимогах з кіберзахисту об'єктів критичної інфраструктури, затверджених постановою Кабінету Міністрів України від 19 червня 2019 року № 518 (в редакції постанови Кабінету Міністрів України від 13 листопада 2025 року № 1470), Національному плані реагування на кіберінциденти, кібератаки та кіберзагрози, затвердженому постановою Кабінету Міністрів України від 26 листопада 2025 року № 1533, Порядку авторизації з безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем, затвердженому постановою Кабінету Міністрів України від 18 червня 2025 року № 712.

II. Базові заходи з кіберзахисту для операторів критичної інфраструктури та власників або розпорядників об'єктів критичної інформаційної інфраструктури I та II категорій критичності

1. УПРАВЛІННЯ (GV): визначення стратегій, політик, ролей та обов'язків, проведення моніторингу щодо управління ризиками кібербезпеки.

1.1. Організаційний контекст (GV.OC): визначення місії, очікування заінтересованих сторін, залежності, нормативних та договірних вимог, яких має дотримуватися суб'єкт у своїй діяльності задля виконання прийнятих рішень щодо управління ризиками кібербезпеки.

1.1.1. **GV.OC-01**: забезпечити розуміння місії суб'єкта та її врахування при управлінні ризиками кібербезпеки.

1.1.2. **GV.OC-02**: визначити внутрішніх та зовнішніх заінтересованих сторін, забезпечити розуміння та врахування їхніх потреб і очікувань щодо управління ризиками.

1.1.3. **GV.OC-03**: визначити та забезпечити виконання співробітниками чинних законодавчих, нормативних та договірних вимог, а також вимог суб'єкта щодо кібербезпеки, включаючи вимоги щодо нерозголошення конфіденційної інформації та захисту прав та свобод.

1.2. Стратегія управління ризиками кібербезпеки (GV.RM): визначення пріоритетів, обмежень, рівнів ризику кібербезпеки, втрат, які суб'єкт може понести, з урахуванням факторів ризику для кожного з видів діяльності, доведення їх до відома заінтересованих сторін для підтримки рішень щодо операційних ризиків.

1.2.1. **GV.RM-01**: визначити та узгодити із заінтересованими сторонами суб'єкта цілі управління ризиками кібербезпеки.

1.2.2. **GV.RM-02**: визначити допустимий рівень ризику кібербезпеки, який суб'єкт може прийняти, довести до відома всіх співробітників та заінтересованих сторін і підтримувати таку інформацію в актуальному стані.

1.2.3. **GV.RM-03**: додати до загальних процесів управління ризиками суб'єкта діяльність з управління ризиками кібербезпеки та досягнення її цілей.

1.3. Ролі, обов'язки та повноваження (GV.RR): визначення та доведення до відома співробітників суб'єкта ролей щодо кібербезпеки, відповідальності, уповноважених суб'єкта для інформування, оцінки ефективності та постійного вдосконалення.

1.3.1. **GV.RR-01**: визначити із числа керівництва суб'єкта посадову особу, яка звітує про ризики кібербезпеки та підтримання культури поведінки щодо усвідомлення ризиків та етики, її постійне вдосконалення, а також відповідає за них.

1.3.2. **GV.RR-02**: встановити, забезпечити комунікацію, розуміння та дотримання ролей та повноважень щодо управління ризиками.

1.3.3. **GV.RR-03**: визначити необхідні ресурси відповідно до стратегії управління ризиками кібербезпеки, ролей, відповідальності та політик.

1.4. Політика (GV.PO): затвердження та сприяння реалізації політики кібербезпеки суб'єкта.

1.4.1. **GV.PO-01**: розробити та довести до відома співробітників суб'єкта політику управління ризиками кібербезпеки, яка визначена з урахуванням структури суб'єкта, стратегії кібербезпеки та пріоритетів.

1.5. Контроль (GV.OV): результати комплексної діяльності з управління ризиками кібербезпеки використовуються для інформування, покращення ефективності та коригування стратегії управління ризиками.

1.5.1. **GV.OV-01:** забезпечити врахування результатів стратегії управління ризиками кібербезпеки для вдосконалення та коригування її напрямів.

1.6. Управління ризиками ланцюга постачання (GV.SC): ідентифікація, визначення, управління, моніторинг виконання процесів управління ризиками кібербезпеки, пов'язаних з ланцюгами постачання, та їх покращення постачальниками товарів, робіт, послуг суб'єкта.

1.6.1. **GV.SC-01**: розробити програму, стратегію, цілі, політики та процеси управління ризиками кібербезпеки, пов'язаними з ланцюгами постачання, погодити їх із заінтересованими сторонами суб'єкта.

1.6.2. **GV.SC-02**: розробити, довести, здійснювати внутрішню та зовнішню координацію ролей з кібербезпеки при їх виконанні постачальниками товарів, робіт, послуг, користувачами та партнерами суб'єкта.

1.6.3. **GV.SC-03**: забезпечити інтеграцію управління ризиками ланцюга постачання у сфері кібербезпеки в процеси управління ризиками кібербезпеки суб'єкта, оцінку ризиків і їх вдосконалення.

1.6.4. **GV.SC-05**: встановити вимоги, пов'язані з ризиками кібербезпеки в ланцюгах постачання, та впровадити їх в договори/контракти або інші типи договорів з постачальниками товарів, робіт, послуг та відповідними третіми сторонами.

1.6.5. **GV.SC-08**: забезпечити залучення відповідних постачальників товарів, робіт, послуг та інших третіх сторін до діяльності щодо планування, реагування на кіберінциденти, кібератаки, кіберзагрози та відновлення після них.

2. ІДЕНТИФІКАЦІЯ (ID): оцінка реальних та потенційних ризиків кібербезпеки для запобігання та нейтралізації кіберзагроз.

2.1. Управління активами (ID.AM): ідентифікація активів (у тому числі даних, програмного забезпечення, систем, засобів, послуг, осіб), які необхідні суб'єкту для досягнення своїх цілей діяльності, та управління ними залежно від їх впливу на цілі суб'єкта та стратегії управління ризиками кібербезпеки.

2.1.1. **ID.AM-01**: забезпечити періодичне проведення інвентаризації обладнання, яким керує суб'єкт.

2.1.2. **ID.AM-02:** забезпечити періодичне проведення інвентаризації програмного забезпечення, послуг і систем, якими керує суб'єкт.

2.1.3. **ID.AM-03:** забезпечити підтримку використання авторизованих мережевих з'єднань та визначити внутрішні і зовнішні мережеві потоки.

2.1.4. **ID.AM-04:** забезпечити періодичне проведення інвентаризації послуг, що надаються постачальниками товарів, робіт, послуг.

2.1.5. **ID.AM-05**: провести розподіл активів за пріоритетністю, враховуючи їх класифікацію, критичність, ресурси, вплив на місію суб'єкта.

2.1.6. **ID.AM-08**: забезпечити управління системами, апаратним та програмним забезпеченням, послугами та даними протягом усього їх життєвого циклу.

2.2. Оцінка ризиків кібербезпеки (ID.RA): усвідомлення суб'єктом ризиків кібербезпеки для нього, його активів і ризиків, які пов'язані з людським фактором.

2.2.1. **ID.RA-01**: ідентифікувати, підтверджувати та вести записи щодо вразливих місць активів.

2.2.2. **ID.RA-02**: організувати отримання інформації про кіберзагрози та вразливості з платформи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози, з репозитарію інформації про кіберінциденти, інших офіційних джерел.

2.2.3. **ID.RA-03**: визначити та задокументувати внутрішні та зовнішні кіберзагрози.

2.2.4. **ID.RA-04**: визначити та задокументувати потенційні наслідки та вірогідні загрози, пов'язані з експлуатацією кіберзагроз та вразливостей.

2.2.5. **ID.RA-06**: визначити заходи реагування на ризики кібербезпеки та встановити їх пріоритетність, забезпечити їх відслідковування та комунікацію щодо них.

2.2.6. **ID.RA-08**: визначити процеси отримання, аналізу та реагування на опубліковані повідомлення про виявлені вразливості.

2.2.7. **ID.RA-09**: проводити перевірку автентичності і цілісності обладнання та програмного забезпечення перед його придбанням і використанням.

2.3. Удосконалення (ID.IM): удосконалення організаційних процесів, процедур і діяльності з управління ризиками кібербезпеки, які визначено у класах заходів кіберзахисту.

2.3.1. **ID.IM-01:** визначити напрями удосконалення за результатами проведеного оцінювання стану кіберзахисту.

2.3.2. **ID.IM-04:** розробити, затвердити, довести до відома співробітників, переглядати та удосконалювати план реагування на кіберінциденти, кібератаки або 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, які впливають на діяльність суб'єкта.

3. ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ (PR): розроблення та впровадження методів, засобів, процедур кіберзахисту, спрямованих на забезпечення 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.

3.1. Управління ідентифікацією, автентифікація та контроль доступу (PR.AA): доступ до фізичних і логічних активів надається лише авторизованим

користувачам, службам та обладнанню та управляється відповідно до оціненого ризику неавторизованого доступу.

3.1.1. **PR.AA-01:** забезпечити на рівні суб'єкта керування обліковими даними для авторизованих користувачів, служб і апаратного забезпечення.

3.1.2. **PR.AA-03:** забезпечити автентифікацію користувачів, служб та апаратного забезпечення.

3.1.3. **PR.AA-05:** визначити в політиці, дотримуючись принципів найменших привілеїв і розподілу обов'язків, дозволи доступу, повноваження та авторизації, керувати ними, застосовувати та переглядати.

3.1.4. **PR.AA-06**: здійснювати управління та моніторинг фізичного доступу до активів відповідно до ризику кібербезпеки.

3.2. Обізнаність і навчання з питань кіберзахисту (PR.AT): суб'єкт здійснює систематичне проведення навчань з питань кіберзахисту для осіб, які в межах своєї компетенції безпосередньо проводять заходи з кіберзахисту.

3.2.1. **PR.AT-01:** систематично проводити інструктажі та тренінги з кібергігієни, а також забезпечити обізнаність і навченість співробітників таким чином, що вони мали знання та навички для виконання основних завдань щодо ризиків кібербезпеки.

3.2.2. **PR.AT-02**: забезпечити обізнаність та навченість співробітників, які безпосередньо виконують завдання із забезпечення кібербезпеки, кіберзахисту таким чином, що вони мали знання та навички для виконання встановлених завдань щодо ризиків кібербезпеки.

3.3. Безпека даних (PR.DS): управління даними здійснюється відповідно до стратегії ризиків кібербезпеки суб'єкта для захисту конфіденційності, цілісності та доступності інформації.

3.3.1. **PR.DS-01**: забезпечити конфіденційність, цілісність і доступність даних, що зберігаються в обладнанні систем суб'єкта.

3.3.2. **PR.DS-02**: забезпечити конфіденційність, цілісність і доступність даних, що передаються.

3.3.3. **PR.DS-10**: забезпечити конфіденційність, цілісність і доступність даних, що використовуються: до яких є доступ; які обробляються та регулярно оновлюються застосунками, користувачами або пристроями суб'єкта.

3.3.4. **PR.DS-11:** забезпечити створення, захист, підтримку та тестування резервних копій даних.

3.4. Безпека платформ (PR.PS): керування апаратним і програмним забезпеченням (наприклад, мікропрограми, операційні системи, застосунки), службами фізичних і віртуальних платформ відповідно до стратегії ризиків кібербезпеки суб'єкта для захисту їх конфіденційності, цілісності та доступності.

3.4.1. **PR.PS-01**: встановити та застосовувати методи керування конфігурацією.

3.4.2. **PR.PS-04**: створити записи журналів подій, які зроблені доступними для постійного моніторингу.

3.4.3. **PR.PS-05**: заборонити встановлення та виконання несанкціонованого програмного забезпечення.

3.5. Стійкість технологічної інфраструктури (PR.IR): керування архітектурою безпеки відповідно до стратегії ризиків кібербезпеки суб'єкта для захисту конфіденційності, цілісності та доступності активів, а також забезпечення стійкості суб'єкта.

3.5.1. **PR.IR-01**: забезпечити захист мережі та середовища від неавторизованого логічного доступу та використання.

3.5.2. **PR.IR-03**: реалізувати механізми для досягнення вимог стійкості в нормальних і несприятливих ситуаціях.

4. ВИЯВЛЕННЯ (DE): проведення ідентифікації, збору та обробки кіберінцидентів, кібератак та кіберзагроз.

4.1. Безперервний моніторинг (DE.CM): моніторинг активів з метою виявлення аномалій, індикаторів компрометації та інших потенційно несприятливих подій у кіберпросторі.

4.1.1. **DE.CM-01:** проводити постійний моніторинг мереж і мережевих служб для виявлення потенційно несприятливих подій.

4.1.2. **DE.CM-03:** проводити постійний моніторинг діяльності співробітників і використання ними технологій для виявлення потенційно несприятливих подій.

4.1.3. **DE.CM-06:** проводити постійний моніторинг діяльності і послуг зовнішнього постачальника товарів, робіт, послуг для виявлення потенційно несприятливих подій.

4.1.4. **DE.CM-09:** проводити постійний моніторинг використання комп'ютерного обладнання та програмного забезпечення, середовища їх виконання та даних для виявлення потенційно несприятливих подій.

4.2. Аналіз несприятливих подій (DE.AE): аналіз аномалій, індикаторів компрометації та інших потенційно несприятливих подій, щоб їх охарактеризувати та виявити кіберінциденти або кібератаки.

4.2.1. **DE.AE-02:** впровадити періодичне проведення аналізу потенційно несприятливих подій для кращого розуміння пов'язаних подій.

4.2.2. **DE.AE-06:** забезпечити передавання інформації про несприятливі події до уповноважених суб'єктів для використання відповідного інструментарію.

4.2.3. **DE.AE-07:** забезпечити збирання, виявлення та аналіз інформації про кіберзагрози та іншої контекстної інформації.

5. РЕАГУВАННЯ (RS): запобігання кіберінцидентам, кібератакам та кіберзагрозам, належне інформування про них, запобігання негативним наслідкам, їх мінімізація та усунення.

5.1. Управління кіберінцидентами (RS.MA): керування процесом реагуванням на виявлені кіберінциденти, кібератаки та кіберзагрози.

5.1.1. **RS.MA-01:** упровадити виконання плану реагування на кіберінциденти, кібератаки або кіберзагрози в координації з відповідними третіми сторонами одразу після оголошення кіберінциденту.

5.1.2. **RS.MA-03:** упровадити таксономію та пріоритизацію кіберінцидентів.

5.2. Аналіз кіберінциденту (RS.AN): проведення розслідувань для забезпечення ефективного реагування на кіберінциденти, кібератаки та кіберзагрози, експертизи кіберінцидентів, а також заходів з відновлення після них.

5.2.1. **RS.AN-03:** запровадити проведення аналізу для встановлення того, що відбулося під час кіберінциденту та які джерела виникнення кіберінциденту.

5.2.2. **RS.AN-06:** запровадити здійснення запису дій, які виконуються під час розслідування кіберінциденту, та забезпечити цілісність і збереження таких записів.

5.2.3. **RS.AN-07**: запровадити здійснення збору та забезпечити цілісність та збереження даних про кіберінциденти та метаданих.

5.3. Звітування про реагування на кіберінциденти, кібератаки, кіберзагрози та комунікація (RS.CO): координація заходів реагування з внутрішніми та зовнішніми заінтересованими сторонами відповідно до законів, нормативних актів або політик.

5.3.1. **RS.CO-02**: запровадити сповіщення внутрішніх та зовнішніх заінтересованих сторін про кіберінциденти, кібератаки та кіберзагрози.

5.3.2. **RS.CO-03:** запровадити надання інформації визначеним внутрішнім і зовнішнім заінтересованим сторонам.

5.4. Пом’якшення кіберінциденту (RS.MI): виконання дій щодо запобігання розширенню подій та пом’якшення їх наслідків.

5.4.1. **RS.MI-01**: забезпечити локалізацію кіберінцидентів.

5.4.2. **RS.MI-02**: забезпечити ліквідацію кіберінцидентів.

6. ВІДНОВЛЕННЯ (RC): 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.

6.1. Виконання плану відновлення після кіберінциденту (RC.RP): проведення відновлювальних заходів для забезпечення доступності систем і служб, які постраждали від кіберінцидентів.

6.1.1. **RC.RP-01**: забезпечити виконання передбачених планом реагування на кіберінциденти, кібератаки або кіберзагрози заходів щодо відновлення одразу

після їх ініціалізації в ході реагування на кіберінциденти, кібератаки та кіберзагрози.

6.1.2. **RC.RP-02**: забезпечити відбір, визначення обсягу, пріоритетність та виконання заходів з відновлення.

6.1.3. **RC.RP-03**: переконатися у цілісності резервних копій та інших ресурсів, які підлягають відновленню, перед їх використанням для відновлення.

6.1.4. **RC.RP-05**: переконатися в цілісності відновлених активів, відновленні систем та служб і підтвердити їх робочий стан.

6.2. Комунікація з відновлення після кіберінциденту (RC.CO): координація заходів щодо відновлення з внутрішніми та зовнішніми сторонами.

6.2.1. **RC.CO-03**: забезпечити інформування визначених внутрішніх і зовнішніх заінтересованих сторін про заходи з відновлення та прогрес у відновленні операційних спроможностей.

6.2.2. **RC.CO-04**: запровадити 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.

III. Базові заходи з кіберзахисту для операторів критичної інфраструктури та власників або розпорядників об’єктів критичної інформаційної інфраструктури III та IV категорій критичності

1. УПРАВЛІННЯ (GV): визначення стратегій, політик, ролей та обов’язків, проведення моніторингу щодо управління ризиками кібербезпеки.

1.1. Організаційний контекст (GV.OC): визначення місії, очікування заінтересованих сторін, залежності, нормативних та договірних вимог, яких має дотримуватися суб’єкт в своїй діяльності задля виконання прийнятих рішень щодо управління ризиками кібербезпеки.

1.1.1. **GV.OC-02**: визначити внутрішніх та зовнішніх заінтересованих сторін, забезпечити розуміння та врахування їхніх потреб і очікувань щодо управління ризиками.

1.1.2. **GV.OC-03**: визначити та забезпечити виконання співробітниками чинних законодавчих, нормативних та договірних вимог, а також вимог суб’єкта щодо кібербезпеки, включаючи вимоги щодо нерозголошення конфіденційної інформації та захисту прав та свобод.

1.2. Стратегія управління ризиками кібербезпеки (GV.RM): визначення пріоритетів, обмежень, рівнів ризику кібербезпеки, втрат, які суб’єкт може понести, з урахуванням факторів ризику для кожного з видів діяльності, доведення їх до відома заінтересованих сторін для підтримки рішень щодо операційних ризиків.

1.2.1. **GV.RM-03**: додати до загальних процесів управління ризиками суб'єкта діяльність з управління ризиками кібербезпеки та досягнення її цілей.

1.3. Ролі, обов'язки та повноваження (GV.RR): визначення та доведення до відома співробітників суб'єкта ролей щодо кібербезпеки, відповідальності, уповноважених суб'єкта для інформування, оцінки ефективності та постійного вдосконалення.

1.3.1. **GV.RR-02**: встановити, забезпечити комунікацію, розуміння та дотримання ролей та повноважень щодо управління ризиками.

1.3.2. **GV.RR-03**: визначити необхідні ресурси відповідно до стратегії управління ризиками кібербезпеки, ролей, відповідальності та політик.

1.4. Політика (GV.PO): затвердження та сприяння реалізації політики кібербезпеки суб'єкта.

1.4.1. **GV.PO-01**: розробити та довести до відома співробітників суб'єкта політику управління ризиками кібербезпеки, яка визначена з урахуванням структури суб'єкта, стратегії кібербезпеки та пріоритетів.

1.5. Управління ризиками ланцюга постачання (GV.SC): ідентифікація, визначення, управління, моніторинг виконання процесів управління ризиками кібербезпеки, пов'язаних з ланцюгами постачання, та їх покращення постачальниками товарів, робіт, послуг суб'єкта.

1.5.1. **GV.SC-05**: встановити вимоги, пов'язані з ризиками кібербезпеки в ланцюгах постачання, та впровадити їх в договори/контракти або інші типи договорів з постачальниками товарів, робіт, послуг та відповідними третіми сторонами.

2. ІДЕНТИФІКАЦІЯ (ID): оцінка реальних і потенційних ризиків кібербезпеки для запобігання та нейтралізації кіберзагроз.

2.1. Управління активами (ID.AM): ідентифікація активів (у тому числі даних, програмного забезпечення, систем, засобів, послуг, осіб), які необхідні суб'єкту для досягнення своїх цілей діяльності, та управління ними залежно від їх впливу на цілі суб'єкта та стратегії управління ризиками кібербезпеки.

2.1.1. **ID.AM-01**: забезпечити періодичне проведення інвентаризації обладнання, яким керує суб'єкт.

2.1.2. **ID.AM-02:** забезпечити періодичне проведення інвентаризації програмного забезпечення, послуг і систем, якими керує суб'єкт.

2.1.3. **ID.AM-03:** забезпечити підтримку використання авторизованих мережевих з'єднань та визначити внутрішні і зовнішні мережеві потоки.

2.1.4. **ID.AM-04:** забезпечити періодичне проведення інвентаризації послуг, що надаються постачальниками товарів, робіт, послуг.

2.1.5. **ID.AM-05**: провести розподіл активів за пріоритетністю, враховуючи їх класифікацію, критичність, ресурси, вплив на місію суб'єкта.

2.1.6. **ID.AM-08**: забезпечити управління системами, апаратним та програмним забезпеченням, послугами та даними протягом усього їх життєвого циклу.

2.2. Оцінка ризиків кібербезпеки (ID.RA): усвідомлення суб'єктом ризиків кібербезпеки для нього, його активів і ризиків, які пов'язані з людським фактором.

2.2.1. **ID.RA-01**: ідентифікувати, підтверджувати та вести записи щодо вразливих місць активів.

2.2.2. **ID.RA-02**: організувати отримання інформації про кіберзагрози та вразливості з платформи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози, з репозитарію інформації про кіберінциденти, інших офіційних джерел.

2.2.3. **ID.RA-03**: визначити та задокументувати внутрішні та зовнішні кіберзагрози.

2.2.4. **ID.RA-06**: визначити заходи реагування на ризики кібербезпеки та встановити їх пріоритетність, забезпечити їх відслідковування та комунікацію щодо них.

2.2.5. **ID.RA-08**: визначити процеси отримання, аналізу та реагування на опубліковані повідомлення про виявлені вразливості.

2.3. Удосконалення (ID.IM): удосконалення організаційних процесів, процедур і діяльності з управління ризиками кібербезпеки, які визначено у класах заходів кіберзахисту.

2.3.1. **ID.IM-01:** визначити напрями удосконалення за результатами проведеного оцінювання стану кіберзахисту.

2.3.2. **ID.IM-04:** розробити, затвердити, довести до відома співробітників, переглядати та удосконалювати план реагування на кіберінциденти, кібератаки або 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, які впливають на діяльність суб'єкта.

3. ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ (PR): розроблення та впровадження методів, засобів, процедур кіберзахисту, спрямованих на забезпечення 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.

3.1. Управління ідентифікацією, автентифікація та контроль доступу (PR.AA): доступ до фізичних і логічних активів надається лише авторизованим користувачам, службам та обладнанню та управляється відповідно до оціненого ризику неавторизованого доступу.

3.1.1. **PR.AA-01:** забезпечити на рівні суб’єкта керування обліковими даними для авторизованих користувачів, служб і апаратного забезпечення.

3.1.2. **PR.AA-03:** забезпечити автентифікацію користувачів, служб та апаратного забезпечення.

3.1.3. **PR.AA-06**: здійснювати управління та моніторинг фізичного доступу до активів відповідно до ризику кібербезпеки.

3.2. Обізнаність і навчання з питань кіберзахисту (PR.AT): суб’єкт здійснює систематичне проведення навчань з питань кіберзахисту для осіб, які в межах своєї компетенції безпосередньо проводять заходи з кіберзахисту.

3.2.1. **PR.AT-01:** систематично проводити інструктажі та тренінги з кібергігієни, а також забезпечити обізнаність і навченість співробітників таким чином, що вони мали знання та навички для виконання основних завдань щодо ризиків кібербезпеки.

3.2.2. **PR.AT-02**: забезпечити обізнаність та навченість співробітників, які безпосередньо виконують завдання із забезпечення кібербезпеки, кіберзахисту таким чином, що вони мали знання та навички для виконання встановлених завдань щодо ризиків кібербезпеки.

3.3. Безпека даних (PR.DS): управління даними здійснюється відповідно до стратегії ризиків кібербезпеки суб’єкта для захисту конфіденційності, цілісності та доступності інформації.

3.3.1. **PR.DS-01**: забезпечити конфіденційність, цілісність і доступність даних, що зберігаються в обладнанні систем суб’єкта.

3.3.2. **PR.DS-11:** забезпечити створення, захист, підтримку та тестування резервних копій даних.

3.4. Безпека платформ (PR.PS): керування апаратним і програмним забезпеченням (наприклад, мікропрограми, операційні системи, застосунки), службами фізичних і віртуальних платформ відповідно до стратегії ризиків кібербезпеки суб’єкта для захисту їх конфіденційності, цілісності та доступності.

3.4.1. **PR.PS-01**: встановити та застосовувати методи керування конфігурацією.

3.4.2. **PR.PS-04**: створити записи журналів подій, які зроблені доступними для постійного моніторингу.

3.4.3. **PR.PS-05**: заборонити встановлення та виконання несанкціонованого програмного забезпечення.

3.5. Стійкість технологічної інфраструктури (PR.IR): керування апаратним і програмним забезпеченням (наприклад, мікропрограми, операційні системи, застосунки), службами фізичних і віртуальних платформ відповідно до стратегії ризиків кібербезпеки суб’єкта для захисту їх конфіденційності, цілісності та доступності.

3.5.1. **PR.IR-01:** встановити та застосовувати методи керування конфігурацією.

4. ВИЯВЛЕННЯ (DE): проведення ідентифікації, збору та обробки кіберінцидентів, кібератак та кіберзагроз.

4.1. Безперервний моніторинг (DE.CM): моніторинг активів з метою виявлення аномалій, індикаторів компрометації та інших потенційно несприятливих подій в кіберпросторі.

4.1.1. **DE.CM-01:** проводити постійний моніторинг мереж і мережевих служб для виявлення потенційно несприятливих подій.

4.1.2. **DE.CM-09:** проводити постійний моніторинг використання комп'ютерного обладнання та програмного забезпечення, середовища їх виконання та даних для виявлення потенційно несприятливих подій.

4.2. Аналіз несприятливих подій (DE.AE): аналіз аномалій, індикаторів компрометації та інших потенційно несприятливих подій, щоб їх охарактеризувати та виявити кіберінциденти або кібератаки.

4.2.1. **DE.AE-02:** впровадити періодичне проведення аналізу потенційно несприятливих подій для кращого розуміння пов'язаних подій.

4.2.2. **DE.AE-06:** забезпечити передавання інформації про несприятливі події до уповноважених суб'єктів для використання відповідного інструментарію.

4.2.3. **DE.AE-07:** забезпечити збирання, виявлення та аналіз інформації про кіберзагрози та іншої контекстної інформації.

5. РЕАГУВАННЯ (RS): запобігання кіберінцидентам, кібератакам та кіберзагрозам, належне інформування про них, запобігання негативним наслідкам, їх мінімізація та усунення.

5.1. Управління кіберінцидентами (RS.MA): керування процесом реагуванням на виявлені кіберінциденти, кібератаки та кіберзагрози.

5.1.1. **RS.MA-01:** упровадити виконання плану реагування на кіберінциденти, кібератаки або кіберзагрози в координації з відповідними третіми сторонами одразу після оголошення кіберінциденту.

5.2. Аналіз кіберінциденту (RS.AN): проведення розслідувань для забезпечення ефективного реагування на кіберінциденти, кібератаки та кіберзагрози, експертизи кіберінцидентів, а також заходів з відновлення після них.

5.2.1. **RS.AN-03:** запровадити проведення аналізу для встановлення того, що відбулося під час кіберінциденту та які джерела виникнення кіберінциденту.

5.2.2. **RS.AN-07**: запровадити здійснення збору та забезпечити цілісність та збереження даних про кіберінциденти та метаданих.

5.3. Звітування про реагування на кіберінциденти, кібератаки, кіберзагрози та комунікація (RS.CO): координація заходів реагування з

внутрішніми та зовнішніми заінтересованими сторонами відповідно до законів, нормативних актів або політик.

5.3.1. **RS.CO-02**: запровадити сповіщення внутрішніх та зовнішніх заінтересованих сторін про кіберінциденти, кібератаки та кіберзагрози.

5.4. Пом'якшення кіберінциденту (RS.MI): виконання дій щодо запобігання розширенню подій та пом'якшення їх наслідків.

5.4.1. **RS.MI-02**: забезпечити ліквідацію кіберінцидентів.

6. ВІДНОВЛЕННЯ (RC): 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.

6.1. Виконання плану відновлення після інциденту (RC.RP): проведення відновлювальних заходів для забезпечення доступності систем і служб, які постраждали від кіберінцидентів.

6.1.1. **RC.RP-01:** забезпечити виконання передбачених планом реагування на кіберінциденти, кібератаки або кіберзагрози заходів щодо відновлення одразу після їх ініціалізації в ході реагування на кіберінциденти, кібератаки та кіберзагрози.

6.1.2. **RC.RP-03:** переконатися у цілісності резервних копій та інших ресурсів, які підлягають відновленню, перед їх використанням для відновлення.

6.2. Комунікація з відновлення після кіберінциденту (RC.CO): координація заходів щодо відновлення з внутрішніми та зовнішніми сторонами.

6.2.1. **RC.CO-03**: забезпечити інформування визначених внутрішніх і зовнішніх заінтересованих сторін про заходи з відновлення та прогрес у відновленні операційних спроможностей.

IV. Базові заходи з кіберзахисту для органів державної влади, інших державних органів, органів місцевого самоврядування, державних підприємств, установ та організацій, які є власниками або розпорядниками систем, в яких обробляються державні інформаційні ресурси

1. УПРАВЛІННЯ (GV): визначення стратегій, політик, ролей та обов'язків, проведення моніторингу щодо управління ризиками кібербезпеки.

1.1. Організаційний контекст (GV.OC): визначення місії, очікування заінтересованих сторін, залежності, нормативних та договірних вимог, яких має дотримуватися суб'єкт в своїй діяльності задля виконання прийнятих рішень щодо управління ризиками кібербезпеки.

1.1.1. **GV.OC-03**: визначити та забезпечити виконання співробітниками чинних законодавчих, нормативних та договірних вимог, а також вимог суб'єкта

щодо кібербезпеки, включаючи вимоги щодо нерозголошення конфіденційної інформації та захисту прав та свобод.

1.2. Стратегія управління ризиками кібербезпеки (GV.RM): визначення пріоритетів, обмежень, рівнів ризику кібербезпеки, втрат, які суб'єкт може понести, з урахуванням факторів ризику для кожного з видів діяльності, доведення їх до відома заінтересованих сторін для підтримки рішень щодо операційних ризиків.

1.2.1. **GV.RM-03:** додати до загальних процесів управління ризиками суб'єкта діяльність з управління ризиками кібербезпеки та досягнення її цілей.

1.3. Політика (GV.PO): затвердження та сприяння реалізації політики кібербезпеки суб'єкта.

1.3.1. **GV.PO-01:** розробити та довести до відома співробітників суб'єкта політику управління ризиками кібербезпеки, яка визначена з урахуванням структури суб'єкта, стратегії кібербезпеки та пріоритетів.

1.4. Управління ризиками ланцюга постачання (GV.SC): ідентифікація, визначення, управління, моніторинг виконання процесів управління ризиками кібербезпеки, пов'язаних з ланцюгами постачання, та їх покращення постачальниками товарів, робіт, послуг суб'єкта.

1.4.1. **GV.SC-01**: розробити програму, стратегію, цілі, політики та процеси управління ризиками кібербезпеки, пов'язаними з ланцюгами постачання, погодити їх із заінтересованими сторонами суб'єкта.

2. ІДЕНТИФІКАЦІЯ (ID): оцінка реальних і потенційних ризиків кібербезпеки для запобігання та нейтралізації кіберзагроз.

2.1. Управління активами (ID.AM): ідентифікація активів (у тому числі даних, програмного забезпечення, систем, засобів, послуг, осіб), які необхідні суб'єкту для досягнення своїх цілей діяльності, та управління ними залежно від їх впливу на цілі суб'єкта та стратегії управління ризиками кібербезпеки.

2.1.1. **ID.AM-01**: забезпечити періодичне проведення інвентаризації обладнання, яким керує суб'єкт.

2.1.2. **ID.AM-02:** забезпечити періодичне проведення інвентаризації програмного забезпечення, послуг і систем, якими керує суб'єкт.

2.1.3. **ID.AM-05**: провести розподіл активів за пріоритетністю, враховуючи їх класифікацію, критичність, ресурси, вплив на місію суб'єкта.

2.1.4. **ID.AM-08:** забезпечити управління системами, апаратним та програмним забезпеченням, послугами та даними протягом усього їх життєвого циклу.

2.2. Оцінка ризиків кібербезпеки (ID.RA): усвідомлення суб'єктом ризиків кібербезпеки для нього, його активів і ризиків, які пов'язані з людським фактором.

2.2.1. **ID.RA-01:** ідентифікувати, підтверджувати та вести записи щодо вразливих місць активів**.**

3. ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ (PR): розроблення та впровадження методів, засобів, процедур кіберзахисту, спрямованих на забезпечення 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.

3.1. Управління ідентифікацією, автентифікація та контроль доступу (PR.AA): доступ до фізичних і логічних активів надається лише авторизованим користувачам, службам та обладнанню та управляється відповідно до оціненого ризику неавторизованого доступу.

3.1.1. **PR.AA-01:** забезпечити на рівні суб'єкта керування обліковими даними для авторизованих користувачів, служб і апаратного забезпечення.

3.1.2. **PR.AA-03:** забезпечити автентифікацію користувачів, служб та апаратного забезпечення.

3.1.3. **PR.AA-05:** визначити в політиці, дотримуючись принципів найменших привілеїв і розподілу обов'язків, дозволи доступу, повноваження та авторизації, керувати ними, застосовувати та переглядати.

3.1.4. **PR.AA-06**: здійснювати управління та моніторинг фізичного доступу до активів відповідно до ризику кібербезпеки.

3.2. Обізнаність і навчання з питань кіберзахисту (PR.AT): суб'єкт здійснює систематичне проведення навчань з питань кіберзахисту для осіб, які в межах своєї компетенції безпосередньо проводять заходи з кіберзахисту.

3.2.1. **PR.AT-01:** систематично проводити інструктажі та тренінги з кібергігієни, а також забезпечити обізнаність і навченість співробітників таким чином, що вони мали знання та навички для виконання основних завдань щодо ризиків кібербезпеки.

3.3. Безпека даних (PR.DS): управління даними здійснюється відповідно до стратегії ризиків кібербезпеки суб'єкта для захисту конфіденційності, цілісності та доступності інформації.

3.3.1. **PR.DS-01:** забезпечити конфіденційність, цілісність і доступність даних, що зберігаються в обладнанні систем суб'єкта.

3.3.2. **PR.DS-11:** забезпечити створення, захист, підтримку та тестування резервних копій даних.

3.4. Безпека платформ (PR.PS): керування апаратним і програмним забезпеченням (наприклад, мікропрограми, операційні системи, застосунки), службами фізичних і віртуальних платформ відповідно до стратегії ризиків кібербезпеки суб'єкта для захисту їх конфіденційності, цілісності та доступності.

3.4.1. **PR.PS-04:** створити записи журналів подій, які зроблені доступними для постійного моніторингу.

3.4.2. **PR.PS-05:** заборонити встановлення та виконання несанкціонованого програмного забезпечення.

3.5. Стійкість технологічної інфраструктури (PR.IR): керування архітектурою безпеки відповідно до стратегії ризиків кібербезпеки суб'єкта для захисту конфіденційності, цілісності та доступності активів, а також забезпечення стійкості суб'єкта.

3.5.1. **PR.IR-01:** забезпечити захист мережі та середовища від неавторизованого логічного доступу та використання.

4. ВИЯВЛЕННЯ (DE): проведення ідентифікації, збору та обробки кіберінцидентів, кібератак та кіберзагроз.

4.1. Безперервний моніторинг (DE.CM): моніторинг активів з метою виявлення аномалій, індикаторів компрометації та інших потенційно несприятливих подій в кіберпросторі.

4.1.1. **DE.CM-01:** проводити постійний моніторинг мереж і мережевих служб для виявлення потенційно несприятливих подій.

5. РЕАГУВАННЯ (RS): запобігання кіберінцидентам, кібератакам та кіберзагрозам, належне інформування про них, запобігання негативним наслідкам, їх мінімізація та усунення.

5.1. Управління кіберінцидентами (RS.MA): керування процесом реагуванням на виявлені кіберінциденти, кібератаки та кіберзагрози.

5.1.1. **RS.MA-01:** упровадити виконання плану реагування на кіберінциденти, кібератаки або кіберзагрози в координації з відповідними третіми сторонами одразу після оголошення кіберінциденту.

5.2. Звітування про реагування на кіберінциденти, кібератаки, кіберзагрози та комунікація (RS.CO): координація заходів реагування з внутрішніми та зовнішніми заінтересованими сторонами відповідно до законів, нормативних актів або політик.

5.2.1. **RS.CO-02**: запровадити сповіщення внутрішніх та зовнішніх заінтересованих сторін про кіберінциденти, кібератаки та кіберзагрози.

6. ВІДНОВЛЕННЯ (RC): 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.

6.1. Виконання плану відновлення після кіберінциденту (RC.RP): проведення відновлювальних заходів для забезпечення доступності систем і служб, які постраждали від кіберінцидентів.

6.1.1. **RC.RP-01:** забезпечити виконання передбачених планом реагування на кіберінциденти, кібератаки або кіберзагрози заходів щодо відновлення одразу після їх ініціалізації в ході реагування на кіберінциденти, кібератаки та кіберзагрози.

V. Базові заходи з кіберзахисту для органів державної влади, інших державних органів, органів місцевого самоврядування, державних підприємств, установ та організацій, які є власниками або розпорядниками систем, в яких обробляється інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом

1. УПРАВЛІННЯ (GV): визначення стратегій, політик, ролей та обов'язків, проведення моніторингу щодо управління ризиками кібербезпеки.

1.1. Стратегія управління ризиками кібербезпеки (GV.RMвизначення пріоритетів, обмежень, рівнів ризику кібербезпеки, втрат, які суб'єкт може понести, з урахуванням факторів ризику для кожного з видів діяльності, доведення їх до відома заінтересованих сторін для підтримки рішень щодо операційних ризиків.

1.1.1. **GV.RM-03**: додати до загальних процесів управління ризиками суб'єкта діяльність з управління ризиками кібербезпеки та досягнення її цілей.

1.2. Управління ризиками ланцюга постачання (GV.SC): ідентифікація, визначення, управління, моніторинг виконання процесів управління ризиками кібербезпеки, пов'язаних з ланцюгами постачання, та їх покращення постачальниками товарів, робіт, послуг суб'єкта.

1.2.1. **GV.SC-01**: розробити програму, стратегію, цілі, політики та процеси управління ризиками кібербезпеки, пов'язаними з ланцюгами постачання, погодити їх із заінтересованими сторонами суб'єкта.

2. ІДЕНТИФІКАЦІЯ (ID): оцінка реальних і потенційних ризиків кібербезпеки для запобігання та нейтралізації кіберзагроз.

2.1. Управління активами (ID.AM): ідентифікація активів (у тому числі даних, програмного забезпечення, систем, засобів, послуг, осіб), які необхідні суб'єкту для досягнення своїх цілей діяльності, та управління ними залежно від їх впливу на цілі суб'єкта та стратегії управління ризиками кібербезпеки.

2.1.1. **ID.AM-01**: забезпечити періодичне проведення інвентаризації обладнання, яким керує суб'єкт.

2.1.2. **ID.AM-02:** забезпечити періодичне проведення інвентаризації програмного забезпечення, послуг і систем, якими керує суб'єкт.

2.1.3. **ID.AM-05**: провести розподіл активів за пріоритетністю, враховуючи їх класифікацію, критичність, ресурси, вплив на місію суб'єкта.

3. ВИЯВЛЕННЯ (DE): проведення ідентифікації, збору та обробки кіберінцидентів, кібератак та кіберзагроз.

3.1. Аналіз несприятливих подій (DE.AE): аналіз аномалій, індикаторів компрометації та інших потенційно несприятливих подій, щоб їх охарактеризувати та виявити кіберінциденти або кібератаки.

3.1.1. **DE.AE-06:** забезпечити передавання інформації про несприятливі події до уповноважених суб'єктів для використання відповідного інструментарію.

Т.в.о. директора Департаменту кіберзахисту
Адміністрації Держспецзв'язку Дмитро ПАХОЛЬЧЕНКО