DKI

неофіційний переклад

CNPIC
CENTRO NACIONAL DE PROTECCION DE INFRAESTRUCTURAS CRÍTICAS

Посібник з належної практики

План безпеки

НАЦІОНАЛЬНИЙ ЦЕНТР
ЗАХИСТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

ЗАГАЛЬНА БЕЗПЕКА,
ЗОБОВ'ЯЗАННЯ КОЖНОГО

GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR
SECRETARÍA DE ESTADO DE SEGURIDAD
DIRECCIÓN GENERAL DE COORDINACIÓN Y ESTUDIOS


CNPIC
CENTRO NACIONAL DE PROTECCION
DE INFRAESTRUCTURAS CRÍTICAS

ЩОБ ВИ МОГЛИ

7 ДОДАТОК 1: ПРИКЛАДИ

8 ДОДАТОК 2: ПЕРЕЛІК СТАНДАРТІВ ТА НАЙКРАЩИХ ПРАКТИК

1

Вступ

1.1 ПРАВОВА ОСНОВА

Нормальне функціонування основних послуг, що надаються населенню, залежить від низки інфраструктур, як державних, так і приватних, функціонування яких є необхідним і не допускає альтернативних рішень: так звані критичні інфраструктури. З цієї причини необхідно розробити однорідну та цілісну політику безпеки в організаціях, спеціально спрямовану на критичні інфраструктури, в якій визначаються підсистеми безпеки, що мають бути впроваджені для їх захисту з метою запобігання руйнуванню, перерванню або збоям, які можуть зашкодити наданню основних послуг населенню та забезпечити безперервність надання цих послуг.

У цьому сенсі Закон 8/2011 від 28 квітня, який встановлює заходи щодо захисту критичної інфраструктури, спрямований на розробку відповідних стратегій та організаційних структур для спрямування та координації дій різних органів державного управління у сфері захисту критичної інфраструктури після її ідентифікації та визначення, а також на сприяння співпраці та залученню органів і компаній, які керують цими об'єктами та володіють ними (критичних операторів), з метою оптимізації ступеня їх захисту від навмисних фізичних та логічних атак, які можуть вплинути на надання основних послуг.

Цей закон імплементується Королівським декретом 704/2011 від 20 травня, який затверджує Регламент заходів щодо захисту критичної інфраструктури.

Стаття 13 цього Закону встановлює низку зобов'язань для державних та приватних операторів, включаючи підготовку Плану безпеки оператора (далі - ПБО) та Спеціальних планів захисту (далі - СПЗ).

Що стосується змісту ПБО, як зазначено в статті 22.4 Королівського Указу 704/2011, Державний секретар з питань безпеки встановив через CNPIC Резолюцією від 8 вересня 2015 року мінімальний зміст, який повинні мати всі ПБО, а також модель, на якій має ґрунтуватися їхня підготовка.

1.2 МЕТА ЦЬОГО ДОКУМЕНТА

Метою цього документу є надання операторам, визначеним як критичні, рекомендацій щодо підготовки їхніх СПЗ, а також доповнення до Резолюції Державного секретаря з питань безпеки щодо мінімального змісту СПЗ. Таким чином, це добровільний документ, який не містить додаткових вимог до тих, що встановлені чинним законодавством або вищезгаданою Постановою.

Цей посібник містить низку додатків (приклади, перелік стандартів і передових практик тощо), які можуть бути корисними для критично важливих операторів при підготовці деяких пунктів мінімального змісту Плану безпеки оператора.

1.3 ЗАХИСТ ІНФОРМАЦІЇ

Після затвердження ОПЗ його рівень секретності має бути "Обмежене поширення", а критичний оператор (далі - КО) повинен визначити свої процедури управління та обробки інформації відповідно до стандартів безпеки, які гарантують адекватний та ефективний захист такої інформації.

З цією метою СО повинна посилатися на керівні принципи, видані Національним органом безпеки щодо захисту секретної інформації з обмеженим доступом, включаючи наступне[1]:

БЕЗПЕКА ДОКУМЕНТІВ

OR-ASIP-04-01.04 - Настанови щодо поводження з секретною інформацією з обмеженим доступом.

БЕЗПЕКА ПЕРСОНАЛУ

OR-ASIP-04-02.02 - Інструкція з безпеки персоналу при доступі до секретної інформації.

ФІЗИЧНА БЕЗПЕКА

OR-ASIP-01-01.03 - Керівництво з розробки плану захисту зони обмеженого доступу.

OR-ASIP-01-02.03 - Настанова щодо встановлення зон обмеженого доступу.

БЕЗПЕКА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ

OR-ASIP-03-01.04 - Настанови з акредитації інформаційно-комунікаційних систем для обробки інформації з обмеженим доступом.

[1] Вищезгадані документи доступні за посиланням: http://www.cni.es/es/ons/documentacion/normativa/.

CNPIC

CENTRO NACIONAL DE PROTECCION
DE INFRAESTRUCTURAS CRÍTICAS

ЗАГАЛЬНА ПОЛІТИКА БЕЗПЕКИ ОПЕРАТОРА ТА СТРУКТУРУ УПРАВЛІННЯ

2.1 ЗАГАЛЬНА ПОЛІТИКА БЕЗПЕКИ КРИТИЧНО ВАЖЛИВОГО ОПЕРАТОРА

Нормативна база будь-якої організації, як правило, складається з набору політик високого рівня, норм або стандартів розвитку, а також операційних процедур або робочих інструкцій. Політика безпеки №2, про яку йдеться в ПБО, є документом найвищого рівня в цьому наборі і повинна відповідати низці вимог, які детально описані нижче.

Ця Політика безпеки може мати різні форми, всі вони однаково дійсні: паперовий документ, заява в Інтранеті організації та, загалом, будь-який носій, що дозволяє перевірити аспекти, викладені в наступних розділах.

2.1.1 Об'єкт

Об'єкт Політики фундаментально визначає подальший розвиток правил, організацію функції та діяльність, пов'язану з безпекою, а також, дуже чітко, які індикатори будуть використовуватися для вимірювання ефективності та результативності вжитих заходів. Цей об'єкт є стратегією функції безпеки, а тому повинен відображати її місію та бачення в контексті загальної стратегії організації, хоча він може мати й інші форми (заява про місію тощо).

Зазвичай стратегія безпеки відображає намір організації досягти своїх довгострокових цілей шляхом мінімізації ризиків, дотримання чинних стандартів безпеки, а також запобігання та прогнозування інцидентів, які можуть вплинути на ці цілі організації. Оскільки абсолютна безпека неможлива, логічно припустити, що інциденти траплятимуться, і що ними будуть керувати, щоб мінімізувати їхній вплив на досягнення цілей організації.

У фокусі політики має бути захист критичної інфраструктури (КІ), особливо від навмисних атак. Оскільки ці загрози мають низьку ймовірність і високий профіль впливу, їх захист не відповідає звичайним параметрам ефективності та результативності. Тому така політика захисту ОКІ повинна включати критерії, які слід застосовувати для адекватного реагування на реалізацію цих загроз з високим ступенем впливу таким чином, щоб мінімізувати шкоду для людей, навколишнього середовища або життєво важливих послуг, що надаються.

2.1.2 Сфера застосування

Політика безпеки може мати обмежену сферу застосування в різних сферах: географічній (країни, регіони тощо), сферах застосування (фізична, логічна тощо), організаційній (підрозділи, дочірні компанії тощо) тощо.

Логічно, що кожен оператор може вирішити, як найкраще організувати свою роботу, і не існує апріорі кращих чи гірших моделей. У будь-якому випадку, для того, щоб політика безпеки була релевантною для ОПЗ, вона повинна включати в себе основні послуги та критичні активи, якими оперує організація.

Вимоги тут полягають у тому, що політика(и) безпеки повинна(ні) всебічно охоплювати всі активи, якими оперує організація, включаючи захист людей, процесів і технологій (цілісний підхід до безпеки).

[2] Додаток 1, розділ 7.1

Що стосується сфери застосування політики, то особливу увагу слід звернути на такі аспекти, як:

- ✓ Комплексний розгляд безпеки, включаючи логічні та фізичні аспекти.
- ✓ Включення як інформаційних систем управління ІКТ, так і інформаційних систем для управління промисловими процесами.
- ✓ Застосування до основних послуг, а також до місць і об'єктів, які вважаються критично важливими.
- ✓ Включення залежних відносин, таких як дочірні компанії, що надають основні послуги, та IICC.

2.1.3 Прихильність вищого керівництва

Прихильність вищого керівництва є важливим фактором у забезпеченні впровадження заходів безпеки в організації, і воно повинно бути залучено з самого початку до самого процесу визначення політики.

Таке зобов'язання може приймати різні форми, але зазвичай найпоширенішою з них є схвалення вищим керівним органом політики безпеки, яка буде впроваджуватися, в ідеалі - підписання відповідного документа.

На додаток до цього формального аспекту, прихильність керівництва має й інші способи відображення у зв'язку з безпекою:

- ✓ Організаційні аспекти: якщо керівництво зобов'язується забезпечувати безпеку, функція, відповідальна за безпеку, повинна бути незалежною від операційної/виробничої діяльності, щоб не виникало здорового конфлікту інтересів між операційною діяльністю та безпекою. Наприклад, особа, відповідальна за інформаційну безпеку, не повинна звітувати перед особою, відповідальною за інформаційні системи.
  З іншого боку, керівництво заохочуватиме та братиме участь у роботі комітетів/робочих груп, створених для прийняття адекватних рішень та управління безпекою спільно з виробничими та допоміжними підрозділами організації.
- ✓ Ресурсне забезпечення: Керівництво забезпечить достатні засоби, в межах можливостей організації, для впровадження, функціонування та підтримки механізмів безпеки, визначених відповідно до мети функції безпеки.
- ✓ Підвищення обізнаності: Керівництво підтримуватиме, братиме участь і стимулюватиме заходи, пов'язані з підвищенням рівня обізнаності працівників і зовнішніх користувачів, залучених до забезпечення безпеки, зокрема, критично важливих об'єктів інфраструктури.
- ✓ Відносини з третіми сторонами: Директорат сприятиме встановленню відносин з іншими організаціями, приватними чи державними, які сприяють безпеці (CERT, FFCCS тощо).

2.1.4 Інтегральна природа безпеки

Незалежно від того, як організована безпека в інших сферах діяльності оператора, важливо підходити до захисту КІКП з комплексним підходом (тобто мати єдине уявлення про фізичні та кіберзагрози для них, а також розробити та впровадити стратегію захисту, яка об'єднує фізичні, IT, операційні та кадрові заходи).

Такий комплексний підхід не передбачає створення єдиної охоронної організації (хоча це було б доцільно, оскільки спростило б інтеграційні процеси), а передбачає наявність механізмів для забезпечення захисту на основі комплексного підходу (насправді, єдина охоронна організація не гарантує, що не збережеться подвійний підхід до захисту).

У зв'язку з цим оператор повинен вказати, наприклад, заходи, які забезпечують такий цілісний підхід:

- ✓ Існування єдиної організації з єдиними цілями, процесами та засобами.
- ✓ Робочі процедури (зустрічі, розробка процедур, спільні механізми моніторингу тощо), спрямовані на забезпечення глобального бачення.
- ✓ Наявність координуючих органів.

2.1.5 Оновлення

Політика безпеки повинна бути живим документом, який відображає зміни в навколишньому середовищі, інфраструктурі, а також зміни самого оператора.

Таким чином, організація повинна вказати механізми оновлення цієї політики, які, як правило, повинні бути втілені в процедурі дворічного перегляду (відповідно до положень Королівського указу), що встановлює відповідальність за проведення такого перегляду, аспекти, що підлягають аналізу, механізми внесення пропозицій щодо змін, а також затвердження, опублікування та розповсюдження змін (у тому числі, у сфері захисту ІСІ, відповідне інформування НКЦПІК).

Враховуючи можливість того, що процес перегляду може бути завершений без змін, існуюча процедура повинна генерувати необхідні докази, які дозволять підтвердити, що перегляд відбувся (протоколи засідань, пункт на порядку денному Комітету з безпеки тощо), навіть якщо він не призвів до змін у Політиці.

2.2 СИСТЕМА УПРАВЛІННЯ БЕЗПЕКОЮ

2.2.1 Організація безпеки та зв'язку

Керівництво організації має офіційно оформити призначення керівника служби безпеки та уповноваженого (уповноважених) відповідно до внутрішніх процедур. Функція безпеки, зокрема, повинна забезпечувати наскрізне охоплення всієї організації, щоб можна було виконати встановлені вимоги.

На додаток до документації, яка повинна бути надана щодо організації безпеки, в основному загальної організаційної схеми оператора, що визначає корпоративну структуру безпеки, і конкретної організаційної схеми функції безпеки, де можна перевірити ієрархічний рівень різних ролей і існуючих комітетів з безпеки, є ще два аспекти, які також слід враховувати.

З одного боку, оператор повинен відобразити, яким чином запропонована організація в достатній мірі забезпечує впровадження та дотримання Політики. У зв'язку з цим слід враховувати, що в організаціях існують функції, які співпрацюють у впровадженні заходів безпеки, такі як, наприклад

Наприклад, функція внутрішнього аудиту, яка в багатьох організаціях має чітку відповідальність за забезпечення дотримання внутрішніх політик та нормативно-правової бази, що застосовуються до організації. З цієї причини слід розглянути можливість їх включення до вищезгаданих організаційних схем.

З іншого боку, існують інструменти, які можуть допомогти продемонструвати необхідну достатність. Наприклад, матриці RACI можуть бути використані для уточнення ролей та обов'язків.[3] Матриці RACI можна використовувати для уточнення ролей та обов'язків, оскільки вони дозволяють точно відобразити, хто є відповідальним і підзвітним за які завдання в організації. Ці матриці будуються шляхом зазначення різних обов'язків, що існують (в даному випадку це будуть завдання, пов'язані із застосуванням та перевіркою Політики безпеки) в рядках, а в стовпчиках - функцій (посад), що існують в організації. Нарешті, перехрестя використовуються для того, щоб вказати, де це можливо, роль функції у виконанні певного завдання. Використовувані ролі - це ті, що дали назву матриці:

- ✓ R - Responsible (відповідальна особа)
- ✓ A - Уповноважуючий (підзвітний)
- ✓ C - Consulted (консультований)
- ✓ I - Поінформований

Для того, щоб побудувати такі матриці, необхідно враховувати деякі дуже прості правила:

- ✓ Для кожного завдання/обов'язку може бути лише один "A" (один затверджувач).
- ✓ Клітинки можуть бути порожніми, що означає, що певна функція не задіяна у виконанні завдання.
- ✓ Всі учасники повинні схвалити матрицю RACI, яку буде розроблено.

Нарешті, якщо деякі завдання передаються на аутсорсинг третій стороні, ця третя сторона, по-перше, повинна бути зазначена в матриці RACI з відповідною роллю у виконанні доручених завдань, а по-друге, слід вказати існуючі зобов'язання.

Зазвичай, найдоцільніше збирати цю інформацію в договорі про надання послуг, хоча є й інші варіанти:

- ✓ Може існувати каталог послуг, який містить замовлення постачальнику(ам).
- ✓ Для існуючих зобов'язань угоди про рівень обслуговування можуть використовуватися як механізми контролю та моніторингу роботи постачальника (метрики, які також повинні включати елементи безпеки).

У будь-якому випадку, оператор повинен описати механізми, які він використовує для контролю за дотриманням існуючих зобов'язань з постачальником і, зокрема, як він управляє субпідрядними завданнями самого постачальника та звітуванням про інциденти.

Якщо в охоронній організації існує Комітет з питань безпеки, бажано, щоб принаймні один член або представник керівництва був членом цього комітету, щоб рішення, прийняті на ньому, неявно підтримувалися керівництвом.

[3] Додаток 1, розділ 7.2.

2.2.1.1 Офіцер з питань безпеки та зв'язку / Офіцер з питань безпеки[4]

Оператор повинен надати інформацію, запитувану в цьому розділі, і, крім того, може також надати інформацію про механізми надзвичайних ситуацій і безперервності, прийняті для забезпечення зв'язку з відповідальним за безпеку та зв'язок у разі інцидентів або у випадку, якщо зазначена особа зазнає впливу будь-якого виду несприятливої події, що перешкоджає його/її доступу до неї.

2.2.2 Навчання та підвищення обізнаності

План навчання та інформування, наданий оператором, повинен бути узгоджений з метою політики безпеки. План повинен містити запитувану інформацію на додаток до звичайної інформації будь- якого такого плану:

- ✓ Тривалість. Плани навчання та підвищення обізнаності, як правило, розраховані на кілька років.
- ✓ Цілі. Тобто, покращення в навчанні та обізнаності, які має забезпечити реалізація плану.
- ✓ Цільова аудиторія. Класифікація та сегментація цільової аудиторії. На цьому етапі важливо розглянути групи, які беруть участь у захисті життєво важливих послуг, як безпосередньо, так і опосередковано, і незалежно від того, чи є вони штатними працівниками, чи залученими на умовах субпідряду.
- ✓ Медіа - Повідомлення. Для кожної з цільових аудиторій, визначених вище, слід відобразити повідомлення, яке потрібно донести, а також засоби, які будуть використані для цього (аудиторні тренінги, відео, онлайн-курси, регулярні інформаційні бюлетені, спеціальний розділ в інтранеті, внутрішні комунікаційні кампанії і т.д.).
- ✓ Моніторинг. Іншими словами, механізми оцінки, які будуть використовуватися для перевірки того, що вжиті заходи сприяють досягненню цілей, викладених у плані (такі як, наприклад, показники придатності та залучення, політика щодо підписів учасників, проведення тестів на залучення тощо). Сюди також можна включити інформацію про те, хто відповідає за збір інформації, методологію, яка буде використовуватися, періодичність проведення заходів, а також передбачені коригувальні дії.
- ✓ Оновлення. Як і будь-який інший план, План навчання та інформування має тимчасовий характер, тому його слід періодично оновлювати, щоб переглядати його цілі, повідомлення тощо. План повинен містити процедуру перегляду: відповідальну особу, елементи, що підлягають перегляду, а також механізм затвердження, публікації та розповсюдження змін до Плану.

Стосовно обізнаності користувачів не слід забувати, що не лише курси та елементи поширення інформації впливають на рівень обізнаності людей, але й каральні елементи також впливають на наші поведінкові моделі, тому плани з підвищення обізнаності можуть також включати такі елементи, як

- ✓ Процедури застосування санкцій у разі недотримання Політики безпеки.
- ✓ Поширення інформації про санкції, інциденти... пов'язані з безпекою.
- ✓ Публікація інформації про моніторинг наявних засобів контролю.

[4] Додаток 1, розділ 7.3

Нарешті, не слід забувати про необхідність прихильності керівництва через надання необхідних засобів і ресурсів, а також через публічні та видимі знаки підтримки, які допоможуть розробити та забезпечити успіх запроваджених планів.

2.2.3 Застосована модель управління

Модель управління безпекою, що використовується організацією для забезпечення впровадження та дотримання Політики безпеки, включає всі типові елементи таких схем, які зазвичай асоціюються з циклом безперервного вдосконалення PDCA (Plan - Do - Check - Act) або циклом Демінга, з тією особливістю, що вони повинні спеціально враховувати захист КІКІ:

- ✓ Створення системи управління (планування)
  - Визначте цілі та політику системи.
  - Створіть необхідні процеси та процедури для адекватного управління ризиками.
  - Створити механізми узгодження цілей системи з цілями бізнесу.
- ✓ Впроваджувати та експлуатувати систему управління та її різні компоненти (Робити)
  - Політики та процедури.
  - Контроль.
  - Процеси.
- ✓ Моніторинг та перегляд системи управління (Перевірка)
  - Оцінювати і, де це можливо, вимірювати ефективність процесів у порівнянні з тим, що визначено в політиці та цілях системи.
  - Повідомте про результати оцінки керівництву на розгляд.
  - Проводити профілактичні заходи.
  - Вжиття коригувальних заходів за результатами внутрішніх перевірок та аудитів.

Що стосується самих заходів безпеки, то на додаток до вищезгаданої системи управління, вони повинні охоплювати всі випадки, коли вони необхідні. Наприклад, їх можна розділити на наступні категорії:

- ✓ Профілактика та виявлення
  - Відповідальність за безпеку.
  - Аналіз та управління ризиками.
- ✓ Захист і оборона
  - Управлінський контроль.
  - Закупівля/забезпечення систем та інфраструктури.
- ✓ Попередження та аудити: оцінка та дотримання вимог.
- ✓ Вимірювання та постійне вдосконалення.
- ✓ Координація та реагування: взаємозв'язок між управлінням безпеки та іншими підрозділами організації.

У цьому контексті особливого значення набуває все, що пов'язано з механізмами моніторингу виконання заходів безпеки, а також використовуваними показниками ефективності та результативності, без шкоди для інших механізмів контролю, наприклад, тих, що здійснюються підрозділами внутрішнього аудиту та/або комплаєнсу. З цієї причини функція аудиту повинна включати їх у планування своєї роботи,

огляди, пов'язані із захистом IICC у всіх їхніх аспектах, не забуваючи про такі елементи, як промислове програмне забезпечення для управління.

Аналогічним чином, врахування питань безпеки з самого початку при придбанні та створенні нових систем та інфраструктур є важливим для уникнення помилок, що виникають під час їх проектування. Таким чином, перш ніж будь-яка система або інфраструктура буде введена в експлуатацію, слід перевірити, чи відповідає вона необхідним вимогам безпеки згідно з планом безпеки, прийнятим організацією.

2.2.4 Комунікація

Для того, щоб забезпечити ефективний обмін інформацією між CNPIC та самим оператором з усіх аспектів, що стосуються сфери захисту критичної інфраструктури, важливо, щоб оператор розробив відповідні процедури для ефективного здійснення такої комунікації. Таким чином, оператор повинен включити наступні процедури та будь-які інші, які він вважає за потрібне, а саме

Повідомлення до CNPIC:

- ✓ Інциденти або ситуації, які можуть поставити під загрозу або скомпрометувати цілісну безпеку будь-якої з інфраструктур, менеджером та/або власником якої є оператор, відповідно до протоколу обміну інформацією та інцидентами PIC, розробленого цим Центром та наданого критично важливим операторам.
- ✓ Зміни організаційного, планового або структурного характеру, які відбуваються всередині самого оператора і які певним чином впливають на критичну інфраструктуру, що перебуває під захистом (наприклад, коригування портфеля послуг, злиття, придбання або продаж активів, технічні зміни, модифікація інфраструктури, зміна об'єктів і т.д.).

CNPIC

CENTRO NACIONAL DE PROTECCION
DE INFRAESTRUCTURAS CRÍTICAS

реляція про
надані основні послуги
оператором CRITICO

Основна мета полягає в тому, щоб дати можливість оператору зробити презентацію та короткий опис компанії або групи, до якої він належить, що може враховувати такі аспекти, як

- ✓ Назва компанії та материнська компанія.
- ✓ Розбивка корпоративної структури.
- ✓ Розподіл складу акціонерів та ступінь власності.
- ✓ Головний офіс та географічне розташування.
- ✓ Сектор(и), до якого(их) вона належить відповідно до здійснюваної діяльності.
- ✓ Підсектор(и) для кожного виду діяльності.
- ✓ Роботу виконано.
- ✓ Постачальники, необхідні для надання визначених основних послуг (включаючи таку інформацію, як, наприклад, назва постачальників та тип поставок, що надаються).
- ✓ Кінцеві споживачі наданих послуг, визначені як важливі (включаючи таку інформацію, як, наприклад, країни, адміністрації, компанії, приватні особи тощо).

3.1 ВИЗНАЧЕННЯ ОСНОВНИХ ПОСЛУГ

ЦБ повинен надати короткий опис основних послуг, що надаються громадянам, відповідно до концепції основних послуг у ст. 2 (a) Закону, в межах сектору або стратегічної підгалузі, до якої він входить. З цією метою він може надати таку інформацію:

- ✓ Визначення послуг та сфер діяльності, які є або можуть бути важливими для громадян.
- ✓ Типологія активів або критичної інфраструктури, від яких залежить послуга або сфера діяльності.
- ✓ Матеріальні засоби, персонал та ресурси, доступні для надання послуги.
- ✓ Географічне розташування, де надається послуга, визначена як основна (наприклад, країна, автономна громада, місто тощо), з визначенням населених пунктів та оцінкою кількості населення в зоні її впливу.
- ✓ Компанії, з якими вона має спільне географічне розташування.

3.2 ПІДТРИМКА ІНВЕНТАРИЗАЦІЇ ОСНОВНИХ ПОСЛУГ

Необхідно описати процедуру ведення інвентаризації послуг, визначених як суттєві в результаті нормального розвитку, якого зазнає будь-яка компанія щодо послуг, які вона пропонує. Необхідно описати форми та процедури ідентифікації, ведення, перегляду та оновлення, а також орган, відповідальний за них. Таке ведення повинно принаймні враховувати:

- ✓ Коригування портфелів послуг, злиття, поглинання, продаж активів...
- ✓ Інтернаціоналізація операційних процесів.
- ✓ Періоди, встановлені в Плані відповідно до пункту 1.4, включені до керівництва з мінімального змісту ОСП (законодавство встановлює періоди оновлення раз на два роки або коли відбуваються значні зміни).

3.3 ВИВЧЕННЯ НАСЛІДКІВ ПЕРЕРИВАННЯ НАДАННЯ ОСНОВНОЇ ПОСЛУГИ

Вивчення наслідків, яке має здійснювати СО, має проводитися відповідно до того, що розуміється в законодавстві під "перервою", яка виходить за рамки простої недоступності послуги, оскільки розглядає *"недоступність основної послуги [...], спричинену певною зміною або перервою в часі або частковим чи повним руйнуванням інфраструктури, яка управляє такою послугою".*

Необхідно провести аналіз результатів дослідження наслідків перебоїв та недоступності для кожної з послуг, визначених як основні у разі їх виникнення:

- ✓ Зміна його функції.
- ✓ Перерва в часі.
- ✓ Часткове або повне руйнування інфраструктури, яка керує послугою.
- ✓ І так далі.

Крім того, для кожного випадку слід чітко визначити наступну інформацію:

- ✓ Географічний масштаб та кількість людей, які можуть зазнати впливу.
- ✓ Ефекти з часом.
- ✓ Економічний вплив.
- ✓ Вплив на навколишнє середовище.
- ✓ Вплив на життя та здоров'я людей.
- ✓ Вплив на операторів та основні залежні послуги.
- ✓ Наявність альтернативних варіантів надання основних послуг або механізмів реагування на надзвичайні ситуації, що надаються самим оператором, а також рівень погіршення якості послуг, який вони спричиняють.

3.4 ВЗАЄМОЗАЛЕЖНОСТІ

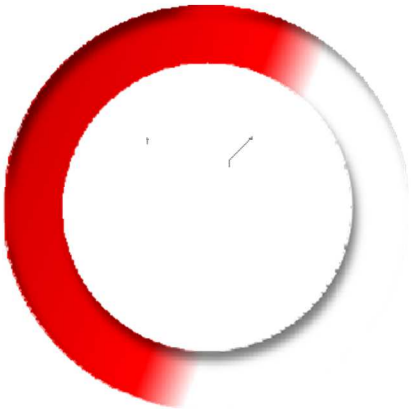
Необхідно скласти опис можливих взаємозалежностей між основними послугами та критичною інфраструктурою, що їх підтримує, а також з іншими операторами в тому ж або інших секторах, які необхідно враховувати при аналізі ризиків. Приклади взаємозалежностей, які слід розглянути, включають наступне:

- ✓ Між власними об'єктами або послугами оператора.
- ✓ З операторами в тому ж секторі.
- ✓ З операторами з різних секторів.
- ✓ З операторами в інших країнах, незалежно від того, працюють вони в тому ж секторі чи ні
- ✓ З їхніми постачальниками послуг у ланцюжку поставок.
- ✓ З укладеними контрактами з постачальниками послуг ІКТ, такими як: телекомунікаційні провайдери, центри обробки даних, служби безпеки (Операційний центр безпеки, приватний CERT тощо) та будь-які інші, із зазначенням для кожного з них назви постачальника, послуг, що надаються за контрактом, угод про рівень обслуговування (SLA) та відповідності послуг, що надаються, загальній політиці безпеки Оператора.
- ✓ з основними послугами, що надаються іншими операторами в тому ж секторі, з коротким поясненням причини такої взаємозалежності.
- ✓ Надаючи основні послуги іншим операторам у різних секторах.

- ✓ З основними послугами, що надаються операторами в інших країнах.
- ✓ І так далі.

CNPIC

CENTRO NACIONAL DE PROTECCION
DE INFRAESTRUCTURAS CRÍTICAS



МЕТОДОЛОГІЯ АНАЛІЗУ РИЗИКІВ

Оператор повинен мати методологію аналізу ризиків для виявлення та управління основними ризиками, на які наражаються критичні послуги з переробки та збуту кожного оператора.

4.1 ОПИС МЕТОДОЛОГІЇ АНАЛІЗУ

Будь-які міжнародно визнані методології, які оператори, можливо, захочуть використовувати для виявлення та подальшого управління своїми ризиками, повинні принаймні враховувати кроки, викладені в наступних параграфах.

Фундаментальним аспектом методологій аналізу ризиків є те, що різні значення, які використовуються, та оцінки різних параметрів (вразливість, вплив...) повторюються з використанням одних і тих самих критеріїв протягом тривалого часу для отримання порівнянних значень.

4.2 ІДЕНТИФІКАЦІЯ ТА ОЦІНКА АКТИВІВ, ЩО ПІДТРИМУЮТЬ ОСНОВНІ ПОСЛУГИ

Рівень деталізації повинен охоплювати щонайменше наступне:

- ✓ Надані послуги; вони можуть бути згруповані в однорідні класи з метою впливу на третіх осіб.
- ✓ Залежності елементів, які є надлишковими таким чином, що в принципі не є критичними для надання послуг, але стають критичними, якщо будь-який з них виходить з ладу.
- ✓ Залежність від послуг третіх сторін, що вказує на залежність між послугами та можливу взаємодоповнюваність, коли одна послуга може замінити іншу (план на випадок непередбачуваних обставин).
- ✓ Фізичні об'єкти, зокрема будівлі, огородження та трубопроводи, які можуть бути вразливими до атак або інцидентів.
- ✓ Команди людей з критично важливими ролями.
- ✓ Підтримка інформаційних систем як системи, не заглиблюючись у компоненти, якщо вони не є унікальними.
- ✓ Промислові системи управління установками (SCADA-системи).

Оцінка активів в основному ґрунтується на оцінці наслідків, що виникають в результаті переривання надання послуги. З точки зору критеріїв такої оцінки, необхідно враховувати положення Закону 8/2011 щодо "горизонтальних критеріїв критичності".

Позавідомчі організації та інші суб'єкти, які мають законний інтерес, можуть звернутися до CNPIC для отримання типової моделі активів, яка може бути використана в якості керівництва для виконання цієї роботи.

4.3 ІДЕНТИФІКАЦІЯ ТА ОЦІНКА ЗАГРОЗ

На основі переліку виявлених активів слід визначити загрози, які можуть вплинути на ці активи, щоб спробувати охопити якомога більше потенційних ризикових ситуацій.

Для такої ідентифікації рекомендується створити таксономію з кодом, який ідентифікує кожен тип загрози, та ієрархічну структуру, яка може бути вдосконалена за необхідності,

Для кожної потенційної небезпеки, що розглядається, слід встановити шкалу ймовірності виникнення з метою подальшого аналізу (якісного або кількісного).

Командири та інші офіцери повинні звертатися до дерева загроз, наданого CNPIC, приділяючи особливу увагу загрозам терористичного або навмисного походження.

4.4 ОЦІНКА ТА УПРАВЛІННЯ РИЗИКАМИ

Метою цієї діяльності є визначення комбінацій активів/загроз, які можуть вплинути на надання критично важливих послуг, з конкретизацією цих наслідків загалом і особливо на доступність послуг.

Для досягнення цієї мети необхідно оцінити потенційний вплив, який матеріалізація кожної загрози матиме на активи, визначені оператором. Потенційний вплив вимірює можливу шкоду, незалежно від того, чи є вона більш або менш ймовірною. Він просто визначає, чи можлива вона.

Може виникнути потреба у визначенні погіршених рівнів обслуговування, які, хоча і не забезпечують якість, необхідну за нормальних умов, але забезпечують певний рівень "живучості".

На основі цієї оцінки розраховується потенційний ризик як результат поєднання потенційного впливу з імовірністю того, що загроза матеріалізується у вигляді інциденту або атаки.

Всіма потенційними ризиками, які були виявлені, необхідно буде управляти. Це управління полягає у визначенні заходів безпеки для зменшення потенційних ризиків. Особливий інтерес представляє контроль інцидентів. Ризики, що виникають в результаті впровадження цих заходів контролю, визначатимуть залишкові ризики, на які наражається кожен оператор.

Зокрема, враховуючи характер навмисних загроз, оператор повинен вказати, як він буде реагувати на малоймовірні загрози з високим ступенем впливу (в будь-якому з вимірів їх оцінки). У зв'язку з цим він повинен вказати комбінацію заходів безпеки, які він буде застосовувати для запобігання, виявлення або дій у випадку, якщо будь-яка з цих загроз, наприклад, матеріалізується:

- ✓ Система раннього виявлення.
- ✓ Процедури реагування на інциденти.
- ✓ Механізми на випадок непередбачених обставин.
- ✓ І так далі.

Було б доцільно, як частину методології аналізу ризиків, вказати форму, в якій повинні бути представлені результати аналізу ризиків, і зібрати необхідну інформацію для подальшої оцінки аналізу ризиків Радою з МСФЗ.

5

КРИТЕРІЇ ДЛЯ ЗАСТОСУВАННЯ КОМПЛЕКСНИХ ЗАХОДІВ БЕЗПЕКИ

В якості належної практики для впровадження комплексних заходів безпеки Оператор може оберіть заходи безпеки, які необхідно впровадити, наприклад, на основі міжнародно визнаних стандартів безпеки та галузевого або загального законодавства.[5]

У сфері логічної безпеки належною практикою є вибір засобів контролю безпеки, які слід впроваджувати та керувати ними, на основі ISO 27002:

- ✓ Визначте політику корпоративної безпеки
- ✓ Організація інформаційної безпеки
- ✓ Управління активами
- ✓ Кадрова безпека
- ✓ Комунікації та управління операціями
- ✓ Контроль доступу
- ✓ Придбання, розробка та обслуговування інформаційних систем
- ✓ Управління інцидентами безпеки
- ✓ Управління безперервністю бізнесу
- ✓ Дотримання чинного законодавства
- ✓ Огляд та аудит діючої інтегрованої системи управління безпекою.

У сфері фізичної безпеки не існує жодних правил щодо каталогу попередніх заходів безпеки, але він повинен відповідати тому, що визначено законодавством таких країн, як

Приватна охорона, особливо те, що міститься в Наказі Міністерства внутрішніх справ № 316/2011, і його посилання на стандарт UNE/EN.

У зв'язку з цим особливо корисним буде дотримання рекомендацій стандарту UNE/CLC TS 50131-7 (Системи сигналізації. Системи охоронної сигналізації. Частина 7. Посібник із застосування).

З огляду на комплексний підхід до заходів безпеки та відповідно до загальної класифікації заходів, наведеної в розділі 4.2 "Заходи безпеки" Посібника з мінімального складу ЗІЗ, доцільно відобразити критерії застосування різних заходів, включених до цієї класифікації, які відтворені в наступній таблиці з деякими додатковими деталями.

Що стосується цих критеріїв, слід ще раз підкреслити, що пріоритетом має бути впровадження цих заходів відповідно до впливу, який загрози можуть мати на основні послуги (тобто ймовірність відіграє другорядну роль, оскільки метою є запобігання та захист критично важливої інфраструктури).

УПО та інші зацікавлені сторони, які мають законний інтерес, можуть звернутися до ЦНПІК, щоб отримати модель дерева гарантій, яка може бути використана в якості керівництва для здійснення цієї діяльності.

Нижче наведено приклади заходів безпеки, що застосовуються до активів фізичної та інформаційної безпеки:

[5] Додаток 2 - Перелік стандартів та найкращих практик містить перелік документації, яка може бути використана для визначення комплексних заходів безпеки.

	АКТИВИ	
	ФІЗИКА	ІНФОРМАЦІЙНІ СИСТЕМИ
ОРГАНІЗАЦІЙНІ АБО УПРАВЛІНСЬКІ		
Аналіз ризиків	Оцінка та аналіз небезпек, впливів та ймовірностей для визначення рівня ризику.	
Планування	Визначення цілей та програмування заходів для їх досягнення.	
Визначення ролей та обов'язків	Розподіл обов'язків з безпеки	
Регуляторний орган	Розробка політик, стандартів і процедур безпеки	
Відповідність нормативним вимогам	Ідентифікація та дотримання чинних нормативно-правових актів	
Сертифікація, акредитація та оцінка безпеки	Періодичні перевірки систем для оцінки рівня їхньої безпеки.	
ОПЕРАЦІЙНІ АБО ПРОЦЕДУРНІ		
Управління активами та конфігурацією	Ідентифікація активів, контроль запасів	
Навчання та підвищення обізнаності	Плани підвищення обізнаності та навчання з питань безпеки	
Плани на випадок надзвичайних ситуацій	Комп'ютерні та фізичні плани на випадок надзвичайних ситуацій	
Постійний моніторинг	Безперервна оцінка / аудит систем	
Безпека персоналу	Процедури відбору, внутрішні правила, процедури звільнення	
Керування доступом - Керування користувачами	Додавання, видалення та модифікації	
Керування доступом - Тимчасове керування доступом	людей, транспортних засобів тощо.	Тимчасові ідентифікатори користувачів систем (технічне обслуговування...)
Керування доступом - Контроль входу та виходу	Посилки, листування...	Медіа, обладнання інформації (DLP, DRM...)
Оперативні процедури для персоналу служби безпеки	Контроль безпеки	Н/Д
Евакуація	План евакуації	Н/Д
ЗАХИСТ АБО ТЕХНІЧНИЙ		
Заходи профілактики та виявлення		
Захист від вторгнення	Фізична та електронна охорона периметра, системи виявлення по периметру	Міжмережеві екрани, DMZ, сегментація мережі , захист робочих станцій, шифрування, VPN
Контроль доступу (включаючи автентифікацію)	Люди, транспортні засоби, посилки та товари (людські ресурси, активні картки, зчитувачі карток, зчитувачі номерних знаків, турнікети), сканер тощо).	Реєстрація користувачів, управління привілеями, управління секретними ключами, перегляд прав доступу..., ідентифікатори користувачів SSII доступу
Безпечне встановлення та налаштування	Безпечна конфігурація обладнання та систем до їх введення в експлуатацію, обслуговування обладнання та контроль змін. Забезпечення умов умови навколишнього середовища для його роботи (температура, вологість...)	
Захист від шкідливого програмного забезпечення	Н/Д* Н/Д* Н/Д* Н/Д* Н/Д* Н/Д* Н/Д* Н/Д* Н/Д* Н/Д* Н/Д* Н/Д* Н/Д* Н/Д* Н/Д	Встановлення антивірусних, антишпигунських та інших систем.
Безпечна розробка додатків	Н/Д* Н/Д* Н/Д* Н/Д* Н/Д* Н/Д* Н/Д* Н/Д* Н/Д* Н/Д* Н/Д* Н/Д* Н/Д* Н/Д* Н/Д	Розвиток на основі кращих практик, аудитів передвиробнича підготовка
Заходи з координації та моніторингу		
Моніторинг	Системи відеоспостереження (камери, відеоспостереження)	IDS, системи забезпечення цілісності програмного забезпечення, системи моніторингу та ведення журналів

Координація (управління інцидентами)	Диспетчерський пункт, власний центр сигналізації, системи зв'язку...	Створення груп реагування на інциденти (CSIRT), інфраструктури SOC

супровідна документація

6.1 ПОЛІТИКА, КРАЩІ ПРАКТИКИ ТА РЕГУЛЯТОРНІ НОРМИ

Оператор повинен викласти в короткому довіднику всі нормативні акти та найкращі практики, що регулюють належне функціонування основних послуг, які надаються кожною з його інфраструктур, а також причини, чому вони застосовуються до них.

Нормативно-правові акти, що підлягають включенню, включають як національні, регіональні, європейські та міжнародні нормативні акти, так і галузеві нормативні акти, що стосуються:

- ✓ Фізична безпека.
- ✓ Кібербезпека.
- ✓ Інформаційна безпека.
- ✓ Особиста охорона.
- ✓ Екологічна безпека.
- ✓ Самозахист та запобігання професійним ризикам.

6.2 КООРДИНАЦІЯ З ІНШИМИ ПЛАНАМИ

Необхідно визначити всі ті плани, розроблені оператором, що стосуються різних аспектів, таких як безперервність бізнесу, управління ризиками, реагування, кібербезпека, самозахист, надзвичайні ситуації, які можуть бути скоординовані з Планом безпеки оператора та відповідними Спеціальними планами захисту, і які будуть активовані у разі відмови механізмів запобігання після того, як інцидент стався, повинні бути ідентифіковані.

ДОДАТОК 1:

ПРИКЛАДИ

7.1 ПОЛІТИКА БЕЗПЕКИ

7.1.1 Ухвалення та набуття чинності

Текст ухвалено <день> <місяць> <рік> <організацією, що затвердила>.

Ця Політика інтегрованої безпеки діє з цієї дати до моменту її заміни новою Політикою.

Цей текст скасовує попередній текст, затверджений <день> <місяць> <рік> <органом>, який його затвердив.

7.1.2 Вступ

Нормальне функціонування основних послуг, які <критичний оператор> надає населенню, залежить від низки інфраструктур, функціонування яких є необхідним і не допускає альтернативних рішень, відомих як критичні інфраструктури. Тому необхідно розробити однорідну і всеосяжну політику безпеки, яка визначає підсистеми безпеки, що мають бути впроваджені для їх захисту з метою запобігання їх руйнуванню, перериванню або порушенню роботи, що може призвести до порушення надання основних послуг населенню або до катастрофічних наслідків для життя людей або навколишнього середовища.

Для захисту від цих загроз необхідна стратегія, яка адаптується до мінливих умов навколишнього середовища, щоб забезпечити безперервне надання послуг. Це означає, що відділи повинні впроваджувати визначені заходи безпеки, а також постійно контролювати рівень надання послуг, відстежувати та аналізувати вразливості, про які повідомляється, і готувати ефективне реагування на інциденти, щоб забезпечити безперервність надання послуг.

Різні відомства повинні забезпечити, щоб безпека була невід'ємною частиною кожного етапу життєвого циклу життєво важливої послуги, починаючи з її концепції, через рішення про розробку або закупівлю та оперативну діяльність і закінчуючи її виведенням з експлуатації.

7.1.3 Застосування

Ця політика застосовується до всіх об'єктів критичної інфраструктури <критичного оператора> та до всіх членів організації без винятку.

7.1.4 Місія

Опишіть критичні цілі обслуговування оператора.

7.1.5 Нормативно-правова база

Перелічіть закони, нормативні акти та інші правила, національні або міжнародні, яким підпорядковується критичний оператор.

7.1.6 Організація безпеки

7.1.6.1 Комітети: ролі та обов'язки

Комітет інтегрованої безпеки складається з <...>. Корпоративні посади та назвидепартаментів в агентстві з'являються тут там, де це доречно.

Секретарем Комітету з питань безпеки ІКТ є <...>, його функції полягають у

<...>. Секретарем Комітету з фізичної безпеки є <...>, а його функції полягають у

<...>. Комітет з інтегральної безпеки підзвітний

<...>. Комітет інтегральної безпеки виконує такі

функції: <...>.

7.1.6.2 Ролі: ролі та обов'язки

У разі необхідності, слід зазначити деталі призначення співробітників служби безпеки та делеговані їмфункції.

Функції офіцера з питань безпеки та зв'язку також повинні бути детально описані.

7.1.6.3 Огляд

Завданням Комітету з інтегральної безпеки є перегляд цієї Політики безпеки та внесення пропозиційщодо її перегляду або підтримання в актуальному стані.

Політика має бути затверджена <затверджуючим органом> та доведена до відома всіх зацікавленихсторін.

7.1.7 Управління інформацією

<критичний оператор> обробляє персональні дані. У <документі про безпеку>, який можна знайти за адресою <вказати, як знайти документ про безпеку та отримати доступ до нього>, перелічені файли, яких це стосується, та особи, відповідальні за них. Всі інформаційні системи <критичного оператора> повинні відповідати рівням безпеки, що вимагаються нормативно-правовими актами щодо характеру та призначення персональних даних, включених до вищезгаданого документа про безпеку.

З іншого боку, інформація, що стосується Комплексного плану безпеки, буде оброблятися і захищатися відповідно до конкретних процедур (згідно з чинним законодавством) відповідно дотого, що вона розглядається як інформація з обмеженим доступом.

7.1.8 Управління ризиками

Усі послуги, на які поширюється дія цієї Політики, повинні проводити аналіз ризиків, оцінюючи загрозита ризики, на які вони наражаються. Цей аналіз повинен повторюватися:

- ✓ регулярно, принаймні раз на рік,

- ✓ коли змінюються послуги, що надаються,
- ✓ коли трапляється серйозний інцидент з безпекою,
- ✓ коли повідомляється про серйозні вразливості.

Для гармонізації аналізу ризиків Комітет з інтегрованої безпеки встановлює базову оцінку для різних типів інформації, що обробляється, та різних послуг, що надаються. У цьому контексті, Комітет з питань інтегрованої безпеки

7.1.9 Запобігання, виявлення, реакція та відповідь

Відділи повинні бути готові запобігати, виявляти, реагувати та відновлюватися після інцидентів відповідно до Закону про захист критичної інфраструктури.

7.1.9.1 Профілактика

Міністерства повинні уникати або, принаймні, максимально запобігати тому, щоб інформація, послуги, життя людей або навколишнє середовище завдавали шкоди через інциденти, спричинені зловмисними діями. Для цього департаменти повинні впровадити заходи безпеки, а також будь-які додаткові засоби контролю, визначені за допомогою оцінки загроз і ризиків. Ці засоби контролю, а також функції безпеки та обов'язки всього персоналу мають бути чітко визначені та задокументовані.

7.1.9.2 Виявлення

Оскільки служби можуть швидко погіршуватися через інциденти, починаючи від простого сповільнення до зупинки, служби повинні постійно відстежувати роботу на наявність аномалій у рівнях надання послуг і діяти відповідно.

Моніторинг є особливо актуальним, коли лінії захисту встановлені на різних рівнях, тому будуть встановлені механізми виявлення, аналізу та звітності, які регулярно охоплюють відповідальних осіб, і коли є значне відхилення від параметрів, які були попередньо встановлені як нормальні.

7.1.9.3 Відповідь

Відділи повинні:

 Встановіть механізми для ефективного реагування на інциденти безпеки.

 Призначте контактну точку для зв'язку щодо інцидентів, виявлених в інших відділах або інших критичних операторах.

 Створіть протоколи для обміну інформацією, пов'язаною з інцидентом.

 Зв'яжіться з силами та органами безпеки згідно з конкретними процедурами.

 Налагодити зв'язок з органами з надзвичайних ситуацій та цивільного захисту.

7.1.9.4 Відновлення

Щоб забезпечити доступність критично важливих послуг, відділи повинні розробити плани безперервності систем як частину свого загального плану безперервності бізнесу та діяльності з відновлення.

7.1.10 Обов'язки персоналу

Усі члени <критичного оператора> зобов’язані знати та дотримуватися цієї Комплексної політики безпеки, оскільки Комітет із комплексної безпеки зобов’язаний забезпечити необхідні засоби для того, щоб інформація дійшла до тих, кого це стосується.

Усі члени <критичного оператора> принаймні раз на рік відвідуватимуть комплексну сесію з питань безпеки. Буде запроваджено безперервну програму інформування для всіх членів <організації>, особливо для тих, хто нещодавно прийнятий на роботу.

Люди, відповідальні за використання, експлуатацію або адміністрування основних послуг, пройдуть навчання з безпечного поводження з системами в тій мірі, в якій вони потребують для виконання своєї роботи. Навчання буде обов’язковим перед тим, як взяти на себе відповідальність, незалежно від того, чи це ваше перше призначення, чи це зміна роботи чи обов’язків на ній.

7.1.11 Треті сторони

Коли <критичний оператор> надає послуги іншим <...> або обробляє інформацію від третіх осіб <...>, вони будуть ознайомлені з цією Комплексною політикою безпеки, будуть встановлені канали для звітування та координації відповідної Комплексної політики Комітети безпеки та процедури реагування на інциденти безпеки.

Коли <критичний оператор> використовує сторонні служби або передає інформацію третім сторонам, вони будуть ознайомлені з цією Політикою безпеки, яка стосується зазначених послуг або інформації. Зазначена третя сторона буде підлягати зобов’язанням, встановленим у зазначених положеннях, маючи можливість розробити власні операційні процедури для їх виконання. Буде встановлено спеціальні процедури звітування про інциденти та їх вирішення. Буде гарантовано, що персонал третьої сторони буде належним чином обізнаний про безпеку, принаймні на тому ж рівні, що встановлено в цій Політиці.

Якщо будь-який аспект Політики не може бути задоволений третьою стороною, як це вимагається в попередніх параграфах, буде потрібен звіт від Менеджера з безпеки, який визначає понесені ризики та спосіб їх усунення. Перш ніж продовжити, необхідно схвалити цей звіт особами, відповідальними за інформацію та відповідні послуги.

7.1.12 Розробка комплексної політики безпеки

Ця комплексна політика безпеки доповнює політику безпеки <критичного оператора> в різних питаннях:

 Перелічіть посилання на інші політики безпеки.

Ця Політика буде розроблена на основі правил безпеки, які стосуються конкретних аспектів. Правила безпеки будуть доступні всім членам організації, яким необхідно їх знати, зокрема тим, хто використовує, керує або керує інформаційно-комунікаційними системами.

Правила безпеки будуть доступні в інтранеті: URL та роздруковані за адресою (МІСЦЕ).

7.2 МАТРИЦЯ RACI

	Генеральний Директор - CEO	Комітет безпеки	Начальник Інформаційної Служби	Начальник служби безпеки	Відділ кадрів	Операційний Директор
Розробка з Політика в Безпека	A	C	I	R		
виконання з План Навчання і обізнаність		I		R	A	C
Підготовка та проведення аналізу ризики	A	R		I		C
План розробки з Лікування з Ризик	R	A		I		C

7.3 ПРИЗНАЧЕННЯ ВІДПОВІДАЛЬНИХ

Відповідальний з Безпека і Посилання

<Ім'я організація> призначає <ім'я і прізвище> як відповідального з безпеки та захисту . Заступником відповідального призначено <ім'я і прізвища>.

The даних з призначений є:

	Відповідальний	Заступник
Ім'я		
Адреса		
телефони		
Електронна пошта		
Номер індиф.карти засвідченої Уповноваженим органом.		
Наказ або копія призначення.		

Даний відповідальний, та в разі необхідності його заступник, будуть мати наступні функції:

- Представляти оператора ОКІ в комунікації з Уповноваженим органом

  - З питань забезпечення безпеки та захисту ввіреної інфраструктури

  - З питань планів реагування де зазначена дана організація та інфраструктура

- Для здійснення постійного обміну інформацією у визначений Законом метод

ПІДПИС

Делегати з Безпеки по критичній інфраструктурі.

<Ім'я організація> визначила наступних працівників як Делегата та його заступника по питання критичної інфраструктури.

Дані по Делегатам та їх заступникам :

інфраструктури		Відповідальний	Замінник
Інфраструктура X	Ім'я		
	Адреса		
	телефони		
	Електронна пошта		
	Довідка або копія призначення.		
Інфраструктура I	Ім'я		
	Адреса		
	телефони		
	Електронна пошта		

Делегат, та в разі його відсутності його заступник, призначені бути відповідальними за наступні питання:

- Надавати та приймати інформацію з питань безпеки та захисту від відповідних держ.органів
- Здійснювати оперативний обмін інформацією в разі настання інциденту..

ПІДПИС

8

Додаток 2 :

ПЕРЕЛІК СТАНДАРТІВ ТА КРАЩОЇ ПРАКТИКИ

Нижче наведено низку стандартів, посібників і найкращих практик, які існують на національному та міжнародному рівнях.

8.1 НАЦІОНАЛЬНІ СТАНДАРТИ ТА КРАЩА ПРАКТИКА

8.1.1 Системи SCADA та національна схема безпеки 6

У наведеній нижче таблиці містяться різні посібники з безпеки промислових систем управління (SCADA), посібники, пов'язані зі схемою національної безпеки, можна знайти за адресою: https://www.ccn-cert.cni.es/guias/guias - series-ccn-stic/800-guide-national-security-scheme.html. Ці посібники були підготовлені Національним криптологічним центром Національного центру розвідки Міністерства Президента та призначені для різних державних адміністрацій.

СЕРІЯ	CCN-STIC	ІМ'Я	ВЕРСІЯ
	480	Безпека системи SCADA	Бер-10
	480A	Безпека системи SCADA – Гід добра практики	лют-10
	480B	Безпека системи SCADA – Ризик-менеджмент	Бер-10
	480C	Безпека системи SCADA – Реалізація архітектури безпеки	Бер-10
	480D	Безпека в системи SCADA – Встановити можливості	Бер-10
	480E	Безпека в системи SCADA – Поліпшити обізнаність і навички	Січ-10
	480F	Безпека в системи SCADA – Керування ризиками третьою стороною	березень-09
	480G	Безпека в системи SCADA – Фасадна сторона Проекту	березень-09
	480H	Безпека в системи SCADA – Встановлення постійної адреси	Бер-10

8.1.2 Фізична безпека

UNE-EN 50131-1:2008/A1:2010 Системи сигналізації проти вторгнення та пограбування
Частина 1: Системні вимоги. Багатокомпонентний стандарт, специфічний для систем сигналізації
Надає загальний опис систем виявлення вторгнень із зазначенням ступенів безпеки.
UNE/CLC TS 50.131.7 Системи сигналізації. Системи охоронної сигналізації. Частина 7. Посібник із застосування
У ньому наведено посібник із правильного впровадження системи захисту від вторгнень із зазначенням кроків, яких слід виконати під час проекту, встановлення, запуску, обслуговування та експлуатації.

8.1.3 Метрики та індикатори

UNE 66175 Системи управління якістю. Керівництво по впровадженню індикаторних систем
Цей стандарт полегшує встановлення індикаторів і інформаційних панелей, які активно сприяють вимірюванню явищ, що стосуються діяльності організації, і полегшують прийняття рішень. Він також пояснює зв'язок між системами показників, індикаторами та цілями.

6 Посібників CCN-STIC щодо систем SCADA: https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic/400-guias- generales.html

8.1 МІЖНАРОДНІ СТАНДАРТИ ТА КРАЩА ПРАКТИКА

8.1.1 Управління та управління IT, включаючи якість і ланцюг постачання

ISO/IEC 20000 Інформаційні технології. Управління послугами

Це багатокомпонентний стандарт на основі ITIL (IT-інфраструктурна бібліотека) для керування IT-послугами. Це набір передових практик, застосовних до державного та приватного секторів. Можливі сертифікація, акредитоване навчання та використання інструментів для полегшення її впровадження.

ISO/IEC 20000 Частина 1:2005 Управління послугами інформаційних технологій. Описує вимоги до управління IT-послугами, на відповідність яким організація може бути сертифікована.

ISO/IEC 20000 Частина 2:2005 Управління послугами інформаційних технологій. Кодекс практики управління послугами. Він надає практичний посібник для розробників і набір хороших практик для управління послугами.

ISO/IEC 38500 – Корпоративне управління інформаційними технологіями – стандарт корпоративного управління інформаційними технологіями
Він містить керівні принципи для тих, хто відповідає за організації, щодо прийнятного, ефективного та ефективного використання інформаційних технологій в організації. Стандарт стосується процесу управління IT та рішень, пов’язаних з інформаційно-комунікаційними послугами організації.

ISO/IEC 13335 Управління IT-безпекою
Це багатокомпонентний стандарт, який містить набір вказівок щодо управління IT-безпекою, приділяючи особливу увагу засобам технічного контролю безпеки. Ці стандарти частково замінено сімейством 270xx.

ISO 9003:2004 Розробка програмного забезпечення - Настанови щодо застосування ISO 9001:2000 до комп'ютерного програмного забезпечення
Він розглядає аспекти якості від розробки, постачання, придбання, експлуатації та обслуговування програмного забезпечення.

Специфікація ISO/IEC 28000 для систем управління безпекою для ланцюга поставок
Його мета полягає в тому, щоб підвищити безпеку ланцюга постачання за допомогою аналізу ризиків і відповідних планів реагування. Для цього організація повинна оцінити середовище безпеки, в якому вона працює, стосовно фінансування, виробництва, управління інформацією, а також місць розташування, упаковки, зберігання, транспортування та розташування. Тож визначте, чи прийнято адекватні заходи безпеки та чи існують інші нормативні вимоги, яким дотримується організація.

8.1.2 IT-безпека

ISO/IEC 27000:2009
Це вступ і опис стандартів сімейства 270xx.

ISO/IEC 27001:2005 Системи управління інформаційною безпекою. Вимоги
Це офіційний набір специфікацій, який описує «Систему управління інформаційною безпекою (ISMS)» (ISMS іспанською), за якою організація може бути сертифікована.

ISO/IEC 27002:2005, Кодекс практики управління інформаційною безпекою
Це набір належних практик і заходів контролю, застосовних до управління безпекою інформаційних систем.

ISO/IEC 27003, Настанова щодо впровадження системи менеджменту інформаційної безпеки
Посібник для фасилітатора щодо впровадження ISO 27001. Описує проектування СУІБ та процес специфікації від початку до остаточного впровадження.

ISO/IEC 27006:2007 Вимоги до органів, що здійснюють аудит та сертифікацію систем управління інформаційною безпекою
Цей стандарт служить керівництвом для органів сертифікації щодо визначення формальних процесів сертифікації систем управління інформаційною безпекою як третіх сторін, залучених до процесу.

ISO/IEC 27007 Настанови щодо аудиту систем управління інформаційною безпекою
Стандарт, безпосередньо пов'язаний із ISO 19011. Надає вказівки щодо компетенції аудиторів і акредитаторів систем СУІБ, а також вимог до відповідності стандарту ISO/IEC 27001.

ISO 21827 Systems Security Engineering Capability Maturity Model (SSE CMM)
Він описує основні характеристики процесу розробки безпеки, який повинен існувати в організації, і включає існуючі практики в галузі.

8.2.3 Аварія та відновлення

ISO/IEC 24762 Керівні принципи щодо служб аварійного відновлення інформаційно-комунікаційних технологій
Містить інструкції щодо надання послуг аварійного відновлення для інформаційно-комунікаційних технологій (ICT DR), застосовних до власних (власних) і зовнішніх (зовнішніх) послуг.

BS 25999 Управління безперервністю бізнесу
Британський багатокомпонентний стандарт для управління безперервністю бізнесу. У першій частині встановлюються процеси, принципи та термінологія разом із набором належних практик для всього життєвого циклу управління безперервністю. Друга частина надає формальні специфікації, за якими перевіряють організації на відповідність. Це стане майбутнім стандартом ISO 22301 «Суспільна безпека – Системи управління готовністю та безперервністю – Вимоги».

SO/IEC 27031:2011 Інформаційні технології. Методи безпеки. Настанови щодо готовності інформаційно-комунікаційних технологій до безперервності бізнесу
На основі старого стандарту BS 25777:2008 Управління безперервністю інформаційно-комунікаційних технологій. Кодекс практики. Він містить рекомендації щодо концепцій і принципів, що лежать в основі інформаційних і комунікаційних аспектів забезпечення безперервності бізнесу. Цей стандарт охоплює всі події та інциденти, а не лише ті, що стосуються

інформаційної безпеки, на основі концепції ICT Readiness for Business Continuity (IRBC).

ISO/PAS 22399 Соціальна безпека - Керівництво щодо готовності до інцидентів та управління безперервністю роботи
Він містить вказівки для організації щодо розробки власних критеріїв ефективності щодо готовності до інцидентів, безперервності операцій, а дизайн системи управління дозволяє організації послідовно вимірювати свою «стійкість».

8.2.4 Метрики та індикатори

ISO/IEC 27004 Управління інформаційною безпекою. Вимірювання
Він надає вказівки щодо розробки та використання заходів і показників для оцінки ефективності встановлених засобів контролю та самої СУІБ, запровадженої в організації.

Аудит і контроль

ISO 19011:2002 Настанови щодо аудиту систем управління якістю та/або навколишнього середовища ISO 19011 Настанови щодо аудиту систем управління якістю та/або навколишнього середовища
Цей міжнародний стандарт містить настанови щодо управління програмами аудиту, проведення внутрішніх або зовнішніх аудитів систем управління якістю та/або навколишнім середовищем, а також щодо компетентності й оцінювання аудиторів.

8.2.5 Управління ризиками

ISO/IEC 27005:2008 Управління ризиками інформаційної безпеки
Надає вказівки щодо управління ризиками в IT-безпеці та підтримує підхід, заснований на оцінці ризиків, концепцій, запропонованих ISO/IEC 27001 та ISO/IEC 27002.

ISO 31000 Управління ризиками — Принципи та настанови
Цей стандарт замінює AS/NZS 4360. Він надає вказівки та принципи впровадження управління ризиками, встановлюючи, як організація повинна розуміти свій конкретний контекст, у якому слід запроваджувати управління ризиками. Таким чином, стандарт охоплює управління ризиками в широкому сенсі і не зосереджується конкретно на інформаційній безпеці чи IT-ризиках.

ISO/IEC 31010 Управління ризиками – Методи оцінки ризиків
Надає вказівки щодо вибору та систематичного застосування методів оцінки ризиків як невід'ємної частини управління ризиками, щоб менеджери могли зрозуміти ризики, які можуть вплинути на бізнес-цілі, щоб їх можна було оцінити та забезпечити ефективні засоби контролю та придатні для їх пом'якшення.

8.2.6 Охорона праці

OHSAS 18001 Системи управління охороною праці
Визначає вимоги до системи управління гігієною та безпекою праці (СУОП), призначеної для того, щоб організація могла контролювати свої ризики з гігієни та безпеки праці та покращувати ефективність захисту гігієни та безпеки праці.

8.2.7 Сертифікація та акредитація

ISO/IEC 15408:2008 (Інформаційні технології. Методи безпеки. Критерії оцінювання безпеки IT
Цей багатокомпонентний стандарт описує загальні критерії оцінки (CC) безпеки інформаційних технологій (IT). Продукти, які перевіряються на відповідність цьому стандарту, досягають певного рівня гарантії інформаційної безпеки. Цей рівень оцінювання визнається всіма членами, які дотримуються угоди (домовленості) про загальні критерії.

ISO/IEC TR 19791:2010 Інформаційні технології. Методи безпеки. Оцінка безпеки операційних систем
У цьому технічному звіті оцінка продуктів, встановлена стандартом ISO/IEC 15408 Common Criteria, поширюється на операційні системи, надаючи вказівки та критерії оцінки безпеки для цих систем, беручи до уваги середовище операційної системи, що підлягає оцінці, а також можливість декомпозиції складної операційної системи на домени безпеки, які можна незалежно оцінити.

8.2.8 Координація та відповідь

ISO/IEC 18043 Вибір, розгортання та функціонування систем виявлення вторгнень (IDS)
Надає посібник із розуміння переваг і обмежень IDS: як інтегрувати систему виявлення вторгнень у вашу організацію, розробити стратегію IDS і план впровадження, як ефективно керувати результатами та як інтегрувати систему IDS у практику організації, яка приймає враховувати юридичні потреби та потреби конфіденційності, які впливають на IDS.

ISO/IEC 27035:2011 Інформаційні технології. Методи безпеки. Управління інцидентами інформаційної безпеки
Інциденти так чи інакше трапляються завжди через недосконалість і неефективність превентивного контролю. Таким чином, ефективне управління інцидентами включає дефектні та коригуючі засоби контролю, призначені для мінімізації несприятливого впливу та отримання уроків щодо вдосконалення СУІБ, особливо впровадження більш ефективних запобіжних засобів контролю.

CENTRO NACIONAL DE PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS

CNPIC

CENTRO NACIONAL DE PROTECCION DE INFRAESTRUCTURAS CRÍTICAS