ЗАТВЕРДЖЕНО

Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України
___ _____ 2025 року № ___

Базові заходи з кіберзахисту

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

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

1.1.1. **GV.OC-01**: забезпечити усвідомлення органами державної влади, підприємствами, установами, організаціями будь-якої форми власності, юридичною та/або фізичною особою, якому/якій на правах власності, оренди або на інших законних підставах належить об'єкт кіберзахисту або який/яка відповідає за його поточне функціонування (далі – організація), які здійснюють управління ризиками кібербезпеки, місії організації.

1.1.2. **GV.OC-02**: внутрішні та зовнішні заінтересовані сторони усвідомили, а їхні потреби та очікування від впровадження управління ризиками кібербезпеки визначені та впроваджені.

1.1.3. **GV.OC-03**: визначити та забезпечити виконання персоналом існуючих законодавчих, нормативних та договірних вимог, а також вимог організації щодо кібербезпеки, включаючи вимоги щодо нерозголошення конфіденційної інформації та захисту прав та свобод.

1.1.4. **GV.OC-04**: визначити ключові цілі, критичні послуги та спроможності, які очікуються постачальниками від організації, що доведені та усвідомлені її персоналом.

1.1.5. **GV.OC-05**: визначити наслідки, спроможності та послуги, від яких залежить діяльність організації, довести та забезпечити їх усвідомлення персоналом.

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

1.2.1. **GV.RM-01**: визначити та узгодити із заінтересованими сторонами організації цілі управління ризиками.

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

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

1.2.4. **GV.RM-04**: визначити та довести до відома персоналу стратегічні напрями, які описують відповідні варіанти реагування на ризики.

1.2.5. **GV.RM-05**: визначити та довести до відома персоналу способи обміну інформацією всередині організації щодо ризиків кібербезпеки, включаючи ризики, які несуть постачальники та інші треті сторони.

1.2.6. **GV.RM-06**: визначити та довести до відома персоналу стандартизовані методи розрахунку, документування, ідентифікації та визначення пріоритетності ризиків кібербезпеки.

1.2.7. **GV.RM-07**: визначити, охарактеризувати та забезпечувати обговорення зі співробітниками організації стратегічних можливостей щодо управління ризиками кібербезпеки.

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

1.3.1. **GV.RR-01**: визначити із числа керівництва організації 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**: визначити ролі, відповідальність та державні органи (підрозділи), залучені до управління ризиками кібербезпеки, забезпечити їх розуміння персоналом і здійснювати контроль за їх дотриманням.

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

1.3.4. **GV.RR-04**: додати кібербезпеку до практик управління людськими ресурсами.

1.4. **Політика (GV.PO):** затвердження, доведення та сприяння реалізації політики кібербезпеки організації.

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

1.4.2. **GV.PO-02**: забезпечити періодичний перегляд, оновлення, доведення та виконання політики управління ризиками кібербезпеки з урахуванням змін нормативних вимог, загроз, технологій та місії організації.

1.5. **Контроль (GV.OV):** використання результатів комплексної діяльності з управління ризиками кібербезпеки здійснюється 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.

1.5.2. **GV.OV-02**: забезпечити перегляд та коригування стратегії управління ризиками кібербезпеки для забезпечення охоплення нею вимог організації та ризиків.

1.5.3. **GV.OV-03**: забезпечити оцінювання продуктивності управління ризиками кібербезпеки для перегляду, внесення необхідних коригувань відповідно до поточних потреб.

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 організації.

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 організації.

1.6.2. **GV.SC-02**: розробити, довести, здійснювати внутрішню та зовнішню координацію ролей з кібербезпеки при їх виконанні постачальниками, користувачами та партнерами організації.

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

1.6.4. **GV.SC-04**: визначити та пріоритизувати постачальників за ступенем критичності.

1.6.5. **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 та відповідними третіми сторонами.

1.6.6. **GV.SC-06**: забезпечити планування та комплексну перевірку постачальників або інших третіх сторін для зменшення ризиків перед початком договірних відносин з ними.

1.6.7. **GV.SC-07**: визначити ризики, пов'язані з постачальником, його продукцією та послугами, які він надає, з іншими третіми сторонами, усвідомити їх, зареєструвати, пріоритизувати та забезпечити реагування на них і контроль протягом всієї співпраці.

1.6.8. **GV.SC-08**: забезпечити залучення відповідних постачальників та інших третіх сторін до діяльності щодо планування, реагування та відновлення після інцидентів.

1.6.9. **GV.SC-09**: інтегрувати практичні заходи щодо забезпечення безпеки ланцюга постачання в програми організації щодо кібербезпеки та управління ризиками, контролювати їх ефективність протягом всього життєвого циклу

користування продуктами та послугами, які суб’єкт отримує від постачальника чи інших третіх сторін.

1.6.10. **GV.SC-10**: передбачити в планах управління ризиками кібербезпеки, пов’язаними з ланцюгами постачання, порядок дій, які необхідно виконати після прийняття рішення щодо партнерства або укладання договору про надання послуг.

2. ІДЕНТИФІКАЦІЯ (ID): оцінка реальних та потенційних ризиків у сфері 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 організації для досягнення своїх цілей діяльності, та управління ними залежно від їх впливу на цілі організації та стратегії управління ризиками.

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

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

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.

2.1.5. **ID.AM-05**: здійснити пріоритизацію активів за їх класифікацією, критичністю, ресурсами, впливом на місію організації.

2.1.6. **ID**.**AM-07**: забезпечити інвентаризацію даних і пов'язаних з ними метаданих відповідно до визначених типів даних.

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

2.2. **Оцінка ризиків (ID.RA):** усвідомлення всією організацією ризиків кібербезпеки для неї, її 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 загрози безпеки та вразливості з форумів обміну інформацією та офіційних джерел.

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

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

2.2.5. **ID.RA-05**: забезпечити використання інформації про вірогідні загрози, вразливості та можливі наслідки від їх настання для розуміння невід'ємного ризику та інформування про пріоритетність реагування на ризики.

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

2.2.7. **ID.RA-07**: забезпечити управління, оцінювання на предмет ризику, реєстрацію та відстеження змін та винятків до затвердженої документації.

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

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

2.2.10. **ID.RA-10**: забезпечити проведення оцінювання постачальників перед придбанням у них критично важливих для організації продуктів і послуг.

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-02:** визначити напрями удосконалення за результатами тестування безпеки та навчальних вправ, включаючи їх виконання у взаємодії з постачальниками та відповідними третіми сторонами.

2.3.3. **ID.IM-03:** визначати покращення під час виконання операційних процесів, процедур і дій.

2.3.4. **ID.IM-04:** розробити, затвердити, довести до відома персоналу, переглядати та удосконалювати Плани реагування на інциденти та інші плани кібербезпеки, які впливають на діяльність організації.

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 та кібератаки з урахуванням необхідності забезпечення пропорційності та/або співрозмірності можливостей таких систем реальним та потенційним ризикам.

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 організації керування суб'єктами та їх обліковими даними для авторизованих користувачів, служб і апаратного забезпечення.

3.1.2. **PR.AA-02:** забезпечити підтвердження ідентичності користувачів та їх відповідність обліковим записам на основі умов взаємодії.

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

3.1.4. **PR.AA-04:** забезпечити перевіряння, захист та передавання інформації про запити на ідентифікацію.

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

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

3.2. **Обізнаність і навчання (PR.AT):** персонал організації має обізнаність у кібербезпеці, проходить навчання з кібербезпеки таким чином, що може виконувати свої завдання, пов'язані із забезпеченням кібербезпеки.

3.2.1. **PR.AT-01:** забезпечити обізнаність та навченість персоналу таким чином, що він має 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 мають знання та навички для виконання встановлених завдань щодо ризиків кібербезпеки.

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

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

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 організації.

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

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

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

3.4.2. **PR.PS-02**: забезпечити належне обслуговування, заміну та видалення програмного забезпечення відповідно до ризику.

3.4.3. **PR.PS-03**: забезпечити обслуговування, заміну та видалення обладнання відповідно до ризику.

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

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

3.4.6. **PR.PS-06**: інтегрувати практики безпечної розробки програмного забезпечення та контролювати їх виконання протягом життєвого циклу розробленого програмного забезпечення.

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

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

3.5.2. **PR.IR-02:** забезпечити захист технологічних активів від загроз навколишнього середовища.

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

3.5.4. **PR.IR-04**: забезпечити управління пропорційністю та адекватністю застосування ресурсів для їх доступності.

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

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

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

4.1.2. **DE.CM-02:** проводити постійний моніторинг фізичного середовища для виявлення потенційно несприятливих подій.

4.1.3. **DE.CM-03:** проводити постійний моніторинг діяльності персоналу та використання ним технологій для виявлення потенційно несприятливих подій.

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

4.1.5. **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 інциденти кібербезпеки.

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

4.2.2. **DE.AE-03:** впровадити періодичне проведення пошуку та зіставлення інформації з кількох джерел.

4.2.3. **DE.AE-04:** забезпечити усвідомлення очікуваного впливу і масштабу несприятливих подій.

4.2.4. **DE.AE-06:** забезпечити передавання інформації про несприятливі події до уповноважених підрозділів (організацій) для використання відповідного інструментарію.

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

4.2.6. **DE.AE-08:** впровадити здійснення оголошення про інцидент, коли несприятливі події відповідають визначеним критеріям інциденту.

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

5.1. **Управління інцидентами (RS.MA):** керування реагуванням на виявлені інциденти кібербезпеки.

5.1.1. **RS.MA-01:** впровадити виконання планів реагування на інцидент в координації з відповідними третіми сторонами одразу після оголошення інциденту.

5.1.2. **RS.MA-02:** впровадити здійснення сортування звітів про інциденти після їх підтвердження.

5.1.3. **RS.MA-03:** впровадити класифікацію та пріоритизацію інцидентів.

5.1.4. **RS.MA-04**: впровадити інформування та підвищення рівнів критичності інцидентів (за потреби).

5.1.5. **RS.MA-05**: впровадити застосування критеріїв для ініціювання відновлення після інциденту.

5.2. **Аналіз інциденту (RS.AN):** проведення розслідувань для забезпечення ефективного реагування та експертизи інцидентів, а також заходів з відновлення після них.

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

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

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

5.2.4. **RS.AN-08**: запровадити оцінювання масштабу інциденту та документально його підтверджувати.

5.3. **Звітування про реагування на інциденти 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 інциденти.

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

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

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

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

6. ВІДНОВЛЕННЯ (RC): поновлення штатного режиму функціонування об’єктів кіберзахисту після 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 інцидент частини заходів щодо відновлення одразу після їх ініціалізації в ході реагування на інцидент.

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-04**: переглянути критичні для місії організації функції для встановлення операційних норм після інцидентів.

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

6.1.6. **RC.RP-06:** задекларувати завершення відновлення після інциденту, підтвердження критеріїв та пов’язаної з інцидентом документації.

6.2. **Комунікація з відновлення після інциденту (RC.CO)**: координація заходів з 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 інциденту, використовуючи затверджені методи та повідомлення.

Директор Департаменту кіберзахисту
Адміністрації Держспецзв’язку
лейтенант Ігор МАЛЬЧЕНЮК