ДЕРЖАВНЕ АГЕНТСТВО УКРАЇНИ З УПРАВЛІННЯ ЗОНОЮ ВІДЧУЖЕННЯ

ДЕРЖАВНЕ СПЕЦІАЛІЗОВАНЕ ПІДПРИЄМСТВО
«ЦЕНТРАЛЬНЕ ПІДПРИЄМСТВО З ПОВОДЖЕННЯ
З РАДІОАКТИВНИМИ ВІДХОДАМИ»

ЗАТВЕРДЖЕНО

В.о. генерального директора

ДСП «ЦППРВ»

_____ Наталія КУРАКОВА

«____» _____2024 року

ПОЛІТИКА

ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Державного спеціалізованого Підприємства

"Центральне підприємство з поводження з радіоактивними відходами"

ПК-І.1.17.0.001 - 2024

Введено в дію
наказом № 236
від «15» квітня 2024р.

м. Чорнобиль

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Політика інформаційної безпеки (далі – Політика ІБ) Державного Спеціалізованого Підприємства "Центральне підприємство з поводження з радіоактивними відходами" (далі – Підприємство), визначає підхід та дотримання щодо забезпечення інформаційної безпеки, а також вимоги, правила, обмеження, рекомендації для об'єктів критичної інфраструктури (далі - ОКІ) та об'єктів критичної інформаційної інфраструктури (далі - ОКІІ), оператором яких визначено Підприємство.

1.2. Керівництво Підприємства усвідомлює важливість та необхідність вдосконалення заходів і засобів забезпечення інформаційної безпеки в контексті розвитку законодавства та норм регулювання діяльності.

1.3. Політика ІБ встановлює цілі, принципи та відповідальність щодо інформаційної безпеки, кібербезпеки в інформаційно-комунікаційних системах та ресурсах Підприємства.

1.4. Дієвість та ефективність Політики ІБ забезпечується впровадженням організаційно-технічних заходів та організаційно-розпорядчих та нормативних документів в сфері інформаційної безпеки.

1.5. Політика ІБ розроблена відповідно до:

1.5.1. Закону України «Про захист інформації в інформаційно-комунікаційних системах».

1.5.2. Закону України «Про основні засади забезпечення кібербезпеки України».

1.5.3. Указу Президента України від 28 грудня 2021 року № 685/2021 «Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки».

1.5.4. Загальних вимог до кіберзахисту об'єктів критичної інфраструктури, затверджених постановою Кабінету Міністрів України від 19.06.2019 № 518

1.5.5. Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, затверджених постановою Кабінету Міністрів України від 29.03.2006 № 373.

1.5.6. Постанови Кабінету Міністрів України від 09 жовтня 2020 р. № 943 «Деякі питання об'єктів критичної інформаційної інфраструктури».

1.5.7. Положення про організаційно-технічну модель кіберзахисту, затвердженого постановою Кабінету Міністрів України від 29 грудня 2021р. № 1426.

1.5.8. Національного стандарту ДСТУ ISO/IEC 27001:2023 «Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою». Вимоги (ISO/IEC 27001:2022, IDT).

1.5.9. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу, наказ ДСТСЗІ СБУ (Державної служби спеціального зв'язку та захисту інформації Служби безпеки України) від 28.04.99 № 22.

1.5.10. НД ТЗІ 2.6-004-21 «Порядок авторизації безпеки інформаційних систем».

1.5.11. НД ТЗІ 3.6-006-21 «Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем».

1.5.12. НД ТЗІ 3.6-007-21 «Порядок впровадження заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем».

1.5.13. НД ТЗІ 3.6-008-21 «Порядок моніторингу безпеки інформаційних систем».

1.5.14. Міжнародних стандартів з питань інформаційної безпеки та загальноприйнятих у міжнародній практиці принципів забезпечення інформаційної безпеки і кіберзахисту (ISO/IEC 27001, NIST Cybersecurity Framework).

2. СФЕРА ЗАСТОСУВАННЯ

2.1. Політика ІБ розроблена для усіх інформаційно-комунікаційних систем та ресурсів Підприємства.

2.2. Дія Політики ІБ поширюється на всі підрозділи Підприємства, ОКІ, оператором для яких визначено підприємство та ОКІІ Підприємства.

2.3. Всі працівники Підприємства, які використовують/користуються ІКС, мають дотримуватись вимог, правил, інструкцій, обмежень, рекомендацій для досягнення мети та цілей з інформаційної безпеки.

3. ВИЗНАЧЕННЯ ТЕРМІНІВ

3.1. **Об'єкт критичної інфраструктури** - об'єкти інфраструктури, системи, їх частини та їх сукупність, які є важливими для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам.

3.2. **Об'єкт критичної інформаційної інфраструктури** - комунікаційна або технологічна система ОКІ, кібератака на яку безпосередньо вплине на стале функціонування такого ОКІІ.

3.3. **Інформаційна безпека** – комплекс організаційних заходів, програмних і технічних засобів, що забезпечують захист інформації від випадкових і навмисних загроз, у результаті реалізації яких можливе порушення доступності, цілісності, конфіденційності інформації.

3.4. **Кіберзахист** – сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем.

3.5. **Інцидент кібербезпеки** (далі - **кіберінцидент**) - подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів.

3.6. **Локальна обчислювальна мережа** (далі - **ЛОМ**) Підприємства – мережа, що представляє собою розподілену систему взаємозв'язаного обладнання (сукупність робочих станцій, комп'ютерів, ноутбуків та ін.) мережі, серверів, комутаційного обладнання, структурованої кабельної мережі, спеціалізованого обчислювального обладнання, офісної та периферійної техніки), які забезпечують виконання статутних функцій Підприємства.

3.7. **Інформаційно-комунікаційна система** (далі - **ІКС**) – сукупність інформаційних та електронних комунікаційних систем, які у процесі обробки інформації діють як єдине ціле.

3.8. **Інформаційний ресурс** – сукупність людських, апаратних та програмних ресурсів в інформаційних системах та процесах Підприємства.

3.9. **Захист інформації** – діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в ІКС та ЛОМ.

3.10. **Цілісність** – властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем та/або процесом.

3.11. **Конфіденційність** – властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем та/або процесом.

3.12. **Доступність** – властивість досяжності й можливості використання інформації на вимогу авторизованого об'єкта.

3.13. **Спостережність** – властивість ІКС, що дозволяє фіксувати діяльність користувачів і процесів, використання пасивних об'єктів, а також однозначно установлювати ідентифікатори причетних до певних подій користувачів і процесів з метою запобігання порушення інформаційної безпеки і/або забезпечення відповідальності за певні дії.

4. МЕТА, ЦІЛІ ТА ПРИНЦИПИ

4.1. **Мета**

4.1.1. Встановлення загальних стандартів та вимог для забезпечення інформаційної безпеки, а також виконання вимог стандарту ISO/IEC 27001:2023.

4.1.2. Захист інформаційних активів від зовнішніх та внутрішніх навмисних та ненавмисних загроз у сфері інформаційно-комунікаційних систем та ресурсів Підприємства.

4.2. **Цілі**

4.2.1 Організація захисту та забезпечення безпеки Підприємства у тому числі ОКІІ для запобігання проявам несанкціонованого втручання в їх функціонування із забезпечення конфіденційності, цілісності, доступності інформації, яка обробляється та зберігається в процесі діяльності Підприємства.

4.2.2 Прогнозування та запобігання кризовим ситуаціям, ризиків операційної діяльності Підприємства та виникнення кіберінцидентів на ОКІІ, ІКС та ЛОМ.

4.2.3 Забезпечення безперервної роботи ОКІІ, ІКС, ЛОМ та сервісів.

4.2.4 Захист інформаційно-комунікаційних ресурсів ОКІІ на ОКІ

4.2.5 Підтримка позитивної репутації Підприємства.

4.3. **Основні принципи**

4.3.1 Підтримка належного стану кібербезпеки із забезпеченням цілісності, конфіденційності, доступності та спостережності інформації.

4.3.2 Ризик-орієнтований підхід з адаптуванням під нові реалії інформаційної безпеки, який забезпечує розуміння, моніторинг та зменшення ризиків критичних бізнес процесів Підприємства.

4.3.3 Стратегія розвитку новітніх технологій на Підприємстві, які пов’язані з інформаційною безпекою.

5. УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

5.1. Підприємство забезпечує інформаційну безпеку фізичними, апаратними, програмними засобами, організаційно-розпорядчими, нормативними документами та цивільно-правовими методами.

5.2. Підтримка високого рівня кібербезпеки забезпечується шляхом:

5.2.1. Встановлення правил доступу до інформаційних ресурсів та програмно-технічних комплексів.

5.2.2. Установки парольного захисту для програмних та сервісних ресурсів.

5.2.3. Забезпечення антивірусним захистом та захистом від зловмисного коду.

5.2.4. Забезпечення захисту ОКІІ, ІКС та ЛОМ.

5.2.5. Використання ідентифікації та автентифікації користувачів.

5.2.6. Використання криптографічного захисту інформації.

5.2.7. Забезпечення резервного копіювання інформації та утворення резерву апаратних комплексів.

5.2.8. Моніторингу кіберзагроз.

5.2.9. Інші заходи, регламентовані нормативно-правовими актами.

5.3. Під час розроблення, впровадження та функціонування програмно-технічних комплексів Підприємства враховуються вимоги до інформаційної безпеки:

5.3.1. ІКС у тому числі ОКІ мають відповідати законодавчим актам та вимогам державних стандартів з кібербезпеки.

5.3.2. Працівники Підприємства зобов'язані дотримуватися вимог кібербезпеки під час обміну інформацією з використанням засобів комунікацій.

5.3.3. Затверджені вимоги, правила, інструкції, обмеження, рекомендації з інформаційної безпеки доводяться до всіх працівників Підприємства під підпис.

5.4. На підприємстві застосовуються процедури кіберзахисту:

5.4.1. Розмежування та контроль доступу, ієрархія санкціонування доступу та періодичний перегляд доступу до ІКС та ЛОМ, у тому числі на ОКІІ.

5.4.2. Використання апаратних, програмних засобів, в тому числі засобів сканування ІКС та ЛОМ.

5.4.3. Виконання резервного копіювання згідно затверджених регламентів.

5.4.4. Інші заходи, регламентовані нормативно-правовими актами.

6. ДОКУМЕНТИ ДО ПОЛІТИКИ ІБ

6.1. Документи до Політики ІБ – це нормативно-розпорядчі документи Підприємства, які регламентують заходи кібербезпеки під час функціонування ОКІІ, ЛОМ та окремих інформаційних систем і сервісів Підприємства. Документи до Політики ІБ можуть мати постійний та тимчасовій характер.

6.2. Документи Політики ІБ визначають вимоги кібербезпеки, необхідні для функціонування ОКИ, ІКС та ЛОМ. До них відносяться наступні вимоги.

6.2.1. Політика безпечного використання електронної пошти.
6.2.2. Політика забезпечення антивірусного захисту.
6.2.3. Політика автентифікації користувачів.
6.2.4. Політика керування паролями облікових записів користувачів.
6.2.5. Політика контролю доступу до інформаційних систем.
6.2.6. Політика віддаленого доступу.

6.2.7. Політика мережевої безпеки.
6.2.8. Політика фізичної безпеки серверних та телекомунікаційних кімнат.
6.2.9. Політика управління, зберігання та знищення електронних носіїв інформації.
6.2.10. Політика управління інцидентами ІБ.
6.2.11. Політика забезпечення безперервності інформаційної безпеки.
6.2.12. Політика управління ризиками інформаційної безпеки.
6.2.13. Плани реагування на інциденти ІБ.
6.2.14. План відновлення ІТ-інфраструктури після надзвичайних ситуацій.
6.2.15. Інші заходи, регламентовані нормативно-правовими актами.

7. РОЛІ ТА ВІДПОВІДАЛЬНІСТЬ

7.1. Керівництво Підприємства здійснює загальне управління інформаційною безпекою, сприяє створенню, впровадженню, контролю та підтримки Політики ІБ. На підприємстві створена та постійно діє комісія з питань технічного захисту інформації, яку очолює генеральний директор Підприємства. Рішення комісії з питань технічного захисту інформації є обов'язковими для виконання всім працівникам Підприємства.

7.2. Постійний контроль впровадження, виконання, вдосконалення та підтримки Політики ІБ в актуальному стані, а також розробки нормативно-розпорядчих документів до Політики ІБ покладається сектор кібербезпеки та захисту інформації (далі - СКБтаЗІ). Нормативно-розпорядчі документи, відповідно до Політики ІБ доступні співробітникам Підприємства у межах їх повноважень і призначені надавати допомогу у виконанні вимог з інформаційної безпеки.

7.3. Кожен працівник Підприємства бере участь у підтримці відповідного рівня з інформаційної безпеки Підприємства в межах своїх обов'язків та повноважень. В своїй роботі всі підрозділи та працівники дотримуються вимог Політики ІБ та несуть відповідальність за їх порушення згідно з чинним законодавством України. Порушення встановлених вимог інформаційної безпеки розцінюється як невиконання розпоряджень керівництва та є основою для накладення дисциплінарного стягнення.

7.4. Для зменшення ризиків виникнення інцидентів кібербезпеки керівництво Підприємства створює працівникам умови для систематичного навчання нормам та заходам інформаційної безпеки.

8. ПЕРЕГЛЯД ПОЛІТИКИ ІБ

8.1. Політика ІБ переглядається не рідше одного разу на рік або при інших підстав.

8.2. Підставами для внесення змін до Політики ІБ Державного спеціалізованого Підприємства "Центральне підприємство з поводження з радіоактивними відходами" є:

8.2.1. Зміни в підходах, принципах чи завданнях щодо забезпечення кібербезпеки внаслідок виникнення нових типів загроз або ризиків.

8.2.2. Удосконалення підходу до забезпечення кібербезпеки на основі вдосконалення та розвитку світової практики в цій сфері.

8.2.3. Зміни в законодавчих, регуляторних та інших актах у сфері кібербезпеки.