ДЕРЖАВНА ІНСПЕКЦІЯ ЯДЕРНОГО РЕГУЛЮВАННЯ УКРАЇНИ

вул. Арсенальна, 9/11, м. Київ, 01011,
тел.: (044) 277-12-04,
факс: (044) 254-33-11
E-mail: pr@snriu.gov.ua,
Сайт: www.snriu.gov.ua
код згідно з ЄДРПОУ 21721086

STATE NUCLEAR REGULATORY INSPECTORATE OF UKRAINE

Arsenalna street, 9/11, Kyiv, 01011,
phone: 38 (044) 277-12-04,
fax: 38 (044) 254-33-11
E-mail: pr@snriu.gov.ua,
WEB: www.snriu.gov.ua,
код згідно з ЄДРПОУ 21721086

від _____ 20__ р. № _____ На № _____ від _____ 20__ р.

Державна регуляторна служба України

Про погодження проєкту наказу Держатомрегулювання

Державною інспекцією ядерного регулювання України (Держатомрегулювання) розроблено проєкт наказу «Про затвердження Вимог до кіберзахисту інформаційних та керуючих систем атомних станцій для забезпечення ядерної та радіаційної безпеки» (далі – проєкт наказу).

Метою розроблення проєкту наказу є визначення та врегулювання вимог до кіберзахисту інформаційних та керуючих систем атомних станцій та приведення національного законодавства у відповідність до міжнародних норм.

Державною регуляторною службою України листом від 11 серпня 2021 р. № 5832/0/20-21 було визнано, що проєкт наказу містить норми регуляторного характеру, а його прийняття потребує реалізації процедур, передбачених Законом України «Про засади державної регуляторної політики у сфері господарської діяльності».

29.11.2021 проєкт наказу та аналіз регуляторного впливу до нього було оприлюднено на офіційному сайті Держатомрегулювання для отримання зауважень та пропозицій, які приймалися до 29.12.2021. Станом на 29.12.2021 зауваження та пропозиції до проєкту наказу до Держатомрегулювання не надходили, тому зміни до проєкту наказу не вносилися.

Просимо розглянути проєкт наказу та, у разі відсутності зауважень, погодити його до 04 лютого 2022 р.

Додатки: 1. Проєкт наказу на 55 арк. у 1 прим.
2. Пояснювальна записка до проєкту наказу на 4 арк. у 1 прим.
3. Аналіз регуляторного впливу до проєкту наказу на 13 арк. у 1 прим.
4. Повідомлення про оприлюднення проєкту наказу на 1 арк. у 1 прим.

Виконуючий обов'язки Голови –
Головного державного інспектора
з ядерної та радіаційної безпеки України **Олег КОРІКОВ**

Андрій Горошанський 277 12 21

ПРОЄКТ

ДЕРЖАВНА ІНСПЕКЦІЯ ЯДЕРНОГО РЕГУЛЮВАННЯ УКРАЇНИ
Н А К А З

«___» _____ 2022 року Київ № _____

Про затвердження Вимог до кіберзахисту інформаційних та керуючих систем атомних станцій для забезпечення ядерної та радіаційної безпеки

Відповідно до статей 8 та 24 Закону України «Про використання ядерної енергії та радіаційну безпеку», підпункту 7 пункту 4 Положення про Державну інспекцію ядерного регулювання України, затвердженого постановою Кабінету Міністрів України від 20 серпня 2014 року № 363,

НАКАЗУЮ:

1. Затвердити Вимоги до кіберзахисту інформаційних та керуючих систем атомних станцій для забезпечення ядерної та радіаційної безпеки.

2. Департаменту з питань безпеки ядерних установок (Борис СТОЛЯРЧУК) забезпечити подання цього наказу на державну реєстрацію до Міністерства юстиції України в установленому порядку.

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

4. Контроль за виконанням цього наказу залишаю за собою.

Виконуючий обов'язки Голови –
Головного державного інспектора
з ядерної та радіаційної безпеки України **Олег КОРІКОВ**

ЗАТВЕРДЖЕНО
Наказ Державної інспекції ядерного регулювання України
_____ № _____

Вимоги до кіберзахисту інформаційних та керуючих систем атомних станцій для забезпечення ядерної та радіаційної безпеки

I. Загальні положення

1. Ці Вимоги встановлюють вимоги до кіберзахисту інформаційних та керуючих систем атомних станцій, їх компонентів (програмно-технічних комплексів, технічних засобів автоматизації) і програмного забезпечення зазначених систем, під час їх розроблення, впровадження, експлуатації та модифікації, з метою забезпечення ядерної та радіаційної безпеки.

2. У цих Вимогах терміни вживаються в таких значеннях:

автентифікація – процес перевірки ідентифікаційних даних користувача або перевірки джерела даних, повідомлень і команд;

авторизація – процес надання інформаційною та/або керуючою системою певному користувачу або групі користувачів (після їх успішної автентифікації) прав на виконання певних дій, а також процес перевірки (підтвердження) наданих прав у разі спроби виконання цих дій;

вироби сторонньої розробки – програмні або апаратні вироби, які виготовлені третьою стороною відносно розробника інформаційної та/або керуючої системи, її компонентів або програмного забезпечення;

віддалений доступ – процес доступу користувача до інформаційної та/або керуючої системи атомної станції, її компонентів та/або програмного

забезпечення, який забезпечує дистанційне використання даних, інформаційно-обчислювальних ресурсів та/або функції цієї системи;

відновлення – процес, спрямований на повернення інформаційної та/або керуючої системи атомної станції, її компонентів, програмного забезпечення до працездатного стану після повної або часткової втрати функціональності;

вразливість – недолік в інформаційній та/або керуючій системі атомної станції, її компонентах та/або програмному забезпеченні, який може бути використаний для реалізації кіберзагрози;

глибокоешелонований кіберзахист – підхід до кіберзахисту інформаційних та/або керуючих систем атомної станції, за якого для забезпечення кіберзахисту розгорнуті кілька послідовних рівнів і заходів кіберзахисту;

демілітаризована зона – фізичний або логічний сегмент мережі, який містить загальнодоступні сервіси, відділений від внутрішніх сервісів і ресурсів атомної станції та використовується з метою введення додаткового захисного бар'єра для локальної мережі;

диференційований підхід – застосування заходів кіберзахисту інформаційної та/або керуючої системи атомної станції пропорційно рівню кіберзахисту;

доступність – властивість, яка гарантує, що авторизований користувач завжди отримає доступ до даних і змогу їх використати;

зона кіберзахисту – група інформаційних та/або керуючих систем атомної станції з однаковими рівнями кіберзахисту, яка виділена для спільного адміністративного управління, комунікації та застосування однакових захисних заходів;

кібератака на інформаційну та/або керуючу систему атомної станції (далі – кібератака) – дії, які здійснюються за допомогою засобів електронних комунікацій (охоплюючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання)

та спрямовані на компрометацію інформаційної та/або керуючої системи атомної станції через використання вразливостей;

кіберзагроза інформаційній та/або керуючій системі атомної станції (далі – кіберзагроза) – наявні та потенційно можливі явища і чинники, що можуть стати потенційною причиною кіберінциденту, який може спричинити нанесення шкоди інформаційній та/або керуючій системі атомної станції;

кіберзахист інформаційних та/або керуючих систем атомної станції (далі – кіберзахист) – комплекс адміністративних, технічних і програмних заходів та засобів, метою яких є запобігання, виявлення і реагування на кібератаки та кіберзагрози;

кіберінцидент з інформаційною та/або керуючою системою атомної станції (далі – кіберінцидент) – подія, під час виникнення якої піддаються компрометації інформаційна та/або керуюча система атомної станції, її компоненти або мережеве обладнання;

компрометація – порушення конфіденційності, цілісності, доступності даних та/або функціонування й характеристик інформаційної та/або керуючої системи атомної станції;

контроль доступу – процес забезпечення санкціонованого, авторизованого доступу до інформаційної та/або керуючої системи атомної станції або її компонентів;

конфіденційність – властивість, яка гарантує, що інформація залишається недоступною або нерозкритою для неавторизованих користувачів;

користувач – фізична особа або програмний процес, що може взаємодіяти з інформаційною та/або керуючою системою атомної станції через наданий інтерфейс;

культура безпеки щодо кіберзахисту (далі – культура кіберзахисту) – набір характеристик та особливостей діяльності організацій і поведінки окремих осіб, які визначають, що забезпечення кіберзахисту є однією з пріоритетних цілей і внутрішньою потребою, що веде до самосвідомості,

відповідальності та самоконтролю під час виконання всіх робіт, що впливають на кіберзахист;

межа – точка розмежування, яка фізично або логічно поділяє зони кіберзахисту;

межовий інтерфейс – інтерфейс, через який здійснюється зв'язок між інформаційними та/або керуючими системами атомної станції, їх компонентами або мережами, що містяться у різних зонах кіберзахисту;

мережа – система електронних комунікацій, яка забезпечує обмін даними між технічними засобами однієї або декількох інформаційних та/або керуючих систем атомної станції;

мережева архітектура – повна структура мережі, яка визначає усі інформаційні та керуючі системи атомної станції, їх компоненти, мережеве обладнання, кабелі, використані топології мережі, протоколи обміну даними;

моніторинг – процес систематичного контролю поточного стану інформаційних та/або керуючих систем атомної станції, їх компонентів і програмного забезпечення;

негативний вплив – вплив на інформаційну та/або керуючу систему атомної станції, її компоненти або програмне забезпечення, який призводить до втрати або порушення функцій, зниження надійності, здатності реагування на кіберінциденти;

план кіберзахисту – документ, що визначає комплекс заходів, спрямованих на забезпечення кіберзахисту на етапах розроблення, впровадження, експлуатації інформаційних та/або керуючих систем атомних станцій, їх компонентів і програмного забезпечення;

політика кіберзахисту – сукупність задокументованих положень, правил і практик, які визначають цілі та порядок забезпечення кіберзахисту на етапах розроблення, впровадження, експлуатації та модифікації інформаційних та/або керуючих систем атомних станцій;

порушник – фізична особа, група або організація, яка проводить або має намір провести дії, що призведуть до порушення безпеки інформаційних та/або керуючих систем атомної станції;

правило двох осіб – принцип, що ґрунтується на спостереженні однієї особи за діями іншої з метою недопущення несанкціонованих дій;

принцип найменших привілеїв – принцип надання користувачу прав на виконання певних дій з певними ресурсами, які є мінімально необхідними для успішного виконання робочої мети;

програма кіберзахисту – документ, який регламентує та визначає застосування узгоджених (послідовних) організаційних і технічних заходів кіберзахисту та процедур для сукупності всіх інформаційних та керуючих систем енергоблока або майданчика атомної станції для забезпечення досягнення цілей кіберзахисту, визначених у політиці кіберзахисту;

раніше розроблене програмне забезпечення – програмне забезпечення, яке було використано в складі діючих інформаційних та/або керуючих систем та без змін або з додатковим конфігуруванням та уточненням параметрів може бути використано в складі інформаційної та/або керуючої системи, що проєктується;

ризик-інформований підхід до кіберзахисту – процес систематичного виявлення потенційних вразливостей інформаційної та/або керуючої системи та кіберзагроз для цієї системи, імовірнісного оцінювання виникнення негативних подій, детерміністичного оцінювання потенційних негативних наслідків цих подій та розроблення рекомендацій щодо реалізації контрзаходів з метою мінімізації вразливостей, імовірностей виникнення негативних подій та негативних наслідків;

рівень кіберзахисту – градація заходів кіберзахисту, що характеризується відповідними наборами вимог, установлених для інформаційної та/або керуючої системи атомної станції, її компонентів або програмного забезпечення, відповідно до максимальних наслідків успішної кібератаки;

цілісність – властивість, яка гарантує збереження повноти та точності даних.

Інші терміни вживаються в значеннях, наведених у Законі України «Про основні засади забезпечення кібербезпеки України», Загальних положеннях безпеки атомних станцій, затверджених наказом Державного комітету ядерного регулювання України від 19 листопада 2007 року № 162, зареєстрованих у Міністерстві юстиції України 25 січня 2008 року за № 56/14747 (далі – Загальні положення безпеки АС), Вимогах до проведення модифікацій ядерних установок та порядку оцінки їх безпеки, затверджених наказом Державного комітету ядерного регулювання України від 10 січня 2005 року № 4, зареєстрованих у Міністерстві юстиції України 24 січня 2005 року за № 78/10358 (далі – Вимоги до проведення модифікацій ядерних установок та порядку оцінки їх безпеки) та Вимогах з ядерної та радіаційної безпеки до інформаційних та керуючих систем, важливих для безпеки атомних станцій, затверджених наказом Державної інспекції ядерного регулювання України від 22 липня 2015 року № 140, зареєстрованих у Міністерстві юстиції України від 06 серпня 2015 року за № 954/27399 (далі – Вимоги з ядерної та радіаційної безпеки до інформаційних та керуючих систем, важливих для безпеки АС).

3. У цих Вимогах вживаються скорочення, що мають такі значення:

АС – атомна станція;

ЕО – експлуатуюча організація;

ІКС – інформаційна та/або керуюча система атомної станції;

ПЗ – програмне забезпечення;

ПТК – програмно-технічний комплекс;

ТЗА – технічний засіб автоматизації;

ЯРБ – ядерна та радіаційна безпека.

4. До ІКС застосовуються положення Закону України «Про основні засади забезпечення кібербезпеки України», як до технологічних систем, які не

взаємодіють з публічними мережами електронних комунікацій (електронними мережами загального користування), не підключені до мережі Інтернет та/або інших глобальних мереж передачі даних. У ІКС не здійснюється обробка державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законодавством.

5. Ці Вимоги регламентують кіберзахист ІКС, який забезпечується завдяки:

застосуванню ризик-інформованого підходу для забезпечення систематичного управління ризиками з метою недопущення зниження рівня ЯРБ;

відповідності параметрів і характеристик ІКС, їх компонентів і ПЗ під час їх розроблення, впровадження, експлуатації та модифікації вимогам до кіберзахисту;

дотриманню порядку розроблення, впровадження, експлуатації та модифікації ІКС, їх компонентів та ПЗ, з урахуванням вимог до кіберзахисту.

6. Ці Вимоги обов’язкові під час здійснення діяльності з:

розроблення, виготовлення, випробувань, приймання та постачання ПТК і ТЗА (крім загальнопромислових), до складу яких входить ПЗ, призначених для застосування на АС як компонентів нових або модифікованих ІКС;

розроблення та верифікації ПЗ ІКС, ПТК і ТЗА;

проєктування, комплектування, монтажу, налагоджувальних робіт, введення в експлуатацію, експлуатації та модифікації ІКС;

розроблення документів, що обґрунтовують безпеку ІКС та/або їх компонентів;

державної експертизи ЯРБ на етапах розроблення, впровадження, експлуатації та модифікації ІКС, їх компонентів та/або ПЗ.

7. Вимоги не поширюються на:

ТЗА, до складу яких не входить ПЗ;

датчики та канали передачі даних систем контролю радіаційних і метеорологічних параметрів у санітарно-захисній зоні та зоні спостереження;

системи фізичного захисту АС;

комп'ютерні системи АС, які використовуються в управлінні та операціях, орієнтованих на організаційно-адміністративну діяльність.

8. ЕО визначає та погоджує з Державною інспекцією ядерного регулювання України необхідність, обсяг і терміни усунення виявлених невідповідностей цим Вимогам тих ІКС та/або їх компонентів, що експлуатуються на АС, або тих, на монтаж яких Державною інспекцією ядерного регулювання України погоджено технічне рішення.

II. Класифікація

1. Класифікація функцій

1. Категорії виконуваних ІКС функцій визначаються згідно з Вимогами з ядерної та радіаційної безпеки до інформаційних та керуючих систем, важливих для безпеки АС.

2. Функції, що виконують ІКС, важливі для безпеки АС, класифікуються за категоріями A, B, C, визначеними відповідно до Вимог з ядерної та радіаційної безпеки до інформаційних та керуючих систем, важливих для безпеки АС, залежно від їх ролі в забезпеченні ЯРБ, а також від можливих наслідків, спричинених невиконанням або помилковим виконанням функції. Функції, що виконують ІКС, які не впливають на безпеку АС, не класифікуються за категоріями.

2. Рівні кіберзахисту ІКС, їх компонентів та ПЗ

1. Рівні кіберзахисту ІКС, їх компонентів та ПЗ встановлюються згідно з цими Вимогами відповідно до категорій функцій ІКС A, B, C, характеру цих функцій (керуючі або інформаційні) та мережевих зв'язків.

2. Рівень кіберзахисту К1 установлюється для ІКС, їх компонентів та ПЗ, що виконують функції категорії А.

3. Рівень кіберзахисту К2 установлюється для ІКС, їх компонентів та ПЗ, що виконують:

функції категорії В;

керуючі функції категорії С;

керуючі некласифіковані функції.

4. Рівень кіберзахисту К3 установлюється для ІКС, їх компонентів та ПЗ, що виконують:

інформаційні функції категорії С;

інформаційні некласифіковані функції.

III. Загальні принципи забезпечення кіберзахисту

1. Політика кіберзахисту

1. ЕО та розробники ПТК, ТЗА, ПЗ розробляють, реалізують і підтримують політику кіберзахисту.

2. Політика кіберзахисту встановлює цілі кіберзахисту, визначає основні положення, правила та практики забезпечення кіберзахисту.

3. Політика кіберзахисту розробляється на виконання цих Вимог, норм і правил з ЯРБ та враховує закони й інші нормативно-правові акти з кібербезпеки.

4. Перегляд політики кіберзахисту здійснюється не рідше ніж один раз на рік або в разі виникнення кіберінцидентів на ІКС АС або змін, які потенційно можуть вплинути на кіберзахист.

5. Політика кіберзахисту, затверджена керівництвом підприємства-розробника, охоплює такі засади щодо ІКС:

розроблення, проєктування та виготовлення ПТК, ТЗА, ПЗ;

порядок застосування виробів сторонньої розробки;

випробування ПТК, ТЗА, ПЗ;

управління доступом до середовища розроблення ПТК, ТЗА, ПЗ;

управління ризиками та кіберзагрозами;

реагування на кіберінциденти;

оцінювання відповідності середовища розроблення ПТК, ТЗА, ПЗ вимогам кіберзахисту.

6. Політика кіберзахисту ІКС АС, затверджена керівництвом ЕО, охоплює такі засади:

ідентифікація ІКС, їх компонентів та ПЗ;

управління доступом до ІКС, їх компонентів та ПЗ;

управління конфігурацією ІКС, їх компонентів та ПЗ;

випробування ІКС, їх компонентів та ПЗ;

впровадження та експлуатація ІКС, їх компонентів та ПЗ;

модифікація ІКС, їх компонентів та ПЗ;

управління ризиками та кіберзагрозами;

реагування на кіберінциденти та відновлення;

оцінювання відповідності ІКС, їх компонентів та ПЗ вимогам кіберзахисту.

7. Політика кіберзахисту ІКС АС поширюється на всі ІКС, їх компоненти та ПЗ, які експлуатуються на конкретній АС.

8. Вимоги політики кіберзахисту ІКС АС враховуються в документах, що обґрунтовують кіберзахист, які використовуються під час реалізації та контролю за виконанням цієї політики.

2. Глибокоешелонований кіберзахист

1. Передбачається застосовування глибокоешелонованого кіберзахисту від кібератак, спрямованих на ІКС, їх компоненти та ПЗ. Стратегія глибокоешелонованого кіберзахисту описується в програмі кіберзахисту.

2. ЕО впроваджує, застосовує та підтримує стратегію глибокоешелонованого кіберзахисту (з урахуванням заходів захисту від несанкціонованого доступу до ІКС, їх компонентів та ПЗ) для забезпечення можливості виявлення, запобігання, реагування, пом’якшення наслідків і відновлення після кібератаки.

3. Глибокоешелонований кіберзахист забезпечується реалізацією сукупності послідовних бар’єрів і заходів кіберзахисту для захисту ІКС, їх компонентів та ПЗ від кіберзагроз. Завдяки цьому відмова одного бар’єра чи заходу кіберзахисту не призводить до невиконання функцій або погіршення характеристик ІКС, їх компонентів та ПЗ.

Захисні бар’єри та пов’язані з ними заходи кіберзахисту забезпечують попередження або затримку розвитку кібератак.

4. Забезпечується незалежна ефективність різних захисних бар’єрів та їх захист від відмов із загальної причини на етапах розроблення, впровадження, експлуатації та модифікації ІКС. Водночас кожен бар’єр реалізує захист від кіберзагроз, які можуть виникати на сполучених бар’єрах.

3. Диференційований підхід до забезпечення кіберзахисту

1. Вимоги з кіберзахисту залежать від рівня кіберзахисту ІКС, їх компонентів та ПЗ. Заходи кіберзахисту застосовуються пропорційно до потенційно можливих наслідків кіберінцидентів. Для різних рівнів кіберзахисту вживаються заходи різної жорсткості (чим вищий рівень, тим більш суворі заходи кіберзахисту застосовуються).

2. Для практичної реалізації диференційованого підходу виконується логічне об’єднання ІКС та їх компонентів переважно з однаковими рівнями кіберзахисту в зони кіберзахисту для адміністрування та реалізації ідентичних захисних заходів. Критеріями для визначення зон кіберзахисту є структура ІКС, фізичне розміщення ІКС та їх компонентів, організація міжсистемних інтерфейсів, топологія локальних мереж.

Установлюється рівень кіберзахисту кожної зони. В обґрунтованих випадках до складу зони можуть належати ІКС та їх компоненти, що мають рівень кіберзахисту нижчий, ніж рівень кіберзахисту цієї зони. Рівень кіберзахисту зони встановлюється відповідно до найвищого рівня кіберзахисту ІКС та їх компонентів які належать до цієї зони. Водночас до усіх ІКС та їх компонентів і ПЗ у межах певної зони встановлюються вимоги з кіберзахисту та застосовуються захисні заходи відповідно до рівня кіберзахисту цієї зони.

Зони відображають логічне та фізичне групування ІКС та їх компонентів, а рівні кіберзахисту визначають ступінь необхідного кіберзахисту. В обґрунтованих випадках для декількох зон може бути встановлений однаковий рівень кіберзахисту.

3. Застосування зон кіберзахисту здійснюється з дотриманням таких принципів:

до ІКС та їх компонентів, які належать до однієї зони, застосовуються однакові захисні заходи;

ІКС та їх компоненти в межах однієї зони утворюють область надійного зв’язку, що не потребує застосування додаткових заходів захисту;

на межах зон реалізуються механізми розв’язування потоків даних для запобігання несанкціонованому доступу та поширенню помилок із зони більш високого рівня кіберзахисту до зони більш низького рівня кіберзахисту;

не допускається організація прямого з’єднання, що проходить більш ніж через дві зони;

мережеве обладнання (комутатори, кабелі) розміщується в тій же зоні кіберзахисту, що й пов’язані з ним ІКС;

мережеве обладнання, яке використовується для з’єднання різних ІКС та/або їх компонентів, що входять до двох різних зон, належать до зони з вищим рівнем кіберзахисту та до нього застосовуються відповідні заходи кіберзахисту;

передача даних здійснюється однонаправлено з боку зони більш високого рівня кіберзахисту до зони більш низького рівня кіберзахисту (зворотній обмін даними обґрунтовується та ініціюється лише з боку зони більш високого рівня кіберзахисту за допомогою запиту до зони більш низького рівня кіберзахисту);

межі двох зон обладнуються технічними та програмними засобами для розділення потоків даних згідно з вимогами, встановленими до зони більш високого рівня кіберзахисту;

потоки даних між різними зонами контролюються для забезпечення ефективності кіберзахисту;

тимчасове обладнання для доступу до ІКС, їх компонентів і ПЗ використовуються тільки в межах однієї зони або визначеного набору зон із однаковим рівнем кіберзахисту.

4. У випадку розміщення компонентів однієї ІКС у зонах з різним рівнем кіберзахисту до них застосовуються принципи, аналогічні тим, що викладені в пункті 3 глави 3 розділу ІІІ цих Вимог. Водночас застосовуються всі необхідні заходи захисту компонентів ІКС, що входять до зони з вищим рівнем кіберзахисту, від потенційного негативного впливу компонентів цієї ж ІКС, що входять до зони з нижчим рівнем кіберзахисту, відповідно до розділів V та VII цих Вимог.

4. Загальні вимоги до забезпечення кіберзахисту

1. ЕО відповідає за кіберзахист під час впровадження, модифікації, експлуатації, технічного обслуговування, ремонту, випробувань ІКС, їх компонентів та/або ПЗ на АС.

Кіберзахист ІКС АС забезпечує окремий підрозділ на майданчику АС, до складу якого входять фахівці, що мають необхідний рівень компетенції щодо кіберзахисту та ЯРБ.

2. Кіберзахист передбачає адміністративні (політика, процедури, дозволи), технічні (двері, замки, пломби), програмні (автентифікація та авторизація, антивірусний захист) та програмно-технічні (система виявлення вторгнень, міжмережеві екрани, пристрої однонаправленої передачі даних) заходи, які забезпечують:

попередження шкідливих дій через протидію та захист ІКС, їх компонентів, мережевого обладнання, ПЗ, даних та експлуатаційно-відновного резерву;

застосування засобів виявлення, затримки та реагування на шкідливі дії з метою мінімізації їх наслідків;

пом’якшення наслідків шкідливих дій, включно із заходами з відновлення нормального функціонування ІКС, їх компонентів та/або мережевого обладнання.

Заходи кіберзахисту гарантують, що будь-які ненавмисні дії та/або помилки персоналу не знижують кіберзахист та не підвищують вразливість ІКС, їх компонентів та ПЗ до шкідливих дій.

3. Під час проєктування ІКС визначаються проєктні заходи кіберзахисту, які реалізуються під час розроблення та виготовлення ПТК, ТЗА, ПЗ і забезпечують виконання вимог до кіберзахисту на етапах впровадження та експлуатації ІКС, їх компонентів та/або ПЗ.

4. Передача даних від ІКС АС до кризових центрів АС захищається та контролюється з використанням заходів кіберзахисту.

5. На етапах розроблення, впровадження, експлуатації та модифікації ІКС, їх компонентів та/або ПЗ застосовується управління конфігурацією для попередження несанкціонованих змін, впровадження надлишкових функцій, використання некоректних даних.

5. Культура кіберзахисту

1. Дотримання культури кіберзахисту є суттєвим фактором забезпечення кіберзахисту. Керівництво ЕО забезпечує повну інтеграцію культури кіберзахисту в загальну культуру безпеки.

2. Основою культури кіберзахисту є розуміння тими, хто виконує функції регулювання, управління або експлуатації АС, існування реальної кіберзагрози та важливості кіберзахисту.

3. Культура кіберзахисту забезпечується за допомогою здійснення діяльності, спрямованої на інформування персоналу та поліпшення розуміння

питань кіберзахисту (за допомогою плакатів, нагадувань, навчання, інструктажу, тестування).

4. Під час оцінювання культури кіберзахисту підтверджується, що:

вимоги кіберзахисту чітко документовані і добре розуміються керівництвом та персоналом;

процеси експлуатації ІКС, їх компонентів і ПЗ задокументовані;

керівництво та персонал розуміють і усвідомлюють важливість дотримання заходів контролю в межах політики та програми кіберзахисту;

обслуговування ІКС, їх компонентів та ПЗ забезпечує їх захист та експлуатацію відповідно до базових принципів і процедур кіберзахисту.

6. Координація між кіберзахистом та функціями ІКС АС

1. Гарантується, що засоби кіберзахисту, їх відмови та технічне обслуговування не мають негативного впливу (перешкоджання, затримання, викривлення) на інтерфейс «людина-машина», технічні характеристики та виконання ІКС функцій, важливих для безпеки АС, в умовах нормальної експлуатації та в разі порушень нормальної експлуатації.

2. Забезпечується запобігання негативному впливу засобів кіберзахисту, які реалізуються в певній ІКС, на сполучені ІКС.

3. Для забезпечення кіберзахисту в системах безпеки перевага надається зовнішнім (стосовно цих систем) засобам кіберзахисту.

4. Розробник ПТК, ТЗА, ПЗ виконує аналіз потенційного негативного впливу засобів кіберзахисту, який може призвести до порушення функціонування та/або погіршення характеристик ІКС (які регламентовані у Вимогах з ядерної та радіаційної безпеки до інформаційних та керуючих

систем, важливих для безпеки АС), у складі якої використовуються або можуть бути використані відповідні ПТК, ТЗА, ПЗ, та мінімізує цей вплив.

Результати вказаного аналізу та реалізовані в ПТК, ТЗА, ПЗ заходи запобігання негативному впливу засобів кіберзахисту на функціонування та характеристики ІКС відображаються в плані кіберзахисту розробника.

5. Відсутність негативного впливу реалізованих у ПТК, ТЗА, ПЗ засобів кіберзахисту на функціонування та характеристики ІКС підтверджується в процесі випробувань з кіберзахисту на майданчику розробника, які проводяться за програмою та методикою, погодженими Державною інспекцією ядерного регулювання України.

IV. Оцінювання кіберзахисту ІКС

1. Виявлення вразливостей ІКС до кіберзагроз

1. На кожному етапі життєвого циклу ІКС проводиться виявлення та документування потенційних кіберзагроз та вразливостей кіберзахисту ІКС, їх компонентів та ПЗ.

2. Розробник здійснює заходи з виявлення вразливостей та захисту від несанкціонованого фізичного доступу до ПТК, ТЗА, а ЕО – до ІКС та їх компонентів (наявність/відсутність замків/пломб на дверях шаф, сигналізації про відкриття дверей шаф).

3. Розробник оцінює порядок та засоби контролю доступу користувачів до ПТК, ТЗА, ПЗ, а ЕО – до ІКС, їх компонентів та ПЗ. Проведення такого оцінювання спрямоване на підтвердження того, що в ІКС, ПТК, ТЗА, ПЗ:

реалізована автентифікація та авторизація користувачів (зокрема, зчитування конфігураційних файлів, що містять деталі облікових записів користувачів) та унеможливлено анонімний доступ до ІКС, ПТК, ТЗА, ПЗ;

забезпечено доступ лише до обмеженого набору функцій, даних і частин ІКС згідно з принципом найменших привілеїв;

унеможливлено віддалений доступ до компонентів та ПЗ ІКС з-за меж АС та із загальностанційних мереж і забезпечено запобігання несанкціонованому віддаленому доступу (віддалений доступ дозволений лише для авторизованих користувачів);

відсутні обхідні облікові записи з правами адміністратора для забезпечення доступу;

забезпечено блокування користувача в разі трьох невдалих спроб доступу до облікових записів та інформування персоналу, який визначено у відповідних документах АС, про намагання несанкціонованого доступу до ІКС, ПТК, ТЗА, ПЗ;

забезпечені необхідні довжина паролів, їх надійність, складність та періодичність зміни;

регламентовані та документовані процедури створення, зміни, блокування та видалення облікових записів користувачів;

визначена періодичність перегляду прав користувачів.

4. Розробник здійснює заходи з виявлення вразливостей та блокування несанкціонованого підключення (зокрема безпровідного) будь-яких зовнішніх пристроїв (сервісного або випробувального обладнання, портативних комп’ютерів, мобільних пристроїв, змінних носіїв даних) до ПТК, ТЗА, а ЕО – до ІКС та їх компонентів.

5. ЕО періодично здійснює заходи з виявлення вразливостей та оцінює відповідність захисту локальних мереж цим Вимогам за допомогою перевірок:

правильності визначення периметра кіберзахисту;

правильності конфігурування мережевого обладнання;

забезпечення кіберзахисту портів на мережевому обладнанні та обмеження доступу до конкретних портів технічних засобів ІКС;

наявності/відсутності відповідного сегментування мереж (використання некерованого трафіку в керуючих мережах, можливість або відсутність доступу до ІКС із загальноблокової мережі, знаходження сервісів керуючої мережі безпосередньо в цій мережі);

використання міжмережевих екранів для розділення локальних мереж і наявності/відсутності підключень в обхід міжмережевих екранів;

наявності/відсутності демілітаризованих зон;

реалізації фільтрації вхідних та вихідних пакетів даних;

правил розмежування доступу.

6. Розробник оцінює організаційні заходи та процедури із забезпечення кіберзахисту середовища розроблення ПТК, ТЗА, ПЗ, зокрема наявність або відсутність:

відповідальних осіб, які забезпечують кіберзахист в організації;

документації з кіберзахисту, яка регламентує процес розроблення ПТК, ТЗА, ПЗ в організації;

локальної мережі середовища розроблення, відокремленої від інших локальних та зовнішніх мереж розробника;

заходів захисту від несанкціонованого доступу (зокрема, порядку авторизації та автентифікації працівників, які беруть участь у розробленні ПТК, ТЗА, ПЗ);

порядку зберігання конфіденційної інформації та документації;

обмежень на використання зовнішніх носіїв даних, портативних та мобільних пристроїв;

порядку проведення оцінювання кіберзахисту;

порядку реєстрації та реагування на кіберінциденти.

7. ЕО оцінює організаційні заходи та процедури із забезпечення кіберзахисту, зокрема наявність або відсутність:

відповідальних осіб, які забезпечують кіберзахист в організаційній структурі АС;

документації з кіберзахисту;

задокументованих процедур резервного копіювання та відновлення;

порядку проведення оцінювання кіберзахисту;

порядку автентифікації та авторизації користувачів;

максимально спрощеної та задокументованої мережевої архітектури;

контролю вхідних та вихідних потоків даних;

моніторингу кіберінцидентів.

8. Результати виявлення вразливостей ПТК, ТЗА, ПЗ до кіберзагроз документуються розробником у відповідному звіті та враховуються в плані кіберзахисту розробника (згідно з главою 3 розділу VIII цих Вимог).

9. Результати виявлення вразливостей ІКС, їх компонентів та ПЗ до кіберзагроз документуються ЕО у звіті з оцінки кіберзахисту та враховуються ЕО в програмі кіберзахисту і в плані кіберзахисту ІКС АС (згідно з главами 2, 4 розділу VIII цих Вимог). Якщо аналіз показує, що заходи кіберзахисту на рівні ІКС недостатні, ЕО в програмі кіберзахисту та плані кіберзахисту ІКС АС визначаються додаткові компенсуючі заходи.

2. Оцінювання повноти та достатності заходів кіберзахисту ІКС

1. Оцінювання повноти та достатності заходів кіберзахисту під час модифікації або впровадження нових ІКС здійснюється спеціально створеною групою, до складу якої входять представники ЕО (фахівці з експлуатації та обслуговування ІКС, ЯРБ, кіберзахисту), розробників ПТК, ТЗА і ПЗ.

ЕО здійснює організацію та проведення первинного оцінювання відповідності повноти та достатності заходів кіберзахисту діючих ІКС цим Вимогам, які вже експлуатуються на АС, у межах аналогічної окремої процедури та за допомогою ризик-інформованого підходу (терміни проведення такого оцінювання визначаються відповідно до пункту 8 розділу I цих Вимог).

Оцінювання відповідності цим Вимогам повноти та достатності заходів кіберзахисту конфігурації та параметрів ІКС на місці експлуатації виконується з метою підтвердження реалізації відповідних заходів захисту від потенційно можливих кіберзагроз. Якщо результати оцінки показують, що реалізовані заходи є недостатніми, визначаються вимоги до додаткових заходів кіберзахисту.

2. Оцінювання відповідності повноти та достатності заходів кіберзахисту ІКС цим Вимогам здійснюється з використанням таких методів для отримання необхідної інформації:

аналіз документації (політики, програми та планів кіберзахисту ІКС АС, звітів з оцінки кіберзахисту, навчальних матеріалів з кіберзахисту, технічної документації ІКС, інвентарних списків технічних засобів ІКС, списків контролю доступу, мережевої архітектури, операційних журналів, звітів про кіберінциденти, оцінки ризиків);

бесіди з персоналом (зокрема, адміністративним керівництвом, оперативним та ремонтним персоналом, фахівцями з кіберзахисту);

безпосереднє обстеження ІКС, їх компонентів та локальних мереж.

3. Під час аналізу документації проводиться оцінювання відповідності передбачених у документації заходів кіберзахисту цим Вимогам і вимогам політики, програми та планів кіберзахисту ІКС АС. Додатково оцінюється відповідність поточного стану кіберзахисту ідентифікованим кіберзагрозам.

4. Бесіди з персоналом спрямовані на оцінювання обізнаності персоналу з політикою та програмою кіберзахисту ІКС АС, ефективності підготовки кадрів щодо кіберзахисту, сприйняття персоналом загроз та ризиків, готовності до реагування на кіберінциденти, визначення обов'язків та розподілу відповідальності, ефективності культури кіберзахисту, заходів забезпечення конфіденційності.

5. У процесі безпосереднього обстеження оцінюються заходи забезпечення кіберзахисту (з урахуванням рівнів кіберзахисту ІКС), реалізації зон кіберзахисту, контролю доступу до ІКС, її компонентів та ПЗ (зокрема до експлуатаційно-відновного резерву), фактичної мережевої архітектури, перевірок і технічного обслуговування ІКС, управління конфігурацією, моніторингу та реєстрації кіберінцидентів.

6. На етапі збору інформації виконується оцінювання:

політики, програми та планів кіберзахисту ІКС АС і звітів з їх реалізації;

порядку, обсягу і результатів аналізу кіберзагроз та їх можливих наслідків;

застосування диференційованого підходу до забезпечення кіберзахисту, визначення рівнів кіберзахисту;

реалізації глибокоешелонованого кіберзахисту на АС;

наявності оцінки ризиків і забезпечення відповідних заходів кіберзахисту.

7. У процесі оцінювання відповідності повноти та достатності заходів кіберзахисту ІКС цим Вимогам виконується аналіз:

обізнаності персоналу з політикою та програмою кіберзахисту ІКС АС, спеціальної підготовки персоналу щодо забезпечення кіберзахисту та наявності відповідальних осіб, які забезпечують кіберзахист;

розподілу обов'язків і порядку доступу до ІКС;

наявності інвентарного переліку ІКС, їх компонентів, мережевого обладнання, ПЗ, експлуатаційно-відновного резерву, їх класифікації з кіберзахисту, відомостей про їх фізичне розміщення, функціональних схем ІКС і схеми зон кіберзахисту (водночас оцінюється відповідність зон кіберзахисту фізичному розміщенню ІКС та їх компонентів і відсутність входження обладнання більше ніж до однієї зони);

реалізації адміністративних, технічних і програмних засобів захисту та контролю несанкціонованого доступу до ІКС, їх компонентів, мережевого обладнання, ПЗ, експлуатаційно-відновного резерву;

порядку використання випробувального, налагоджувального обладнання, портативних пристроїв і зовнішніх носіїв даних у місцях розміщення ІКС та їх компонентів;

процедури утилізації непрацездатних або замінених технічних засобів та знищення носіїв даних;

обмеження доступу користувачів згідно з принципом найменших привілеїв;

можливостей несанкціонованого доступу до ІКС, їх компонентів, ПЗ і даних через мережеве обладнання, модеми, точки дротового або бездротового підключення, порти, незаблоковані ТЗА, сполучені ІКС;

реалізації виявлення вразливостей за допомогою відповідного аналізу та тестування;

достатності реалізованих у ІКС заходів кіберзахисту згідно з планами кіберзахисту ІКС АС;

упровадження компенсуючих заходів у разі, якщо необхідні заходи кіберзахисту не можуть бути застосовані в межах конкретної ІКС;

процедур упровадження або модифікації ІКС, їх компонентів, модифікації або установки нового ПЗ та оцінювання впливу цих змін на кіберзахист;

наявності в розробників ПТК, ТЗА, ПЗ системи менеджменту із забезпечення кіберзахисту, що підтверджується відповідними стандартами розробника;

заходів забезпечення кіберзахисту під час монтажу ІКС, їх компонентів;

програми й методики та результатів випробувань кіберзахисту ПТК, ТЗА, ПЗ у розробника після їх виготовлення та випробувань ІКС на АС;

заходів забезпечення кіберзахисту під час технічного обслуговування;

наявності задокументованих процедур реагування (дій персоналу, інформування, реалізації контрзаходів, відновлення, розслідування, застосування коригувальних заходів) на кіберінциденти, з урахуванням зовнішніх і внутрішніх (інсайдерських) кіберзагроз.

8. Під час використання ризик-інформованого підходу до оцінювання кіберзахисту діючих ІКС, ЕО виконує оцінювання ризиків з метою ідентифікації вразливостей до кібератак, що стосуються цих ІКС, і визначення потенційних наслідків успішного використання порушниками цих вразливостей. Впровадження заходів кіберзахисту базується на результатах такого оцінювання ризиків.

Під час оцінювання ризику виявляються та документуються конкретні поєднання кіберзагроз, вразливостей і наслідків, за результатами аналізу яких, у разі потреби, реалізуються додаткові заходи кіберзахисту, необхідні для запобігання або пом’якшення наслідків кібератак на ІКС.

Оцінювання ризиків ІКС передбачає:

визначення інтерфейсів і загальних умов експлуатації ІКС;

ідентифікацію та визначення характеру кіберзагроз;

виявлення вразливостей;

оцінювання імовірності виникнення негативних подій;

оцінювання наслідків негативних подій;

оцінювання рівня ризику;

визначення рівня прийнятного ризику;

визначення контрзаходів;

визначення остаточних ризиків та оцінювання їх сукупного впливу.

Вимоги до оцінювання кіберзахисту ІКС з використанням ризик-інформованого підходу визначаються та/або конкретизуються в програмі кіберзахисту та підтримуються в актуальному стані.

9. За результатами оцінювання кіберзахисту оформлюється звіт, який надається на погодження до Державної інспекції ядерного регулювання України.

Під час оцінювання та формування звіту забезпечується організаційний захист конфіденційної інформації, зокрема, маркування, збереження, передача та знищення підготовчих матеріалів, технічних записів, проєктів звіту та остаточного звіту. Застосовуються обмеження щодо використання електронних пристроїв і носіїв даних під час підготовки звіту.

3. Переоцінювання кіберзахисту ІКС

1. ЕО виконує періодичне переоцінювання кіберзахисту ІКС, їх компонентів та/або ПЗ згідно з процедурою, наведеною в главі 2 розділу IV цих Вимог, і за допомогою ризик-інформованого підходу протягом експлуатації ІКС, але не пізніше, ніж через один рік після впровадження нової ІКС або після первинного оцінювання діючої ІКС, і не рідше, ніж один раз на два роки з метою врахування появи нових кіберзагроз.

2. Додаткове переоцінювання кіберзахисту ІКС проводиться у разі:

модифікації ІКС, її компонентів та ПЗ;

виникнення кіберінциденту;

виявлення нових вразливостей ІКС;

інших змін, які впливають на ІКС, її компоненти та ПЗ (у разі наявності).

3. Під час переоцінювання здійснюються перевірки достатності реалізованих заходів кіберзахисту та їх відповідності вимогам нормативно-правових актів та програмі кіберзахисту.

4. За результатами переоцінювання кіберзахисту оформлюється звіт, який надається на погодження до Державної інспекції ядерного регулювання України.

Під час проведення переоцінювання та формування звіту забезпечується організаційний захист конфіденційної інформації, зокрема, належне маркування, збереження, передача та знищення підготовчих матеріалів, технічних записів, проєктів звіту та остаточного звіту. Застосовуються обмеження щодо використання електронних пристроїв і носіїв даних під час підготовки звіту.

V. Забезпечення кіберзахисту на етапі розроблення ІКС, їх компонентів та ПЗ

1. Загальні проєктні заходи кіберзахисту ІКС

1. Розроблення ПТК, ТЗА, ПЗ передбачає мінімізацію потенційних вразливостей та реалізацію загальних і додаткових (залежно від рівня кіберзахисту конкретної ІКС, у складі якої використовуються ПТК, ТЗА, ПЗ, що розробляються) засобів кіберзахисту. Під час проєктування враховуються результати виявлення вразливостей ПТК, ТЗА, ПЗ.

2. Реалізуються заходи для мінімізації прихованих функцій в ПЗ ПТК, ТЗА. Виконується аналіз програмного коду власної розробки (зокрема автоматично генерованого коду) та тестування ПЗ з метою підтвердження відсутності прихованих функцій в ПЗ ПТК, ТЗА.

3. ПЗ підлягає верифікації відповідно до Вимог з ядерної та радіаційної безпеки до інформаційних та керуючих систем, важливих для безпеки АС. У процесі верифікації ПЗ виконується перевірка реалізації у ПЗ ІКС та їх компонентах засобів кіберзахисту. Перевіряється відсутність негативного впливу засобів кіберзахисту на виконання функцій ІКС, важливих для безпеки АС.

Верифікація інструментальних засобів власної розробки, що використовуються для розроблення ПЗ, проводиться згідно з вимогами до ПЗ ІКС та їх компонентів. До інструментальних засобів сторонньої розробки застосовуються заходи забезпечення кіберзахисту згідно з главою 3 цього розділу.

4. Забезпечується відсутність впливу ПТК, ТЗА, ПЗ, що розробляються для використання в складі певної ІКС, на кіберзахист інших ІКС.

5. Під час проєктування ПТК, ТЗА, ПЗ враховується, що зв’язок між ІКС різних ступенів кіберзахисту ініціюється з боку ІКС більш високого ступеня кіберзахисту. У ПТК, ТЗА, ПЗ проєктними заходами забезпечується відсутність негативного впливу з боку інших ІКС.

Визначаються проєктні заходи для забезпечення достатньої впевненості в тому, що захист ПТК, ТЗА, ПЗ, що розробляються для використання в складі ІКС певного рівня кіберзахисту, не деградує внаслідок впливу з боку ІКС нижчого рівня кіберзахисту.

6. Використовуються засоби контролю та сигналізації фізичного доступу до ПТК, ТЗА, ПЗ, зміни їх конфігурації або їх відхилення від встановлених проєктом меж.

7. У ПТК мінімізується та обґрунтовується кількість точок доступу до локальних мереж.

8. Реалізуються засоби запобігання негативному впливу на ПТК, ТЗА, ПЗ з боку спеціального обладнання для тестування та технічного обслуговування.

9. Забезпечуються засоби захисту від несанкціонованого доступу до ПТК, ТЗА, ПЗ і мережевого обладнання.

Реалізуються засоби обмеження доступу до програмованих елементів і запобігання несанкціонованому створенню нових шляхів доступу до цих елементів.

10. Права доступу користувачів обмежують з урахуванням можливостей і наслідків потенційних кіберзагроз, керуючись принципом найменших привілеїв.

Доступ користувачів до ПТК, ТЗА, ПЗ реалізується з використанням технічних та/або програмних засобів автентифікації та авторизації. Тільки авторизовані користувачі отримують доступ і дозвіл на внесення змін у ПТК, ТЗА, ПЗ або їх конфігурацію.

Інтерфейс «людина-машина» (що використовується в процесі експлуатації та технічного обслуговування) надає доступ до ПЗ лише авторизованим користувачам, згідно з принципом найменших привілеїв.

Водночас унеможливлюється перехоплення або викривлення даних, що відображаються за допомогою інтерфейсу «людина-машина», спрямоване на запобігання або затримку дій оператора щодо виконання функцій, важливих для безпеки АС.

У ПЗ ІКС рівнів кіберзахисту К1, К2 застосовується процедура багатофакторної автентифікації, з використанням технічних засобів на основі отримання комбінації інформації про знання (зокрема, пароль, код) і про особисту власність (зокрема, ключ, карта з вбудованим мікрочипом). У ПЗ ІКС рівня кіберзахисту К3 застосовують щонайменше один з вищевказаних засобів автентифікації.

11. Визначаються потенційні напрями модифікації ПЗ, здатної спричинити помилкове виконання функцій. Під час верифікації підтверджується здатність виявлення такої модифікації. У ПТК, ТЗА реалізуються засоби перевірки коректності модифікацій, внесених у ПЗ.

12. ПТК, ТЗА, ПЗ проєктуються так, щоб мінімізувати вразливість ІКС.

Для раніше розробленого ПЗ використовуються такі параметри та конфігурація, які мінімізують вразливість ІКС (завдяки мінімізації функцій до необхідної межі або за допомогою існуючих засобів кіберзахисту ПЗ).

ПТК, ТЗА та їх елементи обираються, конфігуруються та налаштовуються так, щоб мінімізувати вразливість ІКС, до складу яких входять ці ПТК, ТЗА.

13. Під час проєктування конфігурації та/або встановлення параметрів програмованого обладнання реалізуються ефективні заходи захисту щодо:

управління вибірковим доступом користувачів до функцій ПЗ та до пам’яті ТЗА;

передачі даних у ІКС з нижчим рівнем кіберзахисту;

відстеження модифікацій ПЗ і параметрів ПТК, ТЗА.

14. У процесі випробувань кіберзахисту ПТК, ТЗА в їх фінальній конфігурації демонструється ефективність засобів кіберзахисту та відсутність їх негативного впливу на функції, які забезпечують ЯРБ.

Під час випробувань кіберзахисту виконується тестування для підтвердження достатності та коректності реалізованих у ПТК, ТЗА, ПЗ заходів кіберзахисту та виявлення потенційних вразливостей кіберзахисту ПТК, ТЗА, ПЗ.

Випробування кіберзахисту ПТК, ТЗА, ПЗ проводяться за програмою та методикою, погодженими Державною інспекцією ядерного регулювання України.

15. Заходи кіберзахисту, які не можуть бути інтегровані безпосередньо в ПТК, ТЗА, ПЗ, упроваджуються у складі ІКС окремо. Для застосування та технічного обслуговування таких окремих пристроїв вживаються додаткові адміністративні заходи управління.

16. Будь-яка інформація, що стосується проєктування, виготовлення, впровадження та експлуатації ПТК, ТЗА, ПЗ ідентифікується та, в разі потреби, позначається як інформація, щодо якої застосовуються відповідні організаційні заходи захисту від несанкціонованого розголошення, розкрадання, викривлення або знищення.

17. Унеможливлюються зміни ПЗ, що зберігається на носіях даних.

18. У ПТК, ТЗА, ПЗ реалізуються проєктні заходи щодо запобігання несанкціонованому віддаленому доступу та повного унеможливлення віддаленого доступу до них із-за меж АС та із загальностанційних мереж.

Віддалений доступ до ПТК, ТЗА, ПЗ рівнів кіберзахисту К1, К2, К3 здійснюється за умови авторизації та автентифікації користувачів з передбачених проєктом робочих місць, які відносяться до того ж або вищого рівня кіберзахисту, що й відповідні ПТК, ТЗА, ПЗ.

В обґрунтованих випадках допускається віддалений доступ до ПТК, ТЗА, ПЗ рівнів кіберзахисту К1, К2, К3 з передбачених проєктом робочих місць, які належать до нижчого рівня кіберзахисту ніж відповідні ПТК, ТЗА, ПЗ за умови виконання вимог глави 3 розділу ІІІ та розділу VII цих Вимог.

19. У ПТК та/або ТЗА забезпечується антивірусний захист.

Для ПТК та/або ТЗА рівнів кіберзахисту К1, К2 застосовуються організаційні та програмно-технічні засоби антивірусного захисту без застосування антивірусного ПЗ сторонньої розробки.

Для ПТК та/або ТЗА рівня кіберзахисту К3 застосовуються організаційні та програмно-технічні засоби антивірусного захисту та/або антивірусне ПЗ сторонньої розробки.

Застосування антивірусного ПЗ сторонньої розробки обґрунтовується та підтверджується відсутністю негативного впливу цього ПЗ на ІКС, їх компоненти та ПЗ, який може призвести до порушення функціонування та/або зміни характеристик ІКС, їх компонентів та ПЗ.

Для антивірусного ПЗ сторонньої розробки забезпечується регулярне оновлення антивірусних баз.

2. Забезпечення кіберзахисту на етапі розроблення ПТК, ТЗА, ПЗ

1. Розробники ПТК, ТЗА, ПЗ забезпечують надійні та контрольовані процеси забезпечення кіберзахисту, передбачені відповідною системою менеджменту.

2. Розроблення ПТК, ТЗА, ПЗ здійснюється в захищеному середовищі з реалізацією відповідних заходів кіберзахисту, які запобігають можливості впровадження програмного коду або даних, що можуть мати негативний вплив на виконання функцій ІКС, а також забезпечують захист інформації, пов’язаної з кіберзахистом ПТК, ТЗА, ПЗ, що розробляються. Проводиться періодичне оцінювання захищеності середовища розроблення та достатності застосовуваних заходів кіберзахисту.

3. У захищеному середовищі розроблення використовуються адміністративні заходи кіберзахисту, а саме управління конфігурацією, обмеження та контроль за використанням портативних пристроїв та змінних носіїв даних.

4. На стадії розроблення забезпечується запобігання несанкціонованому доступу до ПТК, ТЗА, їх елементів та ПЗ.

5. Розроблення ПЗ виконується з використанням ліцензованих та/або верифікованих засобів. Забезпечується ізоляція засобів розроблення ПЗ від зовнішніх мереж.

6. Під час розроблення ПТК, ТЗА, ПЗ враховуються потенційні кіберзагрози та реалізуються заходи захисту від цих загроз.

7. Передбачаються заходи проти впровадження прихованих функцій у прикладне або системне ПЗ.

8. Будь-які технічні та програмні засоби розробки, а також тестове обладнання перевіряються з метою підтвердження неможливості негативного впливу з їх боку та створення шляхів впровадження програмного коду або даних, що можуть мати негативний вплив на виконання функцій ІКС, у захищене середовище розроблення або у ПТК, ТЗА, ПЗ, що розробляються. До засобів розроблення та тестового обладнання застосовуються заходи кіберзахисту, аналогічні тим, що реалізуються в захищеному середовищі розроблення щодо ПТК, ТЗА, ПЗ, що розробляються.

9. Під час транспортування ПТК, ТЗА та/або ПЗ від підприємства-розробника до місця експлуатації застосовуються заходи кіберзахисту з метою запобігання будь-яким шкідливим втручанням.

3. Забезпечення кіберзахисту технічних засобів та програмного забезпечення сторонньої розробки

1. Виконується вхідний контроль усіх виробів сторонньої розробки, які

використовуються розробником для створення ПТК, ТЗА, ПЗ.

2. ПЗ сторонньої розробки, яке використовується розробником для створення ІКС та їх компонентів, підлягає обов'язковому тестуванню з метою перевірки правильності його функціонування та відсутності прихованих функцій.

3. Використання ПЗ сторонньої розробки у ІКС рівня кіберзахисту К1 мінімізується.

4. Для ТЗА та ПЗ сторонньої розробки, що використовуються у складі ІКС, підтверджується відповідність вимогам з кіберзахисту за допомогою проведення відповідних випробувань.

5. У ІКС використовується лише ліцензоване ПЗ сторонньої розробки. Функціональність ПЗ сторонньої розробки (зокрема операційних систем) обмежується лише тим набором можливостей, які необхідні для коректного виконання функцій ІКС. У разі використання неліцензованого ПЗ до нього застосовуються вимоги глави 1 розділу V цих Вимог.

VI. Забезпечення кіберзахисту на етапі впровадження

1. Забезпечення кіберзахисту під час монтажних і пусконалагоджувальних робіт і випробувань на АС

1. Монтаж, пусконалагоджувальні роботи та випробування на АС під час впровадження ІКС, їх компонентів та ПЗ проводяться в захищеному середовищі та з використанням обладнання, до якого застосовуються заходи кіберзахисту, аналогічні тим, що застосовуються до ІКС, їх компонентів та ПЗ, які підлягають

монтажу, пусконалагоджувальним роботам або випробуванням з урахуванням рівня кіберзахисту.

2. Виконується перевірка того, що обладнання, яке використовується під час монтажу, пусконалагоджувальних робіт і випробувань, не утворює нові шляхи для впровадження програмного коду або даних, що можуть мати негативний вплив на виконання функцій ІКС, у захищене середовище або в компоненти ІКС.

3. Реалізуються заходи кіберзахисту для управління та контролю переміщення даних, ПЗ та ТЗА в захищене середовище або за його межі.

2. Порядок доступу до ІКС під час впровадження

1. Доступ до ІКС, їх компонентів та ПЗ персоналу, що здійснює монтаж, ремонт, випробування обмежується відповідно до їх завдань, як щодо тривалості доступу, так і щодо конкретного переліку ІКС, їх компонентів та ПЗ, до яких дозволений доступ.

2. Виконується інструктаж персоналу щодо забезпечення кіберзахисту під час проведення робіт з ІКС, їх компонентами та ПЗ на АС.

3. ЕО забезпечує контроль за діями персоналу під час проведення будь-яких операцій з доступом до ІКС, їх компонентам та ПЗ на АС (зокрема, застосовується правило двох осіб).

VII. Забезпечення кіберзахисту в процесі експлуатації

1. Загальні заходи забезпечення кіберзахисту в процесі експлуатації

1. На АС реалізуються засоби захисту, що відокремлюють ІКС та/або

компоненти ІКС різних рівнів кіберзахисту.

2. Діяльність з модифікації ІКС планується та проводиться з урахуванням потенційних кіберзагроз.

3. Кількість точок доступу до локальних мереж мінімізується, наскільки це можливо, та обґрунтовується.

4. Реалізуються заходи виявлення спроб несанкціонованого входу та підключення до ІКС, їх компонентів та/або локальних мереж із подальшим застосуванням відповідних заходів реагування. Під час реалізації цих заходів забезпечується запобігання порушенням вимог ЯРБ.

Доступ до ІКС, їх компонентів та/або локальних мереж суворо контролюється для запобігання втручанню в їх роботу осіб, що не пройшли автентифікацію. Це забезпечується завдяки реалізації заходів технічного захисту (зокрема, замків на шафах, контролю фізичного доступу в приміщення), програмного обмеження і виявлення несанкціонованого доступу та впровадження відповідних організаційних заходів, які встановлюються відповідно до рівнів кіберзахисту конкретних ІКС та/або їх компонентів.

5. У межах управління конфігурацією усі постійні або тимчасові зміни, які стосуються оновлення ПЗ, побудови та зв’язків ІКС, доступу або підключення додаткових ліній передачі даних для випробувальних пристроїв або технічного обслуговування ідентифікуються та реєструються з метою виявлення змін, здатних негативно вплинути на кіберзахист.

6. Будь-які модифікації ІКС, їх компонентів або ПЗ виконуються відповідно до порядку, визначеного у Вимогах до проведення модифікацій ядерних установок та порядку оцінки їх безпеки.

7. Визначається порядок дій для своєчасного відновлення працездатності ІКС після кіберінциденту. Реалізуються заходи, які мінімізують ймовірність того, що вказаний порядок відновлення буде вразливим для тієї ж кіберзагрози.

8. ЕО здійснює безперервний моніторинг кіберзахисту ІКС, їх компонентів та ПЗ з метою виявлення кіберзагроз, порушень нормального функціонування ІКС, несанкціонованого доступу або змін. Результати моніторингу архівуються та захищаються від видалення або модифікації. Реалізується відповідний інтерфейс «людина-машина» для підтримки персоналу в процесі моніторингу кіберзахисту, ідентифікації, фіксації та сигналізації про кіберзагрози в усіх проєктних режимах роботи АС.

9. Реалізуються заходи запобігання створенню обхідних шляхів передачі даних між ІКС та/або компонентами ІКС різного рівня кіберзахисту через обладнання та лінії передачі даних, що використовуються для контролю, технічного обслуговування та відновлення.

10. Технічне обслуговування ІКС охоплює засоби забезпечення кіберзахисту та передбачає:

періодичне тестування почергово на кожному каналі ІКС, виведеному в технічне обслуговування;

перегляд програмних журналів роботи ІКС;

огляд стану компонентів ІКС;

моніторинг функціонування ІКС у режимі реального часу;

дії з виявлення, попередження та пом’якшення наслідків деградації компонентів;

дії з діагностування, ремонту або заміни компонентів, що відмовили.

Під час проведення технічного обслуговування реалізуються заходи кіберзахисту, які попереджують впровадження в ІКС та/або її компоненти

програмного коду або даних, що можуть мати негативний вплив на виконання функцій ІКС.

Під час проведення технічного обслуговування реалізуються заходи кіберзахисту обладнання, аналогічні тим, що застосовні до відповідної ІКС, з урахуванням рівня її кіберзахисту. Забороняються будь-які підключення обладнання для технічного обслуговування, якщо це не є необхідним або не проводяться відповідні дії з технічного обслуговування.

У разі, якщо для виконання певних дій з технічного обслуговування ІКС необхідно тимчасово відключити окремі засоби забезпечення кіберзахисту, на період проведення цих дій приймаються компенсуючі заходи кіберзахисту.

Після проведення технічного обслуговування або тестування ІКС виконується перевірка конфігурації ПЗ та значень уставок з метою попередження їх несанкціонованої зміни.

11. Дії персоналу під час експлуатації, технічного обслуговування та випробувань ІКС контролюються згідно з регламентованими на АС процедурами (зокрема, застосовується правило двох осіб).

12. У разі використання будь-яких змінних носіїв даних у процесі експлуатації, технічного обслуговування та/або випробувань здійснюється контроль їх вмісту перед під’єднанням до ІКС з метою запобігання внесенню до ІКС програмного коду або даних, що можуть мати негативний вплив на виконання функцій ІКС, та після від’єднання від ІКС для запобігання несанкціонованому копіюванню даних.

13. У разі заміни окремих елементів ІКС під час модифікації, технічного обслуговування та/або ремонту забезпечується вилучення із замінених елементів будь-яких даних і ПЗ з метою запобігання використанню цієї інформації для підготовки та проведення кібератак. У разі неможливості вилучення даних та ПЗ із елемента ІКС, такі елементи підлягають знищенню

або зберіганню із дотриманням відповідних заходів фізичного захисту, кіберзахисту та захисту від несанкціонованого доступу.

2. Заходи забезпечення кіберзахисту в процесі експлуатації (рівень К1)

1. Зв’язки ІКС та/або їх компонентів рівня кіберзахисту К1 обмежуються іншими ІКС та/або їх компонентами рівнів кіберзахисту К1 та К2. Зв’язок ІКС та/або їх компонентів рівня кіберзахисту К1 з ІКС та/або їх компонентами рівня кіберзахисту К3 дозволяється лише за умови детального обґрунтування й аналізу ризиків кіберзахисту.

2. Зв’язок здійснюється в односторонньому напрямку від ІКС та/або їх компонентів рівня кіберзахисту К1 до ІКС та/або їх компонентів рівнів кіберзахисту К2 або К3. Забезпечується фізична (апаратна) неможливість передачі даних у зворотному напрямку.

3. Передача даних від ІКС та/або їх компонентів рівня кіберзахисту К2 до ІКС та/або їх компонентів рівня кіберзахисту К1 дозволяється лише за умови детального обґрунтування й аналізу ризиків кіберзахисту та обмежується лише обов’язковими даними, без яких неможливе виконання функцій у повному обсязі. Достовірність будь-яких даних, що передаються з ІКС та/або їх компонентів рівня кіберзахисту К2 до ІКС та/або їх компонентів рівня кіберзахисту К1 контролюється (зокрема, формат даних, контроль часу передачі, контрольні суми).

4. Оновлення ПЗ і зміни конфігурації ІКС та/або їх компонентів рівня кіберзахисту К1 здійснюються тільки з використанням місцевих засобів апаратного блокування (зокрема, ключів, пломб) та одночасно лише в одному каналі ІКС.

5. Двонаправлена передача даних між ІКС та/або їх компонентами рівня кіберзахисту К1 та обладнанням для технічного обслуговування виконується з використанням окремої виділеної лінії передачі даних, яка відокремлена від інших мереж. Ця лінія передачі даних захищається технічними, програмними та адміністративними засобами.

6. Доступ до ІКС та/або їх компонентів рівня кіберзахисту К1 контролюється за допомогою сигналізації на блоковому, резервному або місцевих щитах управління.

7. Неавторизовані користувачі та непередбачені проєктом ІКС та/або їх компоненти не можуть зчитувати дані або змінювати дані та ПЗ. Водночас забезпечується необхідний доступ для авторизованих користувачів і передбачених проєктом ІКС та/або їх компонентів.

8. Основні заходи захисту (зокрема технічного захисту, приєднання блокуючих пристроїв) здійснюються на рівні ІКС. Основні вимоги щодо ПЗ можуть доповнювати захисні заходи на системному рівні.

9. ПЗ конфігурується та налаштовується так, щоб збирати необхідну інформацію для періодичної перевірки кіберзахисту ІКС та складання відповідного звіту.

3. Заходи забезпечення кіберзахисту в процесі експлуатації (рівень К2)

1. Зв’язки ІКС та/або їх компонентів рівня кіберзахисту К2 обмежуються іншими ІКС та/або їх компонентами рівнів кіберзахисту К1, К2 та К3. Зв’язок здійснюється в односторонньому напрямку від ІКС та/або їх компонентів рівня кіберзахисту К2 до ІКС та/або їх компонентів рівня кіберзахисту К3.

Одностороння передача даних забезпечуються використанням відповідних технічних і програмних засобів (наприклад, спеціального обладнання для фільтрації потоків даних).

2. Передача даних від ІКС та/або їх компонентів рівня кіберзахисту К3 до ІКС та/або їх компонентів рівня кіберзахисту К2 обмежується та використовується лише в обґрунтованих випадках.

3. Унеможливлюється зміна ПЗ та конфігурації ІКС та/або їх компонентів рівня кіберзахисту К2 з боку ІКС та/або їх компонентів рівня кіберзахисту К3.

4. Оновлення ПЗ та зміни конфігурації ІКС та/або їх компонентів рівня кіберзахисту К2 здійснюються одночасно лише в одному каналі ІКС, протягом заздалегідь визначених часових проміжків, та захищаються відповідними блокуваннями. Двонаправлена передача даних між ІКС та/або їх компонентами рівня кіберзахисту К2 та обладнанням для технічного обслуговування виконується з використанням окремої виділеної лінії передачі даних, яка відокремлена від інших мереж. Ця лінія передачі даних захищається технічними, програмними та адміністративними засобами.

4. Заходи забезпечення кіберзахисту в процесі експлуатації (рівень К3)

1. Для ІКС рівня кіберзахисту К3 застосовуються загальні заходи забезпечення кіберзахисту згідно з главою 1 розділу VII цих Вимог.

2. Зв’язки ІКС та/або їх компонентів рівня кіберзахисту К3 обмежуються іншими ІКС та/або їх компонентами рівнів кіберзахисту К1, К2 та К3. Зв’язок ІКС та/або їх компонентами рівня кіберзахисту К3 з іншими комп’ютерними системами або мережами передачі даних обґрунтовується, реалізується з

використанням демілітаризованих зон та застосовується лише в разі, якщо це не ставить під загрозу дотримання вимог з ЯРБ, що встановлені для цієї ІКС та/або їх компонентів.

Якщо у ІКС та/або їх компонентів рівня кіберзахисту К3 передбачена можливість передачі даних до ІКС та/або їх компонентів рівня кіберзахисту К2, то не допускається зв'язок цих ІКС та/або їх компонентів рівня кіберзахисту К3 з іншими комп'ютерними системами або мережами передачі даних, які не відносяться до рівнів кіберзахисту К1, К2, К3.

3. Гарантується відсутність негативного впливу ІКС рівня кіберзахисту К3 на ІКС, їх компоненти та/або ПЗ рівнів кіберзахисту К1, К2.

5. Контроль змін під час модифікації ІКС

1. Необхідні дії з модифікації ПЗ здійснюються з урахуванням потенційних кіберзагроз.

Проводиться оцінювання модифікації на місці експлуатації для перевірки того, що вжиті відповідні заходи захисту від потенційних кіберзагроз.

2. Визначаються особливі режими в процесі введення в експлуатацію та модифікації ІКС, які охоплюють:

інтерфейси та спеціальні можливості ІКС та/або їх компонентів, що блокуються під час роботи на потужності;

функції включення аварійної сигналізації, що блокуються під час модифікації;

використання станцій обслуговування та інструментальних засобів;

необхідність проведення дій оператором з визначеного проєктом місця.

Для забезпечення працездатності та кіберзахисту ІКС та/або їх компонентів будь-які особливі режими компенсуються додатковими заходами під час та/або після модифікації.

3. Обладнання, що використовується під час модифікації ПЗ на місці експлуатації, обирається зважаючи на рівень його потенційної загрози кіберзахисту ІКС та/або їх компонентів, у яких використовується це ПЗ.

4. Нові версії ПЗ, які здійснюють пов’язані з кіберзахистом зміни, підлягають верифікації для підтвердження того, що вимоги з кіберзахисту враховані.

5. Процедура інсталяції ПЗ на місці його експлуатації передбачає перевірки працездатності ПЗ, які проводяться до повномасштабного введення ІКС та/або їх компонентів в експлуатацію.

VIII. Вимоги до документів, що обґрунтовують кіберзахист

1. Загальні вимоги до документації

1. Документи, що обґрунтовують кіберзахист ІКС, їх компонентів та/або ПЗ, містять достатню інформацію для демонстрації того, що заходи кіберзахисту спроєктовані, впроваджені та підтримуються відповідно до визначеного рівня кіберзахисту та забезпечують належний захист від кіберзагроз.

2. Забезпечується організаційний захист документів, що обґрунтовують кіберзахист ІКС, їх компонентів та/або ПЗ, від несанкціонованого розкриття, фальсифікації, вилучення або знищення, відповідно до визначеного рівня кіберзахисту.

2. Програма кіберзахисту

1. ЕО розробляє та впроваджує програму кіберзахисту для кожного

енергоблока АС, а також окрему програму кіберзахисту майданчика АС (для сукупності усіх ІКС рівнів кіберзахисту К1, К2, К3, які знаходяться за межами енергоблоків).

2. Програма кіберзахисту регламентує:

заходи кіберзахисту для сукупності усіх ІКС енергоблока АС або сукупності усіх ІКС рівнів кіберзахисту К1, К2, К3, які знаходяться за межами енергоблоків;

заходи для реалізації цілей, визначених у політиці кіберзахисту;

відсутність впливу кіберзахисту на ЯРБ й заходів забезпечення кіберзахисту на виконання функцій ІКС;

необхідність розроблення планів реалізації заходів кіберзахисту.

3. Програма кіберзахисту описує заходи з реалізації стратегії глибокоешелонованого захисту та її використання для захисту, виявлення, реагування і відновлення ІКС після кібератак.

4. Програма кіберзахисту встановлює рівні кіберзахисту ІКС, їх компонентів та ПЗ і розподіл на зони кіберзахисту й визначає та/або конкретизує заходи кіберзахисту для ІКС, їх компонентів та ПЗ відповідно до рівнів їх кіберзахисту.

5. Програма кіберзахисту визначає:

відповідальних осіб, які забезпечують кіберзахист, та їх обов’язки на етапах впровадження, експлуатації та модифікації ІКС;

порядок доступу до ІКС, їх компонентів, ПЗ, конфігураційних даних та інструментальних засобів на етапах впровадження, експлуатації і модифікації ІКС;

процес ідентифікації та захисту інформації (документація, бази даних, файли, ПЗ), що стосується кіберзахисту ІКС, та розкриття, викривлення або знищення якої може негативно вплинути на кіберзахист.

6. Програма кіберзахисту передбачає проведення та документування оцінювання і періодичного переоцінювання кіберзахисту ІКС (згідно з розділом IV цих Вимог).

7. Програма кіберзахисту за результатами оцінювання, періодичного переоцінювання і випробувань кіберзахисту ІКС, а також реалізації планів кіберзахисту визначає додаткові заходи кіберзахисту та/або конкретизує існуючі заходи кіберзахисту, враховує потенційні вразливості кіберзахисту на етапах впровадження, експлуатації та модифікації ІКС і регламентує процедури усунення цих вразливостей.

8. Програма кіберзахисту визначає та/або конкретизує вимоги до оцінювання кіберзахисту ІКС за допомогою ризик-інформованого підходу та регламентує розроблення відповідної методики оцінювання.

9. Програма кіберзахисту встановлює вимоги до виявлення, реагування та повідомлення про кіберінциденти. Деталізація цих вимог надається в плані реагування на кіберінциденти (згідно з главою 5 розділу VIII цих Вимог).

10. Програма кіберзахисту надається на погодження до Державної інспекції ядерного регулювання України.

11. Перегляд програми кіберзахисту здійснюється не рідше ніж один раз на рік та в разі:

кіберінцидентів на АС;

змін у політиці кіберзахисту;

інших змін, які впливають на програму кіберзахисту (в разі потреби).

12. У разі необхідності внесення змін до програми кіберзахисту за результатами її перегляду, розроблюється сповіщення про зміни в програмі кіберзахисту, в якому наводиться перелік змін та обґрунтування щодо безпеки їх впровадження. Сповіщення про зміни надається на погодження до Державної інспекції ядерного регулювання України.

3. Документи розробника щодо кіберзахисту

1. Розробник ПТК, ТЗА, ПЗ, які належать до рівнів кіберзахисту К1, К2 або К3, у технічному завданні (технічній специфікації, технічних умовах) визначає рівень кіберзахисту ПТК, ТЗА, ПЗ, з урахуванням рівня кіберхзахисту ІКС, у складі якої використовуються ці ПТК, ТЗА, ПЗ, і встановлює вимоги до проєктних заходів кіберзахисту, які реалізуються у ПТК, ТЗА, ПЗ на етапі їх розроблення.

Перегляд технічних умов щодо вимог до кіберзахисту ПТК і ТЗА, які виготовляються серійно, виконується в разі:

змін у ПТК та/або ТЗА, які впливають на кіберзахист;

кіберінцидентів, пов’язаних з цими ПТК та/або ТЗА;

виявлення вразливостей або недостатності реалізованих заходів кіберзахисту, пов’язаних з цими ПТК та/або ТЗА, за результатами оцінювання або періодичного переціновання (згідно з розділом IV цих Вимог);

інших змін, які впливають на технічні умови щодо вимог до кіберзахисту (у разі потреби).

Технічне завдання, технічна специфікація, технічні умови та відповідні зміни й доповнення до них надаються на погодження до Державної інспекції ядерного регулювання України.

2. Розробник ПТК, ТЗА, ПЗ, які належать до рівнів кіберзахисту К1, К2 або К3, розробляє план кіберзахисту розробника для першого (головного) комплекту ПТК або першого (головного) зразка ТЗА, а також для наступних комплектів ПТК і зразків ТЗА.

Розробник ПТК і ТЗА, які виготовляються серійно, розробляє план кіберзахисту розробника та періодично виконує його перегляд (не рідше ніж один раз на рік) та в разі:

змін у ПТК та/або ТЗА, які впливають на кіберзахист;

кіберінцидентів, пов’язаних з цими ПТК та/або ТЗА;

виявлення вразливостей або недостатності реалізованих заходів кіберзахисту, пов’язаних з цими ПТК та/або ТЗА, за результатами оцінювання або періодичного переціновання (згідно з розділом IV цих Вимог);

інших змін, які впливають на план кіберзахисту розробника (в разі потреби).

3. У плані кіберзахисту розробника наводиться перелік проєктних заходів кіберзахисту, які реалізуються у ПТК, ТЗА, ПЗ на етапі їх розроблення.

4. План кіберзахисту розробника визначає та/або конкретизує:

комплекс кроків і дій щодо реалізації проєктних заходів кіберзахисту на етапі розроблення ПТК, ТЗА, ПЗ згідно з главою 1 розділу V цих Вимог і додаткові умови, які впливають на реалізацію цих заходів;

заходи, що гарантують відсутність впливу засобів забезпечення кіберзахисту на виконання функцій ПТК, ТЗА, ПЗ;

процес і вимоги до виявлення вразливостей ПТК, ТЗА, ПЗ до кіберзагроз згідно з главою 1 розділу IV цих Вимог.

5. План кіберзахисту розробника для першого (головного) комплекту ПТК або першого (головного) зразка ТЗА надається на погодження до Державної інспекції ядерного регулювання України.

Плани кіберзахисту розробника для наступних комплектів ПТК або зразків ТЗА надаються на погодження до Державної інспекції ядерного регулювання України в разі:

змін у ПТК та/або ТЗА, які впливають на кіберзахист;

кіберінцидентів, пов’язаних з цими ПТК та/або ТЗА.

План кіберзахисту розробника для ПТК і ТЗА, які виготовляються серійно, та зміни до нього надаються на погодження до Державної інспекції ядерного регулювання України.

6. Для підтвердження реалізації плану кіберзахисту розробника проводяться випробування кіберзахисту на майданчику розробника за відповідною програмою та методикою.

7. Програма та методика випробувань кіберзахисту на майданчику розробника визначає:

мету випробувань;

об’єкт випробувань;

умови проведення випробувань;

перелік відповідальних осіб, які забезпечують проведення випробувань і забезпечення безпеки та кіберзахисту під час випробувань;

заходи з безпеки та кіберзахисту, зокрема вимоги до середовища випробувань, у якому реалізовані заходи кіберзахисту;

перелік документів, які надаються на випробування;

обсяг і послідовність проведення випробувань та перевірок;

методи підтвердження достатності та коректності реалізованих у ПТК, ТЗА, ПЗ заходів кіберзахисту і підтвердження захищеності ПТК, ТЗА, ПЗ від кібератак;

методи підтвердження відсутності впливу заходів забезпечення кіберзахисту на виконання функцій ПТК, ТЗА, ПЗ;

критерії аналізу звіту з виявлення вразливостей ПТК, ТЗА, ПЗ до кіберзагроз;

критерії успішності випробувань і реалізації плану кіберзахисту розробника;

вимоги до оформлення результатів випробувань.

8. Програма та методика випробувань кіберзахисту на майданчику розробника для першого (головного) комплекту ПТК або першого (головного) зразка ТЗА надається на погодження до Державної інспекції ядерного регулювання України, як окремий документ або в складі плану з валідації, який розробляється згідно з Вимогами з ядерної та радіаційної безпеки до інформаційних та керуючих систем, важливих для безпеки АС.

Програма та методика випробувань кіберзахисту на майданчику розробника для наступних комплектів ПТК або зразків ТЗА надається на погодження до Державної інспекції ядерного регулювання України, як окремий документ або в складі програми та методики приймального контролю, яка розробляється згідно з Вимогами з ядерної та радіаційної безпеки до інформаційних та керуючих систем, важливих для безпеки атомних станцій, в разі:

змін у ПТК та/або ТЗА, які впливають на кіберзахист;

кіберінцидентів, пов’язаних з цими ПТК та/або ТЗА.

Програма та методика випробувань кіберзахисту на майданчику розробника для ПТК і ТЗА, які виготовляються серійно, надається на погодження до Державної інспекції ядерного регулювання України, як окремий документ або в складі програми та методики приймальних випробувань на майданчику розробника, яка розробляється згідно з Вимогами з ядерної та радіаційної безпеки до інформаційних та керуючих систем, важливих для безпеки АС.

9. Результати реалізації плану кіберзахисту розробника для першого (головного) комплекту ПТК і першого (головного) зразка ТЗА надаються Державній інспекції ядерного регулювання України, як окремий звіт або в складі звіту з валідації, який розробляється згідно з Вимогами з ядерної та радіаційної безпеки до інформаційних та керуючих систем, важливих для безпеки АС для обґрунтування технічного рішення про проведення монтажу.

Результати реалізації плану кіберзахисту розробника для наступних комплектів ПТК і зразків ТЗА надаються Державній інспекції ядерного регулювання України до погодження технічного рішення про проведення монтажу, як окремий звіт, в разі:

змін у ПТК та/або ТЗА, які впливають на кіберзахист;

кіберінцидентів, пов’язаних з цими ПТК та/або ТЗА.

Звіт з результатами реалізації плану кіберзахисту розробника або змін до плану кіберзахисту розробника для ПТК і ТЗА, які виготовляються серійно, надаються Державній інспекції ядерного регулювання України в строк не більше одного року після погодження плану кіберзахисту розробника або зміни до нього.

4. План кіберзахисту ІКС АС

1. План кіберзахисту ІКС АС розробляється ЕО щодо кожної окремої ІКС, яка впроваджується або модифікується на АС.

2. План кіберзахисту ІКС АС розробляється ЕО щодо діючих ІКС, якщо:

виконується модифікація ІКС, її компонентів та/або ПЗ, яка впливає на кіберзахист;

у звіті за результатами виявлення вразливостей до кіберзагроз, первинного оцінювання кіберзахисту ІКС (згідно з главами 1, 2 розділу IV цих Вимог) та випробувань заходів кіберзахисту діючої ІКС визначена необхідність реалізації додаткових заходів кіберзахисту.

3. План кіберзахисту ІКС АС щодо ІКС, яка впроваджується або модифікується на АС, визначає та/або конкретизує:

комплекс кроків і дій щодо реалізації заходів кіберзахисту на етапі впровадження ІКС, її компонентів і ПЗ (згідно з розділом VI цих Вимог) і в процесі експлуатації ІКС, її компонентів і ПЗ (згідно з розділом VII цих Вимог) та додаткові умови, які впливають на реалізацію цих заходів;

заходи, що гарантують відсутність впливу засобів забезпечення кіберзахисту на виконання функцій ІКС, її компонентів і ПЗ;

процес і вимоги до виявлення вразливостей ІКС, її компонентів і ПЗ до кіберзагроз (згідно з главою 1 розділу IV цих Вимог);

процес і вимоги до оцінювання повноти та достатності заходів кіберзахисту ІКС (згідно з главою 2 розділу IV цих Вимог);

перелік змін, які необхідно внести до програми кіберзахисту.

4. План кіберзахисту ІКС АС щодо ІКС, яка впроваджується або модифікується на АС, надається на погодження до Державної інспекції ядерного регулювання України до погодження технічного рішення про проведення монтажу об’єкта модифікації.

5. Результати реалізації плану кіберзахисту ІКС АС щодо ІКС, яка впроваджується або модифікується на АС, наводяться в звіті з реалізації плану кіберзахисту ІКС АС. У цьому звіті на підставі виконаного оцінювання та випробувань відображається реалізація заходів, зазначених у плані кіберзахисту ІКС АС.

Звіт з реалізації плану кіберзахисту ІКС АС надається на погодження до Державної інспекції ядерного регулювання України до введення об’єкта модифікації в дослідну експлуатацію.

6. План кіберзахисту ІКС АС щодо діючих ІКС визначає та/або конкретизує:

комплекс кроків і дій щодо реалізації додаткових заходів кіберзахисту для усунення невідповідності вимогам за результатами визначення вразливостей до кіберзагроз, первинного оцінювання кіберзахисту ІКС (згідно з главами 1, 2 розділу IV цих Вимог), випробувань заходів кіберзахисту діючої ІКС, та додаткові умови, які впливають на реалізацію цих заходів;

заходи, які гарантують відсутність впливу засобів забезпечення кіберзахисту на виконання функцій ІКС;

процес і вимоги до підтримки передбачених заходів;

процес і вимоги до переоцінювання повноти та достатності заходів кіберзахисту ІКС (згідно з главою 3 розділу IV цих Вимог);

перелік змін, які необхідно внести до програми кіберзахисту.

7. План кіберзахисту ІКС АС для діючих ІКС надається на погодження до Державної інспекції ядерного регулювання України.

8. Результати реалізації плану кіберзахисту ІКС АС для діючих ІКС наводяться у звіті з реалізації плану кіберзахисту ІКС АС. У цьому звіті на підставі виконаного переоцінювання та випробувань відображається реалізація заходів з кіберзахисту, зазначених у плані кіберзахисту ІКС АС.

Звіт з реалізації плану кіберзахисту ІКС АС надається на погодження до Державної інспекції ядерного регулювання України.

9. До чинного плану кіберзахисту ІКС АС вносяться зміни, якщо у звіті за результатами переоцінювання кіберзахисту ІКС (згідно з главою 3 розділу IV цих Вимог) визначена необхідність реалізації додаткових заходів кіберзахисту.

10. У змінах до чинного плану кіберзахисту ІКС АС визначається та/або конкретизується:

комплекс кроків і дій щодо реалізації додаткових заходів кіберзахисту для усунення невідповідності регламентованим вимогам, за результатами

переоцінювання кіберзахисту ІКС (згідно з главою 3 розділу IV цих Вимог), та додаткові умови, які впливають на реалізацію цих заходів;

заходи, що гарантують відсутність впливу засобів забезпечення кіберзахисту на виконання функцій ІКС;

процес і вимоги до підтримки передбачених заходів;

процес і вимоги до переоцінювання повноти та достатності заходів кіберзахисту ІКС (згідно з главою 3 розділу IV цих Вимог);

перелік змін, які необхідно внести до програми кіберзахисту ІКС АС.

11. Зміни до плану кіберзахисту ІКС АС надаються на погодження до Державної інспекції ядерного регулювання України.

12. Результати реалізації змін у плані кіберзахисту ІКС АС наводяться у звіті з реалізації змін плану кіберзахисту ІКС АС. У цьому звіті на підставі виконаного переоцінювання та випробувань відображається реалізація заходів із кіберзахисту, зазначених у змінах до плану кіберзахисту ІКС АС.

Звіт з реалізації змін плану кіберзахисту ІКС АС надається на погодження до Державної інспекції ядерного регулювання України.

13. Для підтвердження реалізації плану або змін до плану кіберзахисту ІКС АС, а також для перевірки відповідності встановленим вимогам наявних заходів кіберзахисту діючої ІКС проводяться випробування кіберзахисту на майданчику АС за відповідною програмою та методикою.

14. Програма та методика випробувань кіберзахисту на майданчику АС визначає:

мету випробувань;

об’єкт випробувань;

умови проведення випробувань;

перелік відповідальних осіб, які забезпечують проведення випробувань і забезпечення безпеки та кіберзахисту під час випробувань;

заходи з безпеки та кіберзахисту, зокрема вимоги до середовища випробувань, у якому реалізовані відповідні заходи кіберзахисту;

перелік документів, які надаються на випробування;

обсяг і послідовність проведення випробувань та перевірок;

методи підтвердження достатності та коректності реалізованих у ІКС заходів кіберзахисту й підтвердження захищеності ІКС, її компонентів і ПЗ від кібератак;

методи підтвердження відсутності впливу заходів кіберзахисту на виконання функції ІКС, її компонентів і ПЗ;

критерії аналізу звітів з оцінювання або переоцінювання кіберзахисту ІКС;

критерії успішності випробувань і реалізації плану кіберзахисту АС;

вимоги до оформлення результатів випробувань.

15. Програма та методика випробувань кіберзахисту на майданчику АС надається на погодження до Державної інспекції ядерного регулювання України як окремий документ або у складі програми та методики попередніх (комплексних) випробувань ІКС на енергоблоці АС.

5. План реагування на кіберінциденти

1. ЕО розробляє план реагування на кіберінциденти, який містить процедури ідентифікації та реагування на можливе відхилення від встановлених проєктом меж. Такий план визначає порядок дій персоналу, спрямованих на запобігання розвитку кібератак та відновлення після кіберінцидентів.

2. План реагування на кіберінциденти передбачає дії з накопичення та збереження інформації для подальшого розслідування кіберінциденту.

3. План реагування на кіберінциденти визначає розподіл обов'язків персоналу, що входить до складу команди реагування на кіберінциденти. До складу команди входить не лише персонал з кіберзахисту, але й персонал, ознайомлений зі специфікою побудови та функціонування ІКС.

4. План реагування на кіберінциденти визначає перелік ПЗ, даних і конфігураційних файлів, які зберігаються у сховищах, фізично відділених від ІКС (з метою запобігання відмовам із загальної причини), та використовуються для відновлення роботи ІКС. Заходи кіберзахисту застосовуються для захисту вказаних сховищ від розкрадання, фальсифікації, пошкодження або видалення.

5. План реагування на кіберінциденти передбачає проведення практичного навчання працівників. Періодично проводяться перевірки знань і навичок персоналу та тренування персоналу відповідно до плану реагування на кіберінциденти. План переглядається не рідше ніж один раз на рік та доповнюється, в разі потреби.

6. План реагування на кіберінциденти надається на погодження до Державної інспекції ядерного регулювання України.

Директор Департаменту з питань безпеки
ядерних установок – заступник
Головного державного інспектора
з ядерної та радіаційної безпеки України **Борис СТОЛЯРЧУК**

Аналіз регуляторного впливу

до проєкту наказу Державної інспекції ядерного регулювання України
«Про затвердження Вимог до кіберзахисту інформаційних та керуючих систем атомних станцій для забезпечення ядерної та радіаційної безпеки»

І. Визначення проблеми

Проєкт наказу «Про затвердження Вимог до кіберзахисту інформаційних та керуючих систем атомних станцій для забезпечення ядерної та радіаційної безпеки» (далі – проєкт НПА) розроблено Державною інспекцією ядерного регулювання України (далі – Держатомрегулювання) з метою удосконалення системи нормативно-правового регулювання ядерної та радіаційної безпеки (далі – ЯРБ) у частині кіберзахисту інформаційних та керуючих систем (далі – ІКС) атомних станцій (далі – АС) та приведення національної нормативної бази у відповідність до міжнародних норм.

Станом на 2021 рік в Україні знаходяться в експлуатації 13 енергоблоків із реакторними установками (далі – РУ) типу ВВЕР-1000 (В-320 (11 енергоблоків), В-302 (1 енергоблок) і В-338 (1 енергоблок)) та 2 енергоблоки з РУ ВВЕР-440/В-213 загальною встановленою потужністю 13 835 МВт. Оператором цих енергоблоків є Державне підприємство «Національна атомна енергогенеруюча компанія «Енергоатом» (далі – ДП «НАЕК «Енергоатом»). Безпосередню експлуатацію енергоблоків здійснюють відокремлені підрозділи (далі – ВП) ДП «НАЕК «Енергоатом», а саме: ВП «Запорізька АЕС», ВП «Рівненська АЕС», ВП «Хмельницька АЕС», ВП «Южно-Українська АЕС».

Управління технологічним процесами на АС є автоматизованим та здійснюється за допомогою ІКС. Проєктні ІКС АС переважно були побудовані на базі аналогових технічних засобів автоматизації без використання програмного забезпечення (далі – ПЗ). Таким чином, ці ІКС не були вразливими до кібернетичних загроз, проте мали низку функціональних і технічних недоліків (низька надійність, відсутність технічного діагностування, низька швидкодія, незручний інтерфейс «людина-машина» тощо). Швидкий розвиток комп'ютерної техніки та інформаційних технологій відкрив можливості вдосконалення ІКС АС та суттєвого покращення їх технічних характеристик. Зважаючи на це за період 2000-2020 років на АС України була проведена широкомасштабна модернізація з впровадження цифрових ІКС, важливих для безпеки. Втілення таких рішень було спрямоване на підвищення ЯРБ АС за допомогою покращених технічних характеристик та функціональних можливостей цифрових ІКС. Проте цифрові ІКС є вразливими для кібернетичних загроз, які стали актуальною проблемою останніх років (у світі було здійснено десятки кібернетичних атак на об'єкти критичної інфраструктури).

Треба зазначити, що станом на 2021 рік лише в Україні щотижня здійснюється понад 40 тисяч кібератак на різні комп'ютерні системи.

Така ситуація у світі зумовила необхідність вдосконалення існуючої законодавчої та нормативно-правової бази та реалізації заходів кіберзахисту для об'єктів критичної інфраструктури (зокрема, АС).

На сьогодні Міжнародна агенція з атомної енергії (далі – МАГАТЕ) та Міжнародна електротехнічна комісія (далі – МЕК) розробили низку документів з кіберзахисту ІКС АС. Вимоги та рекомендації, що містяться у цих документах, спрямовані на реалізацію в ІКС АС засобів захисту від кібернетичних атак, які можуть негативно впливати на забезпечення ЯРБ АС.

Аналогічні роботи зі створення законодавчої та нормативної бази з кіберзахисту реалізуються і в Україні. У 2018 році набрав чинності Закон України «Про основні засади забезпечення кібербезпеки України», дія якого, зокрема, розповсюджується на об'єкти критичної інфраструктури, до яких належать підприємства, установи та організації, які провадять діяльність у галузі енергетики (зокрема, ДП «НАЕК «Енергоатом»). Відповідно до пункту 2 частини третьої статті 8 вказаного закону для функціонування національної системи кібербезпеки необхідне створення нормативно-правової бази у сфері кібербезпеки та гармонізації нормативних документів відповідно до міжнародних стандартів.

У 2018 році набрав чинності документ «Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури», затверджений постановою Кабінету Міністрів України від 19 червня 2019 року № 518 (далі – Загальні вимоги). Зазначений документ має загальний характер та стосується всіх об'єктів критичної інфраструктури. Згідно з пунктом 14 цього документа міністерства та інші центральні органи виконавчої влади можуть розробляти конкретизовані вимоги з кіберзахисту з урахуванням секторальної (галузевої) специфіки функціонування об'єктів критичної інфраструктури, які відносяться до сфери їх управління.

Наразі в Україні відсутні чинні НПА, які містили б вимоги до кіберзахисту ІКС АС, що не дає змоги персоналу АС адекватно та ефективно реагувати на існуючі кібернетичні загрози для забезпечення ядерної та радіаційної безпеки.

Зважаючи на це та з урахуванням положень пункту 14 Загальних вимог було прийнято рішення про розроблення національних вимог до кіберзахисту ІКС АС для забезпечення ЯРБ, які мають враховувати міжнародний досвід із кіберзахисту ІКС АС і рекомендації МАГАТЕ та МЕК. Проєкт НПА враховує норми Закону України «Про основні засади забезпечення кібербезпеки України» та положення Загальних вимог, проте також містить вимоги до кіберзахисту, які враховують специфіку ІКС АС (зокрема, класифікацію ІКС АС за виконуваними функціями та впливом на ЯРБ, значну ізольованість ІКС АС від зовнішніх мереж передачі даних, перевагу забезпечення правильного функціонування над захистом інформації, існування певного регламентованого порядку розроблення, впровадження та експлуатації ІКС АС, необхідність координації між кіберзахистом та ЯРБ тощо). Впровадження проєкту НПА забезпечить можливість захисту існуючих та нових цифрових ІКС АС від кібернетичних загроз, які можуть негативно впливати на ЯРБ.

Кінцевою метою впровадження проєкту НПА є реалізація в ІКС АС заходів попередження, протидії та пом'якшення наслідків потенційних кібератак, які можуть призвести до значних матеріальних збитків внаслідок недовиробітку електроенергії через аварійну зупинку енергоблоків АС або до аварій з викидом радіоактивних речовин, що негативно впливають на навколишнє природне середовище, життя та здоров'я населення.

Основні групи (підгрупи), на які проблема справляє вплив:

Групи (підгрупи)	Так	Ні
Громадяни	-	+
Держава	+	-
Суб'єкти господарювання	+	-
У тому числі суб'єкти малого підприємництва	-	+

Ця проблема не може бути вирішена за допомогою ринкових механізмів, оскільки визначення критеріїв і вимог безпеки, додержання яких обов'язкове під час використання ядерної енергії, зокрема, у сфері кіберзахисту ІКС, важливих для безпеки АС, можливе лише за допомогою державного регулювання.

II. Цілі державного регулювання

Основною ціллю проєкту НПА є захист населення та навколишнього природного середовища через удосконалення системи нормативно-правового регулювання кіберзахисту ІКС АС. Для забезпечення ЯРБ необхідне встановлення єдиних уніфікованих вимог з кіберзахисту ІКС АС з однозначною гармонізацію національного законодавства із європейською практикою, кращим міжнародним досвідом і рекомендаціями МАГАТЕ та МЕК.

III. Визначення та оцінка альтернативних способів досягнення цілей

Під час розроблення проєкту регуляторного акта за результатами міжнародних конференцій МАГАТЕ, консультацій та робочих зустрічей з представниками Комісії ядерного регулювання США визначено два способи досягнення визначеної цілі, а саме:

- залишення існуючої ситуації без змін;
- розроблення нового НПА.

1. Визначення альтернативних способів

Вид альтернативи	Опис альтернативи
Альтернатива 1	Залишення існуючої ситуації без змін. Відсутність регулювання, відсутність дієвого механізму забезпечення кіберзахисту ІКС АС призведе до збільшення ризиків порушення ЯРБ внаслідок кібератак. Невідповідність Закону України «Про основні засади забезпечення кібербезпеки України» вимогам сучасних міжнародних стандартів і рекомендації МАГАТЕ та МЕК.
Альтернатива 2	Розроблення нового НПА. Розроблення «Вимог до кіберзахисту інформаційних та керуючих систем атомних станцій для забезпечення ядерної та радіаційної безпеки», з урахуванням положень сучасних міжнародних стандартів і рекомендацій МАГАТЕ та МЕК до

	кіберзахисту ІКС АС забезпечить ЯРБ за допомогою розроблення та реалізації низки заходів захисту, протидії та пом'якшення наслідків потенційних кібератак, спрямованих проти ІКС АС.

2. Оцінка обраних альтернативних способів досягнення цілей
Оцінка впливу на сферу інтересів держави

Вид альтернативи	Вигоди	Витрати
Альтернатива 1	Відсутні	Відсутність нормативно-правової бази для практичної реалізації заходів кіберзахисту призводить до вразливості ІКС, важливих для безпеки АС, до впливу потенційних кібератак. Збереження існуючої ситуації збільшує ризик значних матеріальних збитків унаслідок недовиробітку електроенергії через аварійну зупинку енергоблоків АС або реалізації заходів ліквідації аварій з викидом радіоактивних речовин, що негативно впливають на навколишнє природне середовище, життя та здоров'я населення.
Альтернатива 2	Розроблення нового НПА, що містить сучасні вимоги до кіберзахисту ІКС АС забезпечить: - приведення у відповідність до Закону України «Про основні засади забезпечення кібербезпеки України» та до вимог сучасних міжнародних стандартів і рекомендацій МАГАТЕ та МЕК; - створення нормативно-правової бази для практичної реалізації заходів кіберзахисту ІКС, важливих для безпеки АС. Це призведе до реалізації у сучасних цифрових ІКС АС	Відсутні

	ефективних заходів захисту від кібератак, підвищить безпеку експлуатації енергоблоків АС, суттєво зменшить імовірність виникнення аварійних ситуацій та аварій (спричинених кібератаками) з вкрай негативними наслідками для держави, населення та навколишнього природного середовища.	

Оцінка впливу на громадян не проводилась, оскільки положення проєкту НПА на них не поширюються.

Оцінка впливу на сферу інтересів суб'єктів господарювання

Показник	Великі	Середні	Малі	Мікро	Разом
Кількість суб'єктів господарювання, що підпадають під дію регулювання (одиниць)	6	-	-	-	6*
Питома вага групи у загальній кількості, відсотків	100	-	-	-	100
* – під дію регулювання підпадає 6 суб'єктів господарювання (4 АС та 2 підприємства-розробники ІКС АС)					

Вид альтернативи	Вигоди	Витрати
Альтернатива 1	Відсутні	Негативний вплив на безпеку АС через ризик виникнення аварійних ситуацій або аварій внаслідок можливих кібернетичних атак, спрямованих на ІКС, важливих для безпеки АС. Виникнення аварійних ситуацій через кібератаки може призвести до зупинки енергоблоків АС, недовиробітку електроенергії та значних матеріальних збитків. Виникнення аварій через

		кібератаки може призвести до забруднення навколишнього природного середовища радіоактивними речовинами, нанесення шкоди здоров'ю персоналу та населення, значних витрат на ліквідацію наслідків аварії та виведення пошкодженого енергоблока з експлуатації.
Альтернатива 2	Підвищення ЯРБ АС завдяки реалізації заходів кіберзахисту ІКС, важливих для безпеки АС. Зменшення імовірності виникнення аварійних ситуацій та аварій внаслідок кібератак. Забезпечення стабільної безпечної та економічно ефективної роботи енергоблоків АС.	Витрати, пов'язані із розробленням та погодженням комплексу заходів, потрібних для приведення діяльності діючих енергоблоків АС у відповідність до нових вимог

Витрати на одного суб'єкта господарювання великого підприємництва (а саме АС), які виникають внаслідок дії регуляторного акта (згідно з додатком 2 до Методики проведення аналізу впливу регуляторного акта).

Порядковий номер	Витрати	За перший рік	За п'ять років
1	Витрати на придбання та впровадження засобів кіберзахисту (обладнання та програмного забезпечення), випробування, технічне обслуговування тощо, гривень*	1 600 000,00	4 000 000,00
2	Витрати, пов'язані з підготовкою (переглядом, внесенням змін) та поданням документів (програма кіберзахисту, плани кіберзахисту, звіт з оцінювання, програми та методики випробувань, план реагування, звіти тощо) державним органам, гривень*	200 000,00	500 000,00
3	Витрати, пов'язані із наймом додаткового персоналу, навчанням/підвищенням кваліфікації	50 000,00	150 000,00

	персоналу, гривень*		
4	Витрати на виявлення вразливостей, оцінювання повноти та достатності заходів кіберзахисту, оцінювання ризиків, моніторинг кіберзахисту, гривень*	100 000,00	500 000,00
5	Разом (сума рядків: 1 + 2 + 3 + 4), гривень:	1 950 000,00	5 150 000,00
6	Кількість суб'єктів господарювання великого та середнього підприємництва, на яких буде поширено регулювання, одиниць	4	4
7	Сумарні витрати об'єктів господарювання великого та середнього підприємництва, на виконання регулювання (вартість регулювання) (рядок 5 х рядок 6), гривень	7 800 000,00	20 600 000,00

* За даними ВП АЕС.

Як видно з цієї таблиці введення в дію проєкту НПА на початковому етапі потребує здійснення певних витрат, пов'язаних із реалізацією на діючих ІКС АС комплексу заходів кіберзахисту, потрібних для приведення діючих енергоблоків АС у відповідність до вимог цього проєкту НПА, але це вимушені витрати, які дозволять підвищити безпеку та в майбутньому уникнути катастрофічних витрат, що пов'язані з ліквідацією наслідків аварій, що можуть виникнути внаслідок кібернетичних атак, спрямованих на ІКС, важливих для безпеки АС.

Сумарні витрати за альтернативами	Сума витрат, гривень
Альтернатива 1	Надвеликі витрати на ліквідацію наслідків аварій на енергоблоках АС
Альтернатива 2	20 600 000,00

Витрати на одного суб'єкта господарювання великого підприємництва (а саме підприємства-розробника ІКС АС), які виникають внаслідок дії регуляторного акта (згідно з додатком 2 до Методики проведення аналізу впливу регуляторного акта).

Порядковий номер	Витрати	За перший рік	За п'ять років
1	Витрати на придбання додаткового обладнання, випробування, гривень*	500 000,00	2 500 000,00
2	Витрати на навчання/підвищення кваліфікації персоналу, гривень*	20 000,00	40 000,00

3	Витрати, пов’язані з підготовкою та поданням документів (плани кіберзахисту, розділи ТЗ/ТУ, програми та методики випробувань, звіти тощо) державним органам, гривень*	100 000,00	400 000,00
4	Разом (сума рядків: 1 + 2 + 3), гривень:	620 000,00	2 940 000,00
5	Кількість суб’єктів господарювання великого та середнього підприємництва, на яких буде поширено регулювання, одиниць	2	2
6	Сумарні витрати об’єктів господарювання великого та середнього підприємництва, на виконання регулювання (вартість регулювання) (рядок 4 х рядок 5), гривень	1 240 000,00	5 880 000,00

* За даними підприємств-розробників ІКС АС.

Як видно з цієї таблиці введення в дію проєкту НПА потребує здійснення певних витрат, пов’язаних із розробленням та впровадженням у ІКС додаткових технічних та програмних засобів кіберзахисту, потрібних для приведення діяльності діючих енергоблоків АС у відповідність до вимог цього проєкту НПА, але це вимушені витрати, які дозволять підвищити безпеку та в майбутньому уникнути катастрофічних витрат, що пов’язані з ліквідацією наслідків аварій, які можуть виникнути внаслідок кібернетичних атак, спрямованих проти ІКС, важливих для безпеки АС.

Сумарні витрати за альтернативами	Сума витрат, гривень
Альтернатива 1.	Надвеликі витрати на ліквідацію наслідків аварій на енергоблоках АС
Альтернатива 2.	5 880 000,00

IV. Вибір найбільш оптимального альтернативного способу досягнення цілей

Рейтинг результативності (досягнення цілей під час вирішення проблеми)	Бал результативності (за чотирибальною системою оцінки)	Коментарі щодо присвоєння відповідного бала
Альтернатива 1	1	Цілі регулювання не можуть бути досягнуті (проблема продовжить існувати).
Альтернатива 2	4	Прийняття НПА забезпечить повною мірою досягнення поставлених цілей

Рейтинг результативності	Вигоди (підсумок)	Витрати (підсумок)	Обґрунтування відповідного місця альтернативи у рейтингу
Альтернатива 1	Відсутні	Відсутність нормативно-правової бази для практичної реалізації заходів кіберзахисту призводить до вразливості ІКС, важливих для безпеки АС, до впливу потенційних кібератак. Збереження існуючої ситуації збільшує ризик значних матеріальних збитків внаслідок недовиробітку електроенергії через аварійну зупинку енергоблоків АС або реалізації заходів ліквідації аварій з викидом радіоактивних речовин, що негативно впливають на навколишнє природне середовище, життя та здоров'я населення. Негативний вплив на безпеку АС через ризик виникнення аварійних ситуацій або аварій внаслідок можливих кібернетичних атак, спрямованих на ІКС, важливих для безпеки АС.	Альтернатива не забезпечує досягнення цілей регулювання. За відсутності вигод, кількість неврегульованих витрат залишається значною.
Альтернатива 2	Розроблення нового НПА, що містить сучасні вимоги до кіберзахисту ІКС АС забезпечить: - приведення у відповідність до Закону	Відсутні	Альтернатива забезпечує досягнення цілей регулювання. За відсутності неврегульованих витрат, дозволяє

	України «Про основні засади забезпечення кібербезпеки України» та до вимог сучасних міжнародних стандартів і рекомендацій МАГАТЕ та МЕК; - створення нормативно-правової бази для практичної реалізації заходів кіберзахисту ІКС, важливих для безпеки АС. Це призведе до реалізації в сучасних цифрових ІКС АС ефективних заходів захисту від кібератак, підвищить безпеку експлуатації енергоблоків АС, суттєво зменшить імовірність виникнення аварійних ситуацій та аварій (спричинених кібератаками) з вкрай негативними наслідками для держави, населення та навколишнього природного середовища.		досягнути максимальної кількості вигод

V. Механізми та заходи, які забезпечать розв’язання визначеної проблеми

Механізмами, що забезпечать розв’язання визначеної проблеми, є розроблення нового НПА «Вимоги до кіберзахисту інформаційних та керуючих систем атомних станцій для забезпечення ядерної та радіаційної безпеки», в якому будуть враховані сучасні міжнародні норми безпеки, зокрема положення документів МАГАТЕ та стандартів МЕК.

Новий НПА врегульовує механізми класифікації ІКС за рівнями кіберзахисту, загальних принципів забезпечення кіберзахисту, оцінювання кіберзахисту ІКС, забезпечення кіберзахисту на різних етапах життєвого циклу ІКС, розроблення та погодження документів, що обґрунтовують кіберзахист ІКС.

Впровадження нового НПА надасть можливість підприємствам-розробникам ІКС та ВП АЕС виробити системний підхід та практично реалізувати заходи

кіберзахисту для запобігання негативному впливу кіберзагроз на ЯРБ.

Організаційні заходи, які необхідно здійснити Держатомрегулюванню для впровадження регуляторного акта:

- направлення ліцензіатам інформаційних листів щодо набрання чинності регуляторним актом;
- розміщення на сайті Держатомрегулювання НПА «Вимоги до кіберзахисту інформаційних та керуючих систем атомних станцій для забезпечення ядерної та радіаційної безпеки».

VI. Оцінка виконання вимог регуляторного акта залежно від ресурсів, якими розпоряджаються органи виконавчої влади чи органи місцевого самоврядування, фізичні та юридичні особи, які повинні проваджувати або виконувати ці вимоги

Реалізація регуляторного акта не потребуватиме додаткових бюджетних витрат і ресурсів на адміністрування регулювання органами виконавчої влади чи органами місцевого самоврядування.

Державне регулювання не передбачає утворення нового державного органу (або нового структурного підрозділу діючого органу).

Відповідно, розрахунок витрат на виконання вимог регуляторного акта для органів виконавчої влади чи органів місцевого самоврядування згідно з додатком 3 до Методики проведення аналізу впливу регуляторного акта не проводився.

Процедура регулювання суб'єктів великого і середнього підприємництва (розрахунок на одного типового суб'єкта господарювання)	Планові витрати часу на процедуру, днів	Вартість часу співробітника органу державної влади відповідної категорії (заробітна плата), грн./день*.	Оцінка кількості процедур за рік, що припадають на одного суб'єкта	Оцінка кількості суб'єктів, що підпадають під дію процедури регулювання	Витрати на адміні-стрування регулювання (за рік), гривень
1. Погодження документів АС з кіберзахисту нових/модернізованих ІКС АС в Держатомрегулюванні	42	404	5	4	339 360,00

2. Погодження з Держатомрегулюванням комплексу заходів, потрібних для приведення діяльності діючих ІКС АС у відповідність до вимог регуляторного акта	42	404	1	4	67 872,00
3. Погодження з Держатомрегулюванням документів з кіберзахисту підприємства розробника ІКС	42	404	3	2	101 808,00
Разом за рік					509 040,00
Сумарно за п’ять років					2 545 200,00

*Вартість часу посадового окладу головного спеціаліста державних органів, юрисдикція яких поширюється на всю територію України, відповідно до постанови Кабінету Міністрів України від 13 січня 2021 року № 15 «Про внесення змін до постанови Кабінету Міністрів України від 18 січня 2017 р. № 15», складає 8500,00 грн./21 робочий день= 404 грн./день.

Для впровадження та виконання вимог регуляторного акта державний орган, для якого здійснюється розрахунок адміністрування регулювання, не буде нести додаткові бюджетні витрати.

VII. Обґрунтування запропонованого строку дії регуляторного акта

Строк дії регуляторного акта пропонується встановити – постійний.

Перегляд акта можливий в разі суттєвих змін міжнародних документів МАГАТЕ та МЕК, на вимогах яких базується проєкт НПА.

VIII. Визначення показників результативності дії регуляторного акта

Прогнозними значеннями показників результативності регуляторного акта є:

- розмір надходжень до державного та місцевих бюджетів і державних цільових фондів, пов’язаних з дією акта – не передбачається;
- кількість суб’єктів господарювання, на яких поширюється дія акта;
- розмір коштів і час, що витрачатимуться суб’єктами господарювання, пов’язаними з виконанням вимог акта – збільшиться, але це збільшення спрямоване на підвищення безпеки та на недопущення в майбутньому величезних витрат, пов’язаних із ліквідацією аварій;

- рівень поінформованості суб’єктів господарювання з основних положень акта – середній. Проєкт акта розміщено на веб-сайті Держатомрегулювання, а після прийняття акта він буде розміщений на сайті www.zakon.rada.gov.ua;

- кількість поданих на погодження документів;

- кількість погоджених документів;

- кількість порушень положень регуляторного акта.

IX. Визначення заходів, за допомогою яких здійснюватиметься відстеження результативності дії регуляторного акта

Базове відстеження результативності регуляторного акта здійснюється після набрання чинності цим регуляторним актом, але не пізніше дня, з якого починається проведення повторного відстеження результативності цього акта.

Повторне відстеження результативності регуляторного акта здійснюється через 1 рік з дня набрання ним чинності.

Періодичні відстеження результативності регуляторного акта здійснюються раз на кожні три роки починаючи з дня закінчення заходів з повторного відстеження результативності цього акта.

Метод проведення відстеження результативності – статистичний, вид даних – статистичні показники.

Виконавець заходів із відстеження – Державна інспекція ядерного регулювання України.

Виконуючий обов’язки Голови –
Головного державного інспектора
з ядерної та радіаційної безпеки України **Олег КОРІКОВ**

«____»_____2022 року

ПОЯСНЮВАЛЬНА ЗАПИСКА

до проєкту наказу Державної інспекції ядерного регулювання України «Про затвердження Вимог до кіберзахисту інформаційних та керуючих систем атомних станцій для забезпечення ядерної та радіаційної безпеки»

1. Мета

Метою розроблення проєкту наказу Державної інспекції ядерного регулювання України «Про затвердження Вимог до кіберзахисту інформаційних та керуючих систем атомних станцій для забезпечення ядерної та радіаційної безпеки» (далі – проєкт наказу) є визначення та врегулювання вимог до кіберзахисту інформаційних та керуючих систем атомних станцій (далі – ІКС АС).

2. Обґрунтування необхідності прийняття акта

Проєкт наказу розроблено Держатомрегулюванням за власною ініціативою відповідно до статті 24 Закону України «Про використання ядерної енергії та радіаційну безпеку» та Положення про Державну інспекцію ядерного регулювання України, затвердженого постановою Кабінету Міністрів України від 20 серпня 2014 року № 363.

Розроблення проєкту наказу зумовлено необхідністю визначення вимог до кіберзахисту ІКС АС за допомогою:

– деталізації та конкретизації регулюючих вимог до кіберзахисту ІКС АС, наведених у законодавстві України;

– установлення вимог до класифікації, оцінювання та забезпечення кіберзахисту ІКС АС і до документів, що обґрунтовують кіберзахист;

– гармонізації з міжнародними стандартами: Міжнародного агентства з атомної енергії, Міжнародної електротехнічної комісії та Комісії ядерного регулювання США.

3. Основні положення проєкту акта

Проєкт наказу встановлює загальні вимоги до:

– класифікації з кіберзахисту ІКС АС, їх компонентів та програмного забезпечення;

– загальних принципів забезпечення кіберзахисту;

– оцінювання кіберзахисту;

– забезпечення кіберзахисту на етапі розроблення;

– забезпечення кіберзахисту на етапі впровадження;

– забезпечення кіберзахисту в процесі експлуатації;

– документів, що обґрунтовують кіберзахист.

4. Правові аспекти

Правовою підставою розроблення проєкту наказу є Положення про Державну інспекцію ядерного регулювання України, затверджене постановою Кабінету Міністрів України від 20 серпня 2014 року № 363 (підпункт 7 пункту 4), згідно з яким Держатомрегулювання визначає критерії та вимоги безпеки, додержання яких обов’язкове під час використання ядерної енергії, відповідно до яких затверджує, зокрема, норми, правила з ядерної та радіаційної безпеки.

У цій сфері регулювання суспільних відносин здійснюється відповідно до таких нормативно-правових актів:

– Закон України «Про використання ядерної енергії та радіаційну безпеку»;

– Закон України «Про основні засади забезпечення кібербезпеки України»;

– Загальні положення безпеки атомних станцій, затверджені наказом Державного комітету ядерного регулювання України від 19 листопада 2007 року № 162, зареєстровані в Міністерстві юстиції України 25 січня 2008 року за № 56/14747;

– Вимоги до проведення модифікацій ядерних установок та порядку оцінки їх безпеки, затверджені наказом Державного комітету ядерного регулювання України від 10 січня 2005 року № 4, зареєстровані в Міністерстві юстиції України 24 січня 2005 року за № 78/10358;

– Вимоги з ядерної та радіаційної безпеки до інформаційних та керуючих систем, важливих для безпеки атомних станцій, затверджених наказом Державної інспекції ядерного регулювання України від 22 липня 2015 року № 140, зареєстровані в Міністерстві юстиції України від 06 серпня 2015 року за № 954/27399.

5. Фінансово-економічне обґрунтування

Реалізація проєкту наказу не потребує додаткових фінансових витрат з державного чи місцевого бюджетів України.

6. Позиція заінтересованих сторін

Проєкт наказу не стосується питань функціонування місцевого самоврядування, прав та інтересів територіальних громад, місцевого та регіонального розвитку, соціально-трудової сфери, прав осіб з інвалідністю, функціонування і застосування української мови як державної.

Проєкт наказу не стосується сфери наукової та науково-технічної діяльності та не потребує розгляду Науковим комітетом Національної ради України з питань розвитку науки і технологій.

Проєкт наказу потребує проведення цифрової експертизи та отримання висновку Міністерства цифрової трансформації України про проведення цифрової експертизи.

7. Оцінка відповідності

У проєкті наказу відсутні положення, що стосуються зобов’язань України у сфері європейської інтеграції.

У проєкті наказу відсутні положення, що стосуються прав та свобод, гарантованих Конвенцією про захист прав людини і основоположних свобод.

У проєкті наказу відсутні положення, які містять ознаки дискримінації.

У проєкті наказу відсутні положення, які впливають на забезпечення рівних прав та можливостей жінок і чоловіків.

У проєкті наказу відсутні положення, які містять ризики вчинення корупційних правопорушень та правопорушень, пов'язаних з корупцією.

Громадська антикорупційна, громадська антидискримінаційна та громадська гендерно-правова експертизи проєкту наказу не проводились.

8. Прогноз результатів

Реалізація положень проєкту наказу дозволить визначити та врегулювати вимоги до кіберзахисту ІКС АС, а також дозволить гармонізувати національне законодавство з міжнародними нормами.

Виконуючий обов'язки Голови
Державної інспекції ядерного
регулювання України –
Головного державного інспектора
з ядерної та радіаційної безпеки України **Олег КОРІКОВ**

«____»_____2022 року

ПОВІДОМЛЕННЯ

про оприлюднення проєкту наказу Державної інспекції ядерного регулювання України «Про затвердження Вимог до кіберзахисту інформаційних та керуючих систем атомних станцій для забезпечення ядерної та радіаційної безпеки»

Держатомрегулюванням відповідно до статті 24 Закону України «Про використання ядерної енергії та радіаційну безпеку» та Положення про Державну інспекцію ядерного регулювання України, затвердженого постановою Кабінету Міністрів України від 20 серпня 2014 року № 363, розроблено проєкт наказу «Про затвердження Вимог до кіберзахисту інформаційних та керуючих систем атомних станцій для забезпечення ядерної та радіаційної безпеки» (далі – проєкт наказу).

Метою розроблення проєкту наказу є визначення та врегулювання вимог до кіберзахисту інформаційних та керуючих систем атомних станцій.

Наразі в Україні відсутні нормативно-правові акти, які містили б вимоги до кіберзахисту інформаційних та керуючих систем атомних станцій, що не дає змоги персоналу атомних станцій адекватно та ефективно реагувати на існуючі кібернетичні загрози для забезпечення ядерної та радіаційної безпеки.

Зважаючи на це, та з урахуванням положень Закону України «Про основні засади забезпечення кібербезпеки України», постанови Кабінету Міністрів України від 19 червня 2019 року № 518 «Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури» було прийнято рішення про розроблення національних вимог до кіберзахисту інформаційних та керуючих систем атомних станцій для забезпечення ядерної та радіаційної безпеки, які мають враховувати міжнародний досвід із кіберзахисту інформаційних та керуючих систем атомних станцій і рекомендації Міжнародного агентства з атомної енергії та Міжнародної електротехнічної комісії.

Зауваження та пропозиції до проєкту наказу приймаються до 29 грудня 2021 року за адресою: 01011, м. Київ, вул. Арсенальна, 9/11; тел. 277-12-21 або на електронну пошту: *as.goroshanskyi@snriu.gov.ua.*