МІНІСТЕРСТВО ЕНЕРГЕТИКИ УКРАЇНИ

Н А К А З

_____ **м. Київ** _____

**Про затвердження Вимог
з кіберзахисту паливно-енергетичного
сектору критичної інфраструктури**

Відповідно до пункту 14 Загальних вимог до кіберзахисту об’єктів критичної інфраструктури, затверджених постановою Кабінету Міністрів України від 19 червня 2019 року № 518, Положення про організаційно-технічну модель кіберзахисту, затвердженого постановою Кабінету Міністрів України від 29 грудня 2021 року № 1426,
НАКАЗУЮ:

1. Затвердити Вимоги з кіберзахисту паливно-енергетичного сектору критичної інфраструктури, що додаються.

2. Визнати таким, що втратив чинність, наказ Міністерства енергетики України від 15 грудня 2022 року № 417 «Про Вимоги з кібербезпеки паливно-енергетичного сектору критичної інфраструктури», зареєстрований в Міністерстві юстиції України 08 лютого 2023 року за № 249/39305.

3. Управлінню кібербезпеки та цифрового розвитку забезпечити подання цього наказу на державну реєстрацію до Міністерства юстиції України в установленому порядку.

4. Цей наказ набирає чинності з дня його офіційного опублікування.

5. Контроль за виконанням цього наказу покласти на заступника Міністра з питань цифрового розвитку, цифрових трансформацій і цифровізації АНДАРАКА Романа.

Міністр **Світлана ГРИНЧУК**

ЗАТВЕРДЖЕНО
Наказ Міністерства енергетики України
_____2025 року № _____

Вимоги
з кіберзахисту паливно-енергетичного сектору критичної інфраструктури

1. Ці Вимоги визначають обов’язкові до виконання операторами критичної інфраструктури паливно-енергетичного сектору критичної інфраструктури (далі – оператори критичної інфраструктури) заходи з кіберзахисту об’єктів критичної інфраструктури I–IV категорій критичності (далі – об’єкти критичної інфраструктури) та об’єктів кіберзахисту (далі – заходи з кіберзахисту) для досягнення конкретного цільового стану кібербезпеки.

2. В цих Вимогах терміни вживаються у значеннях, наведених у Законах України «Про критичну інфраструктуру», «Про основні засади забезпечення кібербезпеки України», «Про захист інформації в інформаційно-комунікаційних системах», постанові Кабінету Міністрів України від 09 жовтня 2020 року № 943 «Деякі питання об’єктів критичної інформаційної інфраструктури», постанові Кабінету Міністрів України від 04 квітня 2023 року № 299 «Деякі питання реагування суб’єктами забезпечення кібербезпеки на різні види подій у кіберпросторі», постанові Кабінету Міністрів України від 04 серпня 2023 року № 818 «Деякі питання паспортизації об’єктів критичної інфраструктури», Загальних вимогах до кіберзахисту об’єктів критичної інфраструктури, затверджених постановою Кабінету Міністрів України від 19 червня 2019 року № 518, Положенні про організаційно-технічну модель кіберзахисту, затвердженому постановою Кабінету Міністрів України від 29 грудня 2021 року № 1426, Вимогах щодо управління ризиками безпеки на об’єктах критичної інфраструктури I категорії критичності, затверджених постановою Кабінету Міністрів України від 01 квітня 2025 року № 367, Базових заходах з кіберзахисту, затверджених наказом Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 30 січня 2025 року № 54.

3. Ці Вимоги описують заходи з кіберзахисту, як перелік впорядкованих та взаємопов’язаних заходів з кіберзахисту.

Заходи з кіберзахисту включають шість функцій – управління, ідентифікація, забезпечення захисту, виявлення, реагування та відновлення, які діляться на категорії та підкатегорії.

Всі заходи з кіберзахисту шести функцій виконуються одночасно. Заходи з кіберзахисту функцій управління, ідентифікація, забезпечення захисту

і виявлення повинні виконуватися безперервно, а заходи з кіберзахисту функцій реагування і відновлення виконуються в разі виникнення інцидентів кібербезпеки.

4. До заходів з кіберзахисту належать:

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

Організаційний контекст (GV.OC): визначення місії, очікування заінтересованих сторін, залежності, яких має дотримуватися оператор критичної інфраструктури в своїй діяльності для виконання прийнятих рішень щодо управління ризиками кібербезпеки та захисту інформації.

GV.OC-01: забезпечити усвідомлення оператором критичної інфраструктури, який здійснює управління ризиками кібербезпеки та захисту інформації, власної місії.

GV.OC-02: потреби внутрішніх та зовнішніх заінтересованих сторін від впровадження управління ризиками кібербезпеки та захисту інформації визначені.

GV.OC-03: забезпечити виконання працівниками існуючих заходів з кіберзахисту, встановлених цими Вимогами та іншими нормативно-правовими актами з питань кібербезпеки.

GV.OC-04: визначити ключові цілі, критичні послуги та спроможності, які очікуються постачальниками від оператора критичної інфраструктури, що доведені та усвідомлені його працівниками.

GV.OC-05: визначити наслідки, спроможності та послуги, від яких залежить діяльність оператора критичної інфраструктури, довести та забезпечити їх усвідомлення працівниками.

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

GV.RM-01: визначити та узгодити із заінтересованими сторонами оператора критичної інфраструктури цілі управління ризиками.

GV.RM-02: визначити допустимий рівень ризику, який оператор критичної інфраструктури може прийняти, довести до відома всіх працівників і заінтересованих сторін та підтримувати таку інформацію в актуальному стані.

GV.RM-03: додати до процесів управління ризиками оператора критичної інфраструктури діяльність з управління ризиками кібербезпеки та захисту інформації і досягнення її цілей.

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

GV.RM-05: визначити та довести до відома працівників способи обміну інформацією всередині оператора критичної інфраструктури щодо ризиків

кібербезпеки та захисту інформації, включаючи ризики, які несуть постачальники та інші треті сторони.

GV.RM-06: визначити та довести до відома працівників стандартизовані методи розрахунку, документування, ідентифікації та визначення пріоритетності ризиків кібербезпеки та захисту інформації.

GV.RM-07: визначити, характеризувати та забезпечувати обговорення з працівниками оператора критичної інфраструктури стратегічних можливостей щодо управління ризиками кібербезпеки та захисту інформації.

Ролі, обов'язки та повноваження (GV.RR): визначення та доведення до відома працівників оператора критичної інфраструктури ролей щодо кібербезпеки, відповідальності, оцінки ефективності та постійного вдосконалення.

GV.RR-01: визначити із числа працівників оператора критичної інфраструктури відповідальну посадову особу, яка звітує про ризики кібербезпеки та захисту інформації.

GV.RR-02: визначити ролі, відповідальність та підрозділи оператора критичної інфраструктури, залучені до управління ризиками кібербезпеки та захисту інформації, здійснювати контроль за їх дотриманням.

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

GV.RR-04: додати кібербезпеку до практик управління персоналом.

Політика (GV.PO): затвердження, доведення та сприяння реалізації політики кібербезпеки оператора критичної інфраструктури.

GV.PO-01: розробити та довести до відома працівників оператора критичної інфраструктури політику управління ризиками кібербезпеки та захисту інформації, яка визначена з урахуванням структури оператора критичної інфраструктури, стратегії кібербезпеки та пріоритетів.

GV.PO-02: забезпечити періодичний перегляд, оновлення, доведення та виконання політики управління ризиками кібербезпеки та захисту інформації з урахуванням змін нормативних вимог, загроз, технологій та місії оператора критичної інфраструктури.

Контроль (GV.OV): використання результатів комплексної діяльності з управління ризиками кібербезпеки та захисту інформації здійснюється для інформування, покращення ефективності та коригування стратегії управління ризиками.

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

GV.OV-02: забезпечити перегляд та коригування стратегії управління ризиками кібербезпеки та захисту інформації для забезпечення охоплення нею вимог оператора критичної інфраструктури та ризиків.

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

Управління ризиками ланцюга постачання (GV.SC): ідентифікація, визначення, управління, моніторинг виконання процесів управління ризиками кібербезпеки та захисту інформації, пов’язаних з постачанням, та їх покращення постачальниками оператора критичної інфраструктури.

GV.SC-01: розробити програму, стратегію, цілі, політики та процеси управління ризиками кібербезпеки та захисту інформації, пов’язаними з постачанням.

GV.SC-02: розробити, довести, здійснювати внутрішню та зовнішню координацію ролей з кібербезпеки при їх виконанні постачальниками, користувачами та партнерами оператора критичної інфраструктури.

GV.SC-03: забезпечити інтеграцію управління ризиками постачання у сфері кібербезпеки в процеси управління ризиками кібербезпеки та захисту інформації оператора критичної інфраструктури, оцінку ризиків і їх вдосконалення.

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

GV.SC-05: встановити вимоги, пов’язані з ризиками кібербезпеки та захисту інформації в постачанні, та впровадити їх.

GV.SC-06: забезпечити планування для зменшення ризиків перед початком відносин з третіми сторонами.

GV.SC-07: визначити ризики, пов’язані з постачальником, його продукцією та послугами, які він надає, з іншими третіми сторонами, усвідомити їх, пріоритизувати та забезпечити реагування на них.

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

GV.SC-09: інтегрувати практичні заходи щодо забезпечення безпеки постачання в програми оператора критичної інфраструктури щодо кібербезпеки та управління ризиками.

GV.SC-10: передбачити в планах управління ризиками кібербезпеки та захисту інформації, пов’язаними з постачанням, порядок дій, які необхідно виконати після прийняття рішення щодо партнерства;

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

Управління активами (ID.AM): ідентифікація активів, які необхідні оператору критичної інфраструктури для досягнення своїх цілей діяльності, та управління ними залежно від їх впливу на цілі оператора критичної інфраструктури та стратегії управління ризиками.

ID.AM-01: забезпечити періодичне проведення інвентаризації обладнання та технічних засобів кіберзахисту, яким керує оператор критичної інфраструктури.

ID.AM-02: забезпечити періодичне проведення інвентаризації програмного забезпечення, послуг і систем, якими керує оператор критичної інфраструктури.

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

ID.AM-04: забезпечити періодичне проведення інвентаризації послуг, що надаються постачальниками.

ID.AM-05: здійснити пріоритизацію активів за їх класифікацією, критичністю, ресурсами, впливом на місію оператора критичної інфраструктури.

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

ID.AM-08: забезпечити управління системами, апаратним та програмним забезпеченням, послугами та даними.

Оцінка ризиків (ID.RA): усвідомлення оператором критичної інфраструктури ризиків кібербезпеки та захисту інформації, його активів і ризиків.

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

ID.RA-02: організувати отримання інформації про загрози безпеки та вразливості з систем обміну інформацією та офіційних джерел.

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

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

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

ID.RA-06: визначити заходи реагування на ризики кібербезпеки та захисту інформації і встановити їх пріоритетність, забезпечити їх аналіз та комунікацію щодо них.

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

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

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

ID.RA-10: забезпечити проведення оцінювання постачальників перед придбанням у них критично важливих для оператора критичної інфраструктури продуктів і послуг.

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

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

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

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

ID.IM-04: розробити, затвердити, довести до відома працівників, переглядати та удосконалювати плани реагування на інциденти кібербезпеки та інші плани кібербезпеки, які впливають на діяльність оператора критичної інфраструктури;

3) забезпечення захисту (PR): розроблення та впровадження методів, засобів, процедур кіберзахисту, спрямованих на забезпечення сталого та надійного функціонування об'єктів критичної інфраструктури та об'єктів кіберзахисту, удосконалення систем реагування на інциденти кібербезпеки та кібератаки з урахуванням необхідності забезпечення пропорційності та/або співрозмірності можливостей таких систем реальним та потенційним ризикам.

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.

PR.AA-01: забезпечити на рівні оператора критичної інфраструктури керування обліковими даними для авторизованих користувачів, служб і апаратного забезпечення.

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

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

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

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

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

Обізнаність і навчання (PR.AT): працівники оператора критичної інфраструктури мають обізнаність у кібербезпеці, проходять навчання з кібербезпеки таким чином, що можуть виконувати свої завдання, пов'язані із забезпеченням кібербезпеки.

PR.AT-01: забезпечити обізнаність та навченість працівників таким чином, що вони мають знання та навички для виконання основних завдань щодо ризиків кібербезпеки та захисту інформації.

PR.AT-02: забезпечити обізнаність та навченість працівників, які безпосередньо виконують завдання із забезпечення кібербезпеки, кіберзахисту, таким чином, що вони мають знання та навички для виконання встановлених завдань щодо ризиків кібербезпеки та захисту інформації.

Безпека даних (PR.DS): управління даними здійснюється відповідно до стратегії ризиків оператора критичної інфраструктури для захисту конфіденційності, цілісності та доступності інформації.

PR.DS-01: забезпечити конфіденційність, цілісність і доступність даних, що зберігаються в обладнанні систем оператора критичної інфраструктури.

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

PR.DS-10: забезпечити конфіденційність, цілісність і доступність даних, що використовуються: до яких є доступ, які обробляються та регулярно оновлюються застосунками, користувачами або пристроями оператора критичної інфраструктури.

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

Безпека платформ (PR.PS): керування апаратним та програмним забезпеченням, службами фізичних і віртуальних платформ відповідно до стратегії ризиків оператора критичної інфраструктури для захисту їх конфіденційності, цілісності та доступності.

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

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

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

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

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

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

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

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

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

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

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

4) виявлення (DE): проведення ідентифікації, збору та обробки інцидентів кібербезпеки та кібератак.

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

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

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

DE.CM-03: проводити постійний моніторинг діяльності працівників та використання ними технологій для виявлення потенційно несприятливих подій.

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

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

Аналіз несприятливих подій (DE.AE): аналіз аномалій, індикаторів компрометації та інших потенційно несприятливих подій, щоб їх характеризувати та виявити інциденти кібербезпеки.

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

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

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

DE.AE-06: забезпечити передавання інформації про несприятливі події до уповноважених підрозділів оператора критичної інфраструктури для використання відповідного інструментарію.

DE.AE-07: забезпечити збирання, виявлення та аналіз інформації про кіберзагрози.

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

5) реагування (RS): запобігання інцидентам кібербезпеки та кібератакам, належне інформування про них, запобігання негативним наслідкам, їх мінімізація та усунення.

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

RS.MA-01: впровадити виконання планів реагування на інциденти кібербезпеки в координації з відповідними третіми сторонами одразу після оголошення про інцидент кібербезпеки.

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

RS.MA-03: впровадити класифікацію та пріоритизацію інцидентів кібербезпеки.

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

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

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

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

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

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

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

Звітування про реагування на інциденти кібербезпеки та комунікація (RS.CO): координація заходів реагування з внутрішніми та зовнішніми заінтересованими сторонами відповідно до цих Вимог та інших вимог законодавства України у сфері кібербезпеки.

RS.CO-02: запровадити сповіщення внутрішніх та зовнішніх заінтересованих сторін про інциденти кібербезпеки.

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

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

RS.MI-01: забезпечити локалізацію інциденту кібербезпеки.

RS.MI-02: забезпечити ліквідацію інциденту кібербезпеки;

6) відновлення (RC): поновлення штатного режиму функціонування критичної інфраструктури після кібератаки та інциденту кібербезпеки, відновлення інформації та відомостей у разі їх пошкодження або видалення, створення умов для проведення розслідування кібератаки та інциденту кібербезпеки.

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

RC.RP-01: забезпечити виконання передбачених планом реагування на інциденти кібербезпеки заходів щодо відновлення одразу після їх ініціалізації в ході реагування на інцидент кібербезпеки.

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

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

RC.RP-04: переглянути критичні для місії оператора критичної інфраструктури функції після інциденту кібербезпеки.

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

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

Комунікація з відновлення після інциденту кібербезпеки (RC.CO): координація заходів з відновлення з внутрішніми та зовнішніми сторонами.

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

RC.CO-04: запровадити інформування про відновлення після інциденту кібербезпеки, використовуючи затверджені методи та повідомлення.

5. Ці Вимоги застосовуються для розроблення профілю кіберзахисту для оператора критичної інфраструктури паливно-енергетичного сектору критичної інфраструктури за формою, наведеною у додатку до цих Вимог (далі – профіль кіберзахисту).

6. Профіль кіберзахисту включає:

поточний профіль кіберзахисту – відображає поточний стан кіберзахисту та визначає основні заходи з кіберзахисту, які оператор критичної інфраструктури наразі впровадив або впроваджує. Дані поточного профілю кіберзахисту використовуються для оцінки поточного стану кіберзахисту. Поточний профіль кіберзахисту можна використовувати для створення плану захисту об’єкта критичної інфраструктури;

цільовий профіль кіберзахисту – визначає бажані результати в майбутньому, які оператор критичної інфраструктури визначив як пріоритетні для впровадження заходів з кіберзахисту та досягнення своїх цілей з управління ризиками кібербезпеки та захисту інформації.

7. Аналіз розбіжностей між поточним та цільовим профілями кіберзахисту передбачає розроблення та затвердження оператором критичної інфраструктури пріоритетного плану дій з кібербезпеки, який повинен містити найменування заходів, відповідальних за виконання заходів, строки виконання заходів та індикатори виконання заходів.

Оператор критичної інфраструктури зобов’язаний дотримуватися та щорічно переглядати і оновлювати пріоритетний план дій з кібербезпеки з метою усунення недоліків та наближення стану кібербезпеки об’єктів критичної інфраструктури та/або об’єктів кіберзахисту до цільового профілю кіберзахисту.

8. Оператор критичної інфраструктури при впровадженні заходів з кіберзахисту враховує ризики кібербезпеки та захисту інформації об’єктів критичної інфраструктури та об’єктів кіберзахисту.

9. Рівні впровадження (зрілості) заходів з кіберзахисту (далі – Рівні) характеризують ступінь практичного впровадження заходів з кіберзахисту, контроль та суворе дотримання практик управління ризиками кібербезпеки та захисту інформації, а також надають контекст того, як оператором критичної інфраструктури розглядаються ризики кібербезпеки та захисту інформації і процеси, що застосовуються для управління цими ризиками.

10. Рівні відображають практики оператора критичної інфраструктури з управління ризиками кібербезпеки та захисту інформації як часткові (Рівень 1), ризик-орієнтовані (Рівень 2), повторювані (Рівень 3) та адаптивні (Рівень 4).

Рівень 1: частковий. Застосування стратегії ризиків кібербезпеки та захисту інформації, впровадження заходів з кіберзахисту управляється в індивідуальному порядку. Пріоритизація є випадковою і формально не базується на цілях чи середовищі загроз. Обізнаність про ризики кібербезпеки та захисту інформації у оператора критичної інфраструктури обмежена. Оператор критичної інфраструктури впроваджує управління ризиками кібербезпеки та захисту інформації та заходи з кіберзахисту на нерегулярній основі. Оператор критичної інфраструктури може не мати процесів, які дозволяють обмінюватися інформацією про кібербезпеку.

Рівень 2: ризик-орієнтований. Методи управління ризиками та впровадження заходів з кіберзахисту встановлені як загальна політика оператора критичної інфраструктури. Пріоритизація діяльності з кібербезпеки та потреб у захисті інформації безпосередньо залежить від цілей організаційних ризиків, середовища загроз або вимог оператора критичної інфраструктури, його місії. Існує усвідомлення ризиків кібербезпеки та захисту інформації на організаційному рівні, але загально-організаційного підходу до управління ризиками кібербезпеки та захисту інформації не встановлено. Врахування кібербезпеки в організаційних цілях і програмах може мати місце на деяких, але не на всіх рівнях. Оцінка ризиків кібербезпеки та захисту інформації, організаційних і зовнішніх активів, впровадження заходів з кіберзахисту здійснюється, але зазвичай не є повторюваною або періодичною. Обмін інформацією про кібербезпеку здійснюється згідно з вимогами законодавства України у сфері кібербезпеки.

Рівень 3: повторюваний. Практики управління ризиками та впровадження заходів з кіберзахисту офіційно затверджені та виражені як політики. Політики, процеси та процедури з урахуванням ризиків визначаються, впроваджуються за призначенням і переглядаються. Організаційні практики кібербезпеки регулярно оновлюються на основі застосування процесів управління ризиками до змін у вимогах оператора критичної інфраструктури, його місії, загрозах і технологічному ландшафті. Існує загально-організаційний підхід до управління ризиками кібербезпеки та

захисту інформації. Інформація про кібербезпеку регулярно передається. Існують узгоджені методи для ефективного реагування на зміни ризику. Працівники володіють знаннями та навичками для виконання своїх призначених ролей і обов'язків. Оператор критичної інфраструктури постійно та точно відстежує ризики кібербезпеки та захисту інформації.

Рівень 4: адаптивний. Існує загально-організаційний підхід до управління ризиками кібербезпеки та захисту інформації, який використовує політику, процеси та процедури з урахуванням ризиків для вирішення потенційних подій кібербезпеки. Взаємозв'язок між ризиками кібербезпеки та захисту інформації і цілями чітко розуміється та враховується під час прийняття рішень. Підрозділи оператора критичної інфраструктури впроваджують та аналізують ризики на системному рівні в контексті допустимих організаційних ризиків. Оператор критичної інфраструктури оперативно та ефективно адаптується до змін у цілях діяльності або завданнях, пов'язаних з основною місією. Це дозволяє своєчасно коригувати підходи до управління ризиками та інформувати про них відповідно до актуальних потреб оператора критичної інфраструктури та зовнішнього середовища.

11. Оператор критичної інфраструктури забезпечує Рівень відповідно до категорій критичності об'єктів критичної інфраструктури.

Ці Вимоги визначають таку відповідність категорій критичності об'єктів критичної інфраструктури (далі – категорія критичності) до Рівнів:

I категорія критичності – Рівень 4;

II, III категорія критичності – Рівень 3 або Рівень 4;

IV категорія критичності – Рівень 2 або Рівень 3 або Рівень 4.

12. Оператор критичної інфраструктури надсилає до Міністерства енергетики України профіль кіберзахисту, затверджений пріоритетний план дій з кібербезпеки не пізніше 01 грудня поточного року.

13. Оператор критичної інфраструктури надає Міністерству енергетики України контактні дані відповідальних осіб з кіберзахисту та підтримує таку інформацію в актуальному стані.

14. Оператор критичної інфраструктури бере участь у проведенні кібернавчань паливно-енергетичного сектору критичної інфраструктури, розробленні програм та методик їх проведення, сценаріїв реагування на кіберзагрози.

Начальник Управління
кібербезпеки та цифрового розвитку **Валерій СТРІГАНОВ**

Додаток
до Вимог з кіберзахисту
паливно-енергетичного сектору
критичної інфраструктури
(пункт 5)

Профіль кіберзахисту
для оператора критичної інфраструктури
паливно-енергетичного сектору критичної інфраструктури

_____

(найменування оператора критичної інфраструктури паливно-енергетичного сектору критичної інфраструктури)

_____

(рівень впровадження (зрілості) заходів з кіберзахисту)

№ з/п	Заходи кіберзахисту	Поточний профіль кіберзахисту	Цільовий профіль кіберзахисту	Заходи для досягнення цільового профіля за роками
1	2	3	4	5
Управління (GV)				
Організаційний контекст (GV.OC)				
1	GV.OC-01			
2	GV.OC-02			
3	GV.OC-03			
4	GV.OC-04			
5	GV.OC-05			
Стратегія управління ризиками (GV.RM)				
6	GV.RM-01			
7	GV.RM-02			
8	GV.RM-03			

Продовження додатка

1	2	3	4	5
9	GV.RM-04			
10	GV.RM-05			
11	GV.RM-06			
12	GV.RM-07			
Ролі, обов’язки та повноваження (GV.RR)				
13	GV.RR-01			
14	GV.RR-02			
15	GV.RR-03			
16	GV.RR-04			
Політика (GV.PO)				
17	GV.PO-01			
18	GV.PO-02			
Контроль (GV.OV)				
19	GV.OV-01			
20	GV.OV-02			
21	GV.OV-03			
Управління ризиками ланцюга постачання (GV.SC)				
22	GV.SC-01			
23	GV.SC-02			
24	GV.SC-03			
25	GV.SC-04			
26	GV.SC-05			
27	GV.SC-06			
28	GV.SC-07			
29	GV.SC-08			
30	GV.SC-09			
31	GV.SC-10			

Продовження додатка

1	2	3	4	5
Ідентифікація (ID)				
Управління активами (ID.AM)				
32	ID.AM-01			
33	ID.AM-02			
34	ID.AM-03			
35	ID.AM-04			
36	ID.AM-05			
37	ID.AM-07			
38	ID.AM-08			
Оцінка ризиків (ID.RA)				
39	ID.RA-01			
40	ID.RA-02			
41	ID.RA-03			
42	ID.RA-04			
43	ID.RA-05			
44	ID.RA-06			
45	ID.RA-07			
46	ID.RA-08			
47	ID.RA-09			
48	ID.RA-10			
Удосконалення (ID.IM)				
49	ID.IM-01			
50	ID.IM-02			
51	ID.IM-03			
52	ID.IM-04			
Забезпечення захисту(PR)				
Управління ідентифікацією, автентифікація та контроль доступу (PR.AA)				
53	PR.AA-01			

Продовження додатка

1	2	3	4	5
54	PR.AA-02			
55	PR.AA-03			
56	PR.AA-04			
57	PR.AA-05			
58	PR.AA-06			
Обізнаність і навчання (PR.AT)				
59	PR.AT-01			
60	PR.AT-02			
Безпека даних (PR.DS)				
61	PR.DS-01			
62	PR.DS-02			
63	PR.DS-10			
64	PR.DS-11			
Безпека платформ (PR.PS)				
65	PR.PS-01			
66	PR.PS-02			
67	PR.PS-03			
68	PR.PS-04			
69	PR.PS-05			
70	PR.PS-06			
Стійкість технологічної інфраструктури (PR.IR)				
71	PR.IR-01			
72	PR.IR-02			
73	PR.IR-03			
74	PR.IR-04			
Виявлення (DE)				
Безперервний моніторинг (DE.CM)				
75	DE.CM-01			

Продовження додатка

1	2	3	4	5
76	DE.CM-02			
77	DE.CM-03			
78	DE.CM-06			
79	DE.CM-09			
Аналіз несприятливих подій (DE.AE)				
80	DE.AE-02			
81	DE.AE-03			
82	DE.AE-04			
83	DE.AE-06			
84	DE.AE-07			
85	DE.AE-08			
Реагування (RS)				
Управління інцидентами (RS.MA)				
86	RS.MA-01			
87	RS.MA-02			
88	RS.MA-03			
89	RS.MA-04			
90	RS.MA-05			
Аналіз інциденту (RS.AN)				
91	RS.AN-03			
92	RS.AN-06			
93	RS.AN-07			
94	RS.AN-08			
Звітування про реагування на інциденти кібербезпеки та комунікація (RS.CO)				
95	RS.CO-02			
96	RS.CO-03			
Пом’якшення інциденту кібербезпеки (RS.MI)				
97	RS.MI-01			

Продовження додатка

1	2	3	4	5
98	RS.MI-02			
Відновлення (RC)				
Виконання плану відновлення після інциденту кібербезпеки (RC.RP)				
99	RC.RP-01			
100	RC.RP-02			
101	RC.RP-03			
102	RC.RP-04			
103	RC.RP-05			
104	RC.RP-06			
Комунікація з відновлення після інциденту кібербезпеки (RC.CO)				
105	RC.CO-03			
106	RC.CO-04			