КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (12), 2021
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2021.12.172186
УДК 004.056.5

Гулак Генадій Миколайович
доктор технічних наук, доцент,
завідувач лабораторії досліджень кібербезпеки,
Інститут проблем математичних машин і систем Національної академії наук України, Київ, Україна
ORCID ID 0000-0001-9131-9233
h.hulak@ukr.net

Скітер Ігор Семенович
кандидат фізико-математичних наук, доцент, старший науковий співробітник
Інститут проблем безпеки атомних електростанцій
Національної академії наук України, Чорнобиль, Україна
ORCID ID 0000-0003-2334-2276
i.skiter@ispnpp.kiev.ua

Гулак Євген Геннадійович
Менеджер з інформаційної безпеки,
ТОВ "ДТЕК СЕРВІС", Київ, Україна
ORCID ID 0000-0003-4984-686X
geg180579@gmail.com

МЕТОДОЛОГІЧНІ ЗАСАДИ СТВОРЕННЯ ТА ФУНКЦІОНУВАННЯ ЦЕНТРУ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ ОБ'ЄКТІВ ЯДЕРНОЇ ЕНЕРГЕТИКИ

Анотація. Об'єкти ядерної енергетики (ОЯЕ) є складними системами структурного типу, які оперують великими масивами інформаційних потоків, викривлення або блокування яких потенційно може призвести до нештатних і навіть катастрофічних ситуацій. Стале безперервне автоматизоване керування технічними засобами зазначених об'єктів є запорукою забезпечення безпеки людини, суспільства та держави. Тому забезпечення гарантоздатності автоматизованих систем ОЯЕ як технологічної основи їх функціонування є пріоритетним завданням наукових досліджень і розробок у цій галузі. В умовах зростання у світі кількості та потужності кібератак на критичні інформаційні системи, тривалого протистояння держави цинічному агресору в гібридній війні і обмежених фінансових ресурсів координація та концентрація зусиль щодо забезпечення кібербезпеки ОЯЕ є єдиним шляхом для розв'язання визначених проблем в галузі. Метою таких заходів має стати побудова єдиного центру кібербезпеки ОЯЄ. Створення такого центру повинно підняти на якісно новий рівень стан інформаційної та функціональної безпеки підприємств галузі. Основними завданнями центру є: забезпечення реалізації компонентів організаційно - технічної моделі інформаційного захисту та кіберзахисту; встановлення обов'язкових вимог інформаційної безпеки для критично важливих об'єктів інформаційної інфраструктури з урахуванням міжнародних стандартів та специфіки галузі, що включає відповідні об'єкти критичної інформаційної інфраструктури; забезпечення моніторингу світового стану інформаційної безпеки та кібербезпеки ОЯЕ; протидії кіберзагрозам шляхом підвищення загальної ситуаційної обізнаності про інциденти та вразливості інформаційних систем і систем захисту серед галузевих установ та їх критичної інфраструктури; запобігання вторгненням шляхом обміну інформацією та організації ініціатив; зменшення вразливостей, запобігання загрозам та їх ефективна локалізація; моніторинг протидії загрозам на об'єктах ядерної енергетики; стимулювання та проведення навчання та підвищення рівня інформаційної обізнаності в частині кібербезпеки серед менеджерів критичної інфраструктури, відповідні випробування, дослідження та розробки. Функціонування центру дозволить координувати та контролювати виконання заходів щодо розгортання системи інформаційної безпеки для критичних об'єктів інформаційної інфраструктури на об'єктах ядерної енергетики. Крім того, він також дасть змогу запобігти втручанню в інформаційні

системи шляхом обміну інформацією та функціонування централізованих та децентралізованих технологічних систем та організаційних ініціатив. Це зменшить кількість наявних вразливостей, запобігатиме появі нових та сприятиме ефективній ідентифікації кібератак. Центр захищатиме від усього спектру загроз, працюючи зі спеціалізованими службами у віртуальному середовищі, стимулюючи та проводячи навчання з інформаційної безпеки серед фахівців; здійснюватиме моніторинг та впровадження стандартів інформаційної безпеки суб'єктами критичної інфраструктури об'єктів ядерної енергетики; розроблятиме та впроваджуватиме нові заходи безпеки для зменшення ризику реалізації кіберзагроз, які постійно та швидко змінюються та розвиваються.

Ключові слова: центр інформаційної безпеки; об'єкти ядерної енергетики; модель системи управління кібербезпекою; критична інфраструктура; протидія кіберзагрозам.

ВСТУП

Об'єкти ядерної енергетики (ОЯЕ) є складними системами структурного типу, які оперують великими масивами інформаційних потоків, викривлення або блокування яких потенційно може призвести до нештатних і навіть катастрофічних ситуацій. Стале безперервне автоматизоване керування технічними засобами зазначених об'єктів є запорукою забезпечення безпеки людини, суспільства та держави. Тому забезпечення гарантоздатності автоматизованих систем ОЯЕ як технологічної основи їх функціонування є пріоритетним завданням наукових досліджень і розробок у цій галузі. В умовах зростання у світі кількості та потужності кібератак на критичні інформаційні системи, тривалого протистояння держави цинічному агресору в гібридній війні і обмежених фінансових ресурсів координація та концентрація зусиль щодо забезпечення кібербезпеки ОЯЕ є єдиним шляхом для розв'язання визначених проблем в галузі. Метою таких заходів має стати побудова єдиного центру кібербезпеки ОЯЕ.

Постановка проблеми. Управління кібербезпекою об'єктів критичної інфраструктури визначається як управління системою, що складається з множини територіально розподілених елементів, кожний з яких функціонує за власними законами та здійснює вплив на інші елементи системи.

Необхідність моніторингу та інтеграції великої кількості різноманітної динамічної інформації, що характеризує стан кожного елемента і системи у цілому, виявлення зв'язків і закономірностей їх взаємного впливу з урахуванням комплексу зовнішніх та внутрішніх загроз, прийняття обґрунтованих оперативних стратегічних рішень по забезпеченню безпеки в режимі реального часу, передбачає створення єдиної комплексної автоматизованої системи управління кібербезпекою об'єктів критичної інфраструктури (ОКІ).

Аналіз останніх досліджень і публікацій. У доповіді на засіданні Президії НАН України [1] зазначено на необхідності узагальнення досвіду, отриманого при здійсненні науково-технічного супроводу робіт, спрямованих на подолання наслідків аварії на ЧАЕС та перетворення об'єкта «Укриття» на екологічно безпечну систему, було наголошено на ефективності прикладних наукових досліджень у вирішенні актуальних науково-технічних проблем, що пов'язані з ліквідацією наслідків Чорнобильської катастрофи, необхідності системного підходу до реалізації задач, пов'язаних з забезпечення гарантоздатності автоматизованих систем ОЯЕ, в тому числі в частині забезпечення кібербезпеки об'єктів.

Роботи зарубіжних авторів мають широкий спектр підходів до проблеми комп'ютерної безпеки об'єктів ядерної енергетики. Так в роботі [2] зазначається, що

комп'ютерна безпека все більше визнається ключовим компонентом ядерної безпеки. У публікації викладено методологію проведення оцінок комп'ютерної безпеки на ядерних установках, яку також можна адаптувати для оцінки на об'єктах з використанням інших радіоактивних матеріалів. Автори [3] зазначають, що цифрові комп'ютери які були обрані системою безпеки на новозбудованих ядерних установках, призвели до зростання кіберзагроз для ядерних установок, а цілісність цифрових систем безпеки опинилася під загрозою. В роботі пропонується метод впровадження заходів та засобів кібербезпеки в рамках загальної системи безпеки на стадії її розробки. Метод запроваджує конкретні заходи безпеки, які базуються на практиці проекту будівництва ядерної установки. Огляд підходів ядерної промисловості до кібербезпеки з точки зору керівництва та проектування наведений в [4]. В роботі [5] розглянута проблема необхідності узагальнення проблем кіберзахисту на різних об'єктах критичної інфраструктури Німеччини та деяких інших країн.

Роботи вітчизняних дослідників в галузі безпеки ОЯЕ в основному спираються на реалізацію заходів з фізичної безпеки, яка, як складову, включає в себе підсистему інформаційної безпеки. Так в роботі [6] проведено аналіз факторів зниження ризику ядерних та радіаційних аварій на АЕС з урахуванням специфічних умов, пов'язаних з інформаційною безпекою в системі фізичного захисту атомних електростанцій. Розглянуто зв'язок гетерогенних факторів, що можуть впливати на ризик виникнення аварій на ОЯЕ, можливість і шляхи подальшого підвищення адекватності моделювання динаміки захисту інформації з обмеженим доступом, що безпосередньо стосується функціонування автоматизованого комплексу інженерно-технічних засобів фізичного захисту АЕС. Залишилося поза увагою авторів питання системного підходу до забезпечення кібербезпеки всього комплексу ядерних об'єктів України.

Проблематика комп'ютерної та інформаційної безпеки у площині фізичного захисту, а також нормативно-правове забезпечення комп'ютерної безпеки на ядерних об'єктах в Україні розглянуті у [7], де основний акцент зроблено на комп'ютерну безпеку інформаційних та керуючих систем (ІКС), важливих для ядерної безпеки. Надано приклад інтегрованого підходу до розгляду вимог з ядерної безпеки та захищеності з урахуванням взаємодії сфер забезпечення захищеності ІКС та ядерної безпеки. Наведено рекомендації та плани на майбутнє щодо вдосконалення комп'ютерної безпеки на ядерних об'єктах в Україні.

Розглядаючи аспекти інформаційної безпеки, автори [8] звертають увагу на потребу нових підходів до забезпечення безпеки для виживання в умовах постійного оновлення кіберзагроз, розробці інформаційних систем, спрямованих не тільки на технічний захист комп'ютерних систем та технологій, а й на запобігання впливу методів соціальної інженерії, підвищенням рівня культури інформаційної безпеки організації. Частково реалізований системний підхід до загальної проблеми інформаційної безпеки базується на створенні локальної модель системи комплексної оцінки рівня персоналу культури інформаційної безпеки (ІСК) як важливого компонента загальної організації інформаційної безпеки і стосується окремих підприємств, організацій тощо.

Систематизація методів, моделей та основних підходів забезпечення інформаційної безпеки, виявлення кіберзагроз та їх класифікації представлена в роботах [9], [10], [11]. У вказаних роботах проведений детальний аналіз методів і моделей безпеки розподілених інформаційних систем. Саме така кваліфікація методів щодо інформаційних систем дає змогу говорити про наступний крок до створення центів кібернетичної безпеки об'єктів критичної інфраструктури.

Метою статті є узагальнення підходів до аналізу розподілених інформаційних систем з точки зору їх інформаційної безпеки, системний підхід до кібербезпеки на рівні об'єктів критичної інфраструктури в ядерній енергетиці, забезпечення гарантоздатності автоматизованих систем ОЯЕ як технологічної основи їх функціонування, створення моделі взаємодії елементів інформаційної системи об'єктів критичної інфраструктури.

ОСНОВНІ ЗАСАДИ УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ.

Об'єкти ядерної енергетики є складовою системи об'єктів критичної інфраструктури України. Управління кібербезпекою об'єктів критичної інфраструктури визначається як управління системою, що складається з множини територіально розподілених елементів, кожний з яких функціонує за власними законами та здійснює вплив на інші елементи системи. На сьогодні забезпечення інформаційної безпеки таких об'єктів регламентується міжнародними [12], [13], [14], [15] та вітчизняними нормативними документами та стандартами [16]-[18].

Необхідність моніторингу та інтеграції великої кількості різноманітної динамічної інформації, що характеризує стан кожного елемента і системи у цілому, виявлення зв'язків і закономірностей їх взаємного впливу з урахуванням комплексу зовнішніх та внутрішніх загроз, прийняття обґрунтованих оперативних стратегічних рішень по забезпеченню безпеки в режимі реального часу, передбачає створення єдиної комплексної автоматизованої системи управління кібербезпекою об'єктів ядерної енергетики. В дослідженні [18] розроблена модель, яка вирішує питання делегування задач кібернебезпеки для різних рівнів захисту. На відміну від представленої моделі розроблена комплексна модель взаємодії елементів ОЯЕ

Елементами інформаційної систем ОЯЕ при цьому виступають : система захисту інформації, програмно-апаратні засоби системи ОЯЕ, інсайдери, які взаємодіють між собою та зовнішнім середовищем.

Модель взаємодії елементів інформаційної системи об'єкту ядерної енергетики приведена на рис. 1.

Рис. 1. Модель взаємодії елементів інформаційної системи об'єкту ядерної енергетики

Основними об’єктами кіберзагроз для інформаційних систем ОЯЕ згідно [19] є:

• зловмисники,
• оператори ботнету,
• злочинні групи,
• іноземні спецслужби,
• інсайдери,
• фішери,
• сніфери,
• спамери,
• автори шпигунського і шкідливого програмного забезпечення,
• терористи,
• промислові шпигуни тощо.

Для протидії кібератакам зовнішнього порушника система захисту інформаційної системи ОКІ повинна мати наступні функції:

• захист периметра мережі;
• забезпечення безпеки міжмережевих взаємодій;
• моніторинг і аудит безпеки;
• виявлення і запобігання діям атак;
• резервне копіювання і відновлення даних;
• аналіз захищеності і керування політикою безпеки;
• контроль цілісності даних;
• захист від шкідливого програмного забезпечення;
• фільтрація контенту і запобігання витоку конфіденційної інформації;
• установка оновлень програмного забезпечення;
• адміністрування безпеки.

Система управління кібербезпекою ОЯЕ повинна забезпечити стійке, живуче і безпечне функціонування об'єктів; безпеку навколишнього середовища; захист інтересів особистості, суспільства і держави, а також споживачів послуг.

Система управління кібербезпекою ОЯЕ представляє собою комплексну організаційно-технічну систему, яка виконує функції аналізу стану, контролю, моніторингу та забезпечення безпеки як окремих функціональних елементів і процесів, так і системи в цілому.

Метою системи є забезпечення такого рівня кібербезпеки, при якому загрози й ризики знижені до мінімально прийнятного рівня [20].

Управління системою передбачає цілеспрямований вплив на об'єкт для підтримки його характеристик на заданому рівні. Управління вимагає постійного відстеження параметрів, що характеризують керований об'єкт, тобто функціонування встановленої системи контролю, моніторингу та оперативного реагування на зміну цих параметрів.

Основними напрямками забезпечення кібербезпеки є:

• нормативно-правове регулювання в сфері забезпечення кібербезпеки;
• класифікація об'єктів критичної інфраструктури;
• оцінка уразливості і ризиків, категоріювання об'єктів;
• розробка та реалізація вимог щодо забезпечення кібербезпеки;
• розробка і реалізація заходів щодо забезпечення кібербезпеки;
• здійснення контролю, моніторингу та нагляду в галузі забезпечення кібербезпеки;
• інформаційне, матеріально-технічне та науково-технічне забезпечення кібербезпеки;
• підготовка фахівців в області забезпечення кібербезпеки.

Основні цілі створення єдиного центру кібербезпеки (ЦКБ) ОЯЕ:

• підвищення ефективності прийняття управлінських рішень за рахунок впровадження нових інструментів управління кібербезпекою, що базуються на сучасних інформаційних технологіях і відповідних кращому міжнародному досвіду в сфері управління складними системами міжнаціонального масштабу;

• уніфікація процедур оцінки рівня кібербезпеки на основі формування відомчої класифікації станів безпеки та множини характеристичних показників поведінки (МХПП) систем;

• утворення належних умов для проведення оперативного (поточного) аудиту кібербезпеки інформаційних систем ОЯЕ на підставі МХПП, тестування систем кіберзахисту на основі затверджених методик, включаючи технології прихованого проникнення в системи;

• утворення умов для централізованого оперативного моніторингу конфігурацій програмних і апаратних платформ інформаційних середовищ, засобів захисту;

• підвищення кваліфікації всіх учасників процесів забезпечення кібербезпеки шляхом проведення в реальному часі тренінгів і навчань, які мають бути наближені до сучасних реалій;

• забезпечення за рахунок формування єдиного інформаційного простору керівного складу і працівників енергетичного комплексу структурованою достовірною та оперативною інформацією згідно наданих їм повноважень;

• скорочення часу на локалізацію наслідків реалізації кіберзагроз та відновлення штатного функціонування завдяки спеціально підготовленого персоналу та захищеного зберігання за дорученням власників систем резервних копій програмного забезпечення та інформаційних масивів;

• забезпечення системного підходу до оперативної аналітики стану кібербезпеки у кіберпросторі, виявлення та аналізу аномальної поведінки систем і мереж, оцінки ризиків, моделювання та прогнозування розвідку подій у кіберпросторі;

• реалізація заходів стримування шифруючих або руйнуючих шкідливих кодів, формування тактики їх нейтралізації та блокування;

• виявлення систематичних спроб проникнення та шкідливих ресурсів в кіберпросторі, інформування правоохоронних органів для прийняття рішень щодо оперативного впливу

• масштабування, інтеграція існуючих і новостворюваних систем кіберзахисту; розвиток інструментів збору та аналітичної обробки інформації.

Основні функції і задачі ЦКБ ОЯЕ приведені на рис. 2.

Рис. 2. Основні функції і задачі ЦКБ ОЯЕ

БАЗОВІ ПРИНЦИПИ РОЗРОБКИ ТА ФУНКЦІОНУВАННЯ ЦКБ ОЯЕ

Розробка ЦКБ ОКІ повинна здійснюватися на основі наступних базових принципів: інтеграції, централізації, уніфікації, еволюційності, масштабованості, модульності та живучості.

Принципи інтеграції та консолідації, реалізовані стосовно розрізнених масивів даних про об'єкт ядерної енергетики, припускають створення консолідованого сховища наборів даних: предметно-орієнтованих, інтегрованих, незмінних, підтримуючих хронологію, постійно оновлюваних новою достовірною інформацією.

Принципи централізації стосуються процедури ведення метаданих і нормативно-довідкової інформації - всі підсистеми автоматизованої системи правління повинні використовувати єдині метадані та нормативно-довідкову інформацію, забезпечувати можливість формування локальних довідників, підтримувати версійність метаданих та нормативно-довідкової інформації для забезпечення проведення аналізу з використанням даних за попередні часові періоди;

Крім того необхідно уніфікувати процеси взаємодії зі структурами і організаціями, що входять в контур управління безпекою в частині єдиної інформаційно-комунікаційної системи і форматів даних.

Архітектура ЦКБ ОЯЕ повинна забезпечувати можливість поетапної розробки і впровадження. Наслідком цього є можливість практично необмеженого розширення функціонального доповнення центру без принципової заміни системно-технічної платформи, що забезпечить відкритість і еволюційність системи;

В умовах зростання потоків даних, кількості робочих місць і кількості завдань без істотної зміни прикладного програмного забезпечення необхідно забезпечити можливість роботи ЦКБ ОЯЕ шляхом його масштабованості.

Принцип модульності передбачає побудову центру як сукупності модулів реалізації окремих функцій і завдань, що забезпечує гнучкість формування функціональності окремих автоматизованих робочих місць, підсистем і системи в цілому під необхідну структуру і механізми управління безпекою;

Крім того, одним із основних принципів побудови ЦКБ ОЯЕ є його живучість - система повинна мати властивість живучості, забезпечувати безперебійну роботу, отримання достовірних результатів і захист від несанкціонованих дій.

Для забезпечення створення і функціонування ЦКБ ОЯЕ необхідно базуючись на основних положеннях існуючого міжнародного правового поля в області кібербезпеки, розробити систему нормативних документів, які передбачають для об'єктів ядерної енергетики, правила з кібербезпеки, засновані на загальних нормах кібербезпеки і експлуатаційної сумісності; підготувати проекти нормативно-правових документів, необхідних для забезпечення ефективної діяльності в галузі забезпечення кібербезпеки в тому числі на основі технологій зв'язку, спостережень і інформування; проводити узгоджену політику інформованості та керованості в області забезпечення кібербезпеки ОЯЕ.

ОРГАНІЗАЦІЙНО-ТЕХНІЧНА МОДЕЛЬ СИСТЕМИ УПРАВЛІННЯ

На основі базових принципів розробки та функціонування ЦКБ ОЯЕ створена структурна схема схема центру кібербезпеки ОЯЕ, представлена на рис.3.

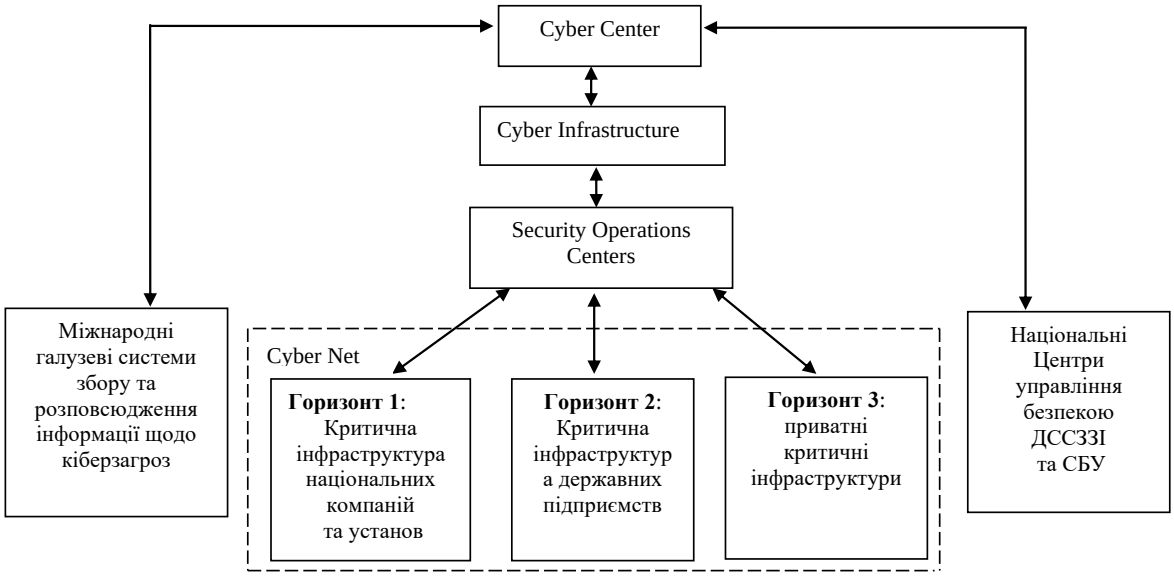

Рис.3. Структурна схема центру кібербезпеки ОЯЕ

Об'єктами кібербезпеки є об'єкти ядерної енергертики, об'єктами кіберзахисту: комунікаційна або технологічна система об'єкта критичної інфраструктури, кібератака на яку безпосередньо вплине на стале функціонування такого об'єкта критичної інфраструктури.

Модель взаємодії складається із двох зон та відповідної взаємодії між ними:

1) Кібер-центр (CyberCenter) – це централізована зона, де відбувається узгоджена концентрація (агрегація) визначеної інформації та сервісів. Така концентрація відбувається завдяки засобам моніторингу та детекції кіберпростору з метою подальшого використання для оперативного, систематичного та планового попередження учасників системи про кіберзагрози. Відповідно до функцій CyberCenter управляється одним центральним (або декількома) суб'єктом системи. CyberCenter забезпечує функціонування централізованих кіберсервісів, таких як: захист від атак типу «відмова в обслуговуванні»; захист від дій шкідливих програм; захист web-додатків та web-сервісів; захист email-додатків та сервісів, а також моніториинг та оцінку поточного стану кіберпростору, виявлення невідомих загроз типу «0-дня», аналіз інцидентів.

2) Кібер-мережа (CyberNet) – це децентралізована зона, представлена галузевими установами-суб'єктами системи, тобто користувачами інформаційних систем, телекомунікаційних мереж, комп'ютерної техніки тощо, - загалом будь-яких засобів, де використовуються інформаційно-телекомунікаційні технології для зберігання, модифікації та обміну даними. Суб'єкт CyberNet є постачальником визначеної інформації про події у власному кіберпросторі до CyberCenter через пристрої безпеки. Пристроями безпеки на стороні суб'єкту CyberNet є телекомунікаційне обладнання (комутатори, маршрутизатори тощо), засоби мережевої безпеки (міжмережеві екрани, системи захисту від атак, антивіруси), кінцеві пристрої користувачів, віртуальні та апаратні засоби аналізу трафіка, спеціалізовані прилади/пристрої/датчики тощо критичної інформаційної інфраструктури, включаючи телеметрію тощо. Через власні пристрої безпеки суб'єкт CyberNet виконує функції кіберзахисту власної інфраструктури, інформаційних систем тощо, а саме: збір

інформації про поточний стан функціонування пристроїв користувачів, виявлення аномалій на рівні мережевих взаємодій, моніторинг мереж та інцидентів безпеки, протидія та блокування

Організаційна, технологічна та інформаційна взаємодія обох зазначених зон (CyberCenter, CyberNet) є ключовою умовою функціонування централізованої системи управління кібербезпекою інфраструктури (CyberInfrastructure, скорочено – iCyber) у цілому та запорукою реалізації заходів попередження, управління та усунення кіберзагроз. Обмін інформацією про події у кіберпросторі є ключовим чинником попередження усіх субєктів про кіберзагрози, а технологічна взаємодія створює умови захисту кожного суб'єкту та забезпечує функціонування системи у цілому.

МАСШТАБУВАННЯ СИСТЕМИ УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ТА ЇЇ ГОЛОВНІ ФУНКЦІЇ

Масштабування iCyber здійснюється за рахунок поступового та спланованого збільшення кількості суб'єктів зони CyberNet, їх підключення до CyberCenter, та налагодження взаємодії. Для управління цим процесом CyberNet розподіляється на логічні горизонти (рис.4.), що виходять, насамперед, із організаційної структури галузі та специфіки управління. Першим горизонтом взаємодії є державні органи влади, що підпорядковані галузевим об'єктам критичної інфраструктури. Другим горизонтом є критична інфраструктура державних підприємств. Третім горизонтом є приватні критичні інфраструктури, котрі взаємодіють із другим та першим горизонтом через відповідні електронні комунікації тощо. Кожен горизонт CyberNet, а в деяких випадках його окремий суб'єкт, має власну специфіку підключення та порядок взаємодії із CyberCenter.

CyberCenter як центральний агрегатор інформації та центральна ланка Системи Кібербезпеки здійснює в межах визначених процедур взаємодію із міжнародними галузевими системами збору та розповсюдження аналітичної та статистичної інформації щодо кіберзагроз (системи кібераналітики). Співпраця із глобальними системами кібербезпеки надає значних переваг, насамперед, у випадках здійснення кібератак з-за кордону, коли їх швидке розпізнавання може бути ускладнене, а протидія лише локальними «силами» може виявитися не завжди ефективною.

Ключовою ланкою взаємодії є інформаційно-технічна взаємодія Системи Кібербезпеки зі створеними національними Центрами управління безпекою ДССЗЗІ та СБУ (специфіка обміну та даних встановлюється відповідними протоколами взаємодії).

Управління горизонтами CyberNet здійснюється через Галузеві центри управління кібербезпекою (Security Operations Centers), котрі створюються відповідно до специфіки галузі (наприклад для паливно-енергетичного комплексу України це ДП "Національна енергетична компанія «Укренерго», ДП "Національна атомна енергогенеруюча компанія "Енергоатом", Національна акціонерна компанія "Нафтогаз України", вугільна промисловість).

Система управління інформаційною безпекою (СУІБ) – частина загальної системи управління, заснована на використанні методів оцінки бізнес-ризиків для розробки, впровадження, функціонування, моніторингу, аналізу, підтримки та поліпшення інформаційної безпеки.

Система управління повинна включати в себе організаційну структуру, політику, діяльність із планування, розподіл відповідальності, практичну діяльність, процедури, процеси і ресурси.

На даний момент стандартом, який визначає вимоги до побудови СУІБ є ISO / IEC 27001-2013. Стандарт ISO 27001 спрямований на впровадження процесів, що дозволяють забезпечити належний рівень інформаційної безпеки системи. СУІБ базується на процедурі оцінки та аналізу ризиків, інтегральних показників захищеності ключових інформаційних активів і виборі заходів щодо мінімізації ризиків до прийнятного залишкового рівня.

Проведення комплексу заходів із побудови системи управління інформаційною безпекою відповідно до вимог стандарту ISO 27001 дозволить вирішити завдання підвищення рівня безпеки, управління (побудову циклічного і керованого процесу забезпечення інформаційної безпеки), оптимізації витрат на інформаційну безпеку, зниження рівня фінансових ризиків, пов'язаних з інформаційною безпекою, шляхом їх ідентифікації, оцінки та прийняття адекватних захисних заходів.

Система управління кібербезпекою завдяки функціонуванню та організаційно-технічній співпраці двох зон (CyberCenter, CyberNet) забезпечує виконання головних функцій безпеки та захисту кіберпростору галузі, а саме: ідентифікація (визначення користувачів та ресурсів, оцінки ризиків, оцінки вразливостей), захист (заходи контролю доступу, захисту даних, опис процесів та процедур, захисту від атак, технічної підтримки, тренування персоналу), виявлення (виявлення аномалій, моніторингу та виявлення інцидентів безпеки, побудови процесу детектування та обміну інформацією), реагування (аналіз інцидентів безпеки, протидія та блокування засобами захисту), відновлення (відновлення після кібератаки та забезпечення відповідного розслідування).

CyberCenter виконує функції централізованого моніторингу та детектування мережевих аномалій; централізованогопопередження атак нового покоління; централізованого детектування та аналізу шкідливого коду; управління центральним шлюзом захисту електронної пошти; інші додаткові централізовані функції.

До інших додаткових централізованих функцій відносяться системи забезпечення спостережності подій та інцидентів безпеки, а також активного попередження складних цільових атак.

CyberNet виконує функції технічної взаємодія із CyberCenter; захисту підключення до мережі Інтернет за допомоги наявних засобів міжмережевого екранування, у відповідності до стандартів "Довіреного Інтернет-підключення"; автономне детектування та протидію атакам існуючими засобами; захист публічних інформаційних ресурсів, що розташовані на рівні CyberNet; захист внутрішньої корпоративної мережі, контроль доступу до неї; антивірусний захист; моніторинг та контроль існуючих засобів захисту.

Суб'єкт CyberNet – державна установа, підприємство, організація - самостійно визначає рівень захисту власної IT-інфраструктури, покладаючись на власну відповідальність та користуючись існуючими нормативними документами, рекомендаціями експертів, виробників, фахівців національних та галузевих SOC-ів, CERT-ів (за наявності).

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Таким чином створення центру кібербезпеки ОЯЕ повинно підняти на якісно новий рівень стан інформаційної та функціональної безпеки підприємств галузі. Функціонування центру дозволить координувати та контролювати виконання заходів щодо розгортання системи інформаційної безпеки для критичних об'єктів інформаційної

інфраструктури на об'єктах ядерної енергетики. Крім того, він також дасть змогу запобігти втручанню в інформаційні системи шляхом обміну інформацією та функціонування централізованих та децентралізованих технологічних систем та організаційних ініціатив. Це зменшить наявні вразливі місця, зменшить можливість появи нових та ефективно їх ідентифікує при виникненні відповідних загроз. Центр захищатиме від усього спектру загроз, працюючи зі спеціалізованими службами у віртуальному середовищі, стимулюючи та проводячи навчання з інформаційної безпеки серед фахівців; здійснюватиме моніторинг та впровадження стандартів інформаційної безпеки суб'єктами критичної інфраструктури об'єктів ядерної енергетики; розроблятиме та впроваджуватиме нові заходи безпеки для зменшення ризику інформапційних та кіберзагроз, які постійно та швидко змінюються та розвиваються.

Продовженням досліджень у напрямку реалізації методичних засад створення та функціонування ЦКБ ОЯЕ є розробка архітектури системи, визначення системних характеристіик центру: структурної та системної складності, ефективності, надійності тощо.

ПОДЯКА

Автори виражають подяку ДСП «Чернобильська АЕС» за надану можливість презентації основних положень щодо створення ЦКБ ОЯЕ, слушні зауваження та пропозиції.

Робота виконана в рамках програми НАТО «Science for Peace», проект «Cyber Rapid Analysis for Defense Awareness of Real-Time Situation- CyRADARS» (grant agreement G5286).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Носовський, А. В. (2021). Науково-технічний супровід робіт з подолання наслідків чорнобильської катастрофи. *Вісник Національної академії наук України*, (7), 32–36.
2. *Проведение оценок компьютерной безопасности на ядерных установках.* (2018). Международное агентство по атомной энергии.
3. Park, J. K., Suh, Y. S., & Park, C. (2016). Implementation of cyber security for safety systems of nuclear facilities. *Progress in Nuclear Energy*, *88*, 88–94.
4. Poresky, C., Andreades, C., Kendrick, J., & Peterson, P. (2017). *Cyber Security in Nuclear Power Plants: Insights for Advanced Nuclear Technologies.* (UCBTH-17-001). CA.
5. Berg, H.-P. (2017). Cybersecurity of critical infrastructures such as nuclear facilities. *ENERGETIKA*, *63*(4), 141–145.
6. Погосов, О. Ю., & Дерев'янко, О. В. (2017). Фізичний захист АЕС та інформаційна безпека як необхідні умови зниження ризиків ядерних і радіаційних аварій. *Ядерна та радіаційна безпека*, *3*(75), 50–55.
7. Чумак, Д. В., & Клевцов, О. Л. (2015). Комп'ютерна безпека на ядерних об'єктах в Україні: області взаємодії між ядерною безпекою та захищеністю. *Ядерна та радіаційна безпека*, *3*(67), 60–64. Chumak, D. V., & Klevtsov, O. L. (2015).
8. Shkarlet, S., Lytvynov, V., Dorosh, M., Trunova, E., & Voitsekhovska, M. (2019). The Model of Information Security Culture Level Estimation of Organization. *Advances in Intelligent Systems and Computing*, *1019*, 249–258.
9. Литвинов, В. В., Казимир, В. В., Стеценко, І. В., Трунова, О. В., & Скітер, І. С. (2017). *Методи аналізу та моделювання безпеки розподілених інформаційних систем.* Національний технологічний університет.

10. Литвинов, В. В., Стоянов, Н., Скітер, І. С., Трунова, О. В., & Гребенник, А. Г. (2018). Захист корпоративних мереж від атак з використанням контент-аналізу глобального інформаційного простору. *Технічні науки та технології, 1*(11), 115–130.
11. *Computer security at nuclear facilities : reference manual : technical guidance.* (2011). International Atomic Energy Agency.
12. International Electrotechnical Commission. (2009). *Nuclear power plants — Instrumentation and control important to safety — Classification of instrumentation and control functions.* (IEC 61226.).
13. International Electrotechnical Commission. (2014). *Nuclear power plants — Instrumentation and control systems — Requirements for security programmes for computerbased system.* (IEC 62645).
14. *Cyber Security in the Energy Sector. Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector* (E03341). (2017). Energy Expert Cyber Security Platform (EECSP).
15. Технічний комітет зі стандартизації «Інформаційні технології» (ТК 20) при Держ-споживстандарті України та Міжнародний науково-навчальний цен. (2004). *Інформаційні технології. Настанови з керування безпекою інформаційних технологій (IT). Частина 2. Керування та планування безпеки IT (41033)* (ДСТУ ISO . ДСТУ ISO/TR 13335-2:2003). ДП «УкрНДНЦ».
16. Технічний комітет стандартизації «Інформаційні технології» (ТК 20) за участю Технічного комітету стандартизації «Банківські та фінансові сис. (2016). *Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги* (ДСТУ ISO/IEC 27001:2015). ДП «УкрНДНЦ».
17. Технічний комітет стандартизації «Інформаційні технології» (ТК 20). (2014). *Інформаційні технології. Методи безпеки. Системи менеджменту інформаційною безпекою. Вимоги* (17. ДСТУ ISO/IEC 27001:2013). ДП «УкрНДНЦ».
18. Turner, P. L., Adams, S. S., & Hendrickson, S. M. (2017). Enhancing Power Plant Safety through Simulated Cyber Events. Submitted to the American Nuclear Society's. У *10th International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human Machine Interface Technologies* (с. 301–313). American Nuclear Society (ANS).
19. *Program on Technology Innovation: Analysis of Hazard Models for Cyber Security, Phase I* (000000003002004995). (2015). EPRI.
20. *Program on Technology Innovation: Cyber Hazards Analysis Risk Methodology, Phase II: A Risk Informed Approach.* (000000003002004997). (2015). EPRI.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (12), 2021
ISSN 2663 - 4023

Henadiy Hulak
Doctor of Technical Sciences, Associate Professor,
Head of Cybersecurity Research Laboratory,
The Institute of Mathematical Machines and Systems Problems of the
Ukraine National Academy of Science, Kyiv, Ukraine
ORCID ID 0000-0001-9131-9233
eh.hulak@ukr.net

Ihor Skiter
PhD in Physical and Mathematical Sciences, Associate Professor, Senior Researcher
National Academy of Science of Ukraine
The Institute for Safety Problems of Nuclear Power Plants, Chornobyl, Ukraine
ORCID ID 0000-0003-2334-2276
i.skiter@ispnpp.kiev.uarname

Yevhen Hulak
Information Security Manager
DTEK SERVICE LLC, Kyiv, Ukraine
ORCID ID 0000-0003-4984-686X
geg180579@gmail.com

METHODOLOGICAL PRINCIPLES OF ESTABLISHMENT AND FUNCTIONING OF THE CYBER SECURITY CENTER OF INFORMATION INFRASTRUCTURE OF NUCLEAR ENERGY FACILITIES

Abstract. Nuclear power facilities (UAEs) are complex structural systems that operate large arrays of information flows, the distortion or blocking of which can potentially lead to inadequate and even catastrophic situations. Constant continuous automated control of the technical means of these objects is the key to ensuring the safety of man, society and the state. Therefore, ensuring the warranty of automated systems of the UAE as a technological basis for their functioning is a priority task of scientific research and development in this field. In the world's growing number and capacity of cyber attacks on critical information systems, long-standing confrontation of the state with hybrid war of limited financial resources, coordination and concentration of efforts to ensure cybersecurity of the UAE is the only way to solve certain problems in the industry. The purpose of such events should be to build a single cybersecurity center of the UIA. The creation of such a center should raise the state of information and functional security of enterprises of the industry to a qualitatively new level. The main tasks of the center are: ensuring the implementation of components of the organizational and technical model of information protection and cyber security; establishing mandatory information security requirements for critical information infrastructure objects taking into account international standards and industry specifics, including relevant critical information infrastructure facilities; monitoring of information security and information security at nuclear power facilities; countering cyber threats by raising general situational awareness of incidents and vulnerabilities among industry institutions and their critical infrastructure; preventing intrusion by sharing information and organizing initiatives; reducing vulnerabilities, preventing threats and their effective localization; monitoring of counteraction to threats at nuclear power facilities; stimulating and conducting training and raising the level of information awareness in terms of cybersecurity among critical infrastructure managers, appropriate testing, research and development. The functioning of the center will allow to coordinate and monitor the implementation of measures to deploy the information security system for critical information infrastructure facilities at nuclear power facilities. In addition, it will also prevent interference in information systems by exchanging information and functioning of centralized and decentralized technological systems and organizational initiatives. This will reduce the available vulnerabilities, reduce the possibility of new ones and effectively identify them when there are appropriate threats. The Center will protect against the whole range of threats, working with specialized services in a virtual environment, encouraging and conducting training on information security among specialists; will monitor and implement information security standards by subjects of critical infrastructure of nuclear power facilities; will

develop and implement new security measures to reduce the risk of information and cyber threats, which are constantly changing and developing rapidly.

Keywords: information security center; nuclear power facilities; model of cybersecurity management system; critical infrastructure; countering cyber threats.

REFERENCES

1. Nosovsky, A.V. (2021). Naukovo-tekhnichnyi suprovid robit z podolannia naslidkiv chornobylskoi katastrofy. [Scientific and technical support of work to overcome the consequences of the Chernobyl disaster]. Bulletin of the National Academy of Sciences of Ukraine, (7), 32–36. Nosovskyi, A. V. (2021). *Visnyk Natsionalnoi akademii nauk Ukrainy - Bulletin of the National Academy of Sciences of Ukraine, (7), 32–36* [In Ukraine]
2. *Provedenye otsenok kompiuternoi bezopasnosty na yadernikh ustanovkakh.* [Conducting computer security assessments at nuclear facilities.] (2018). Mezhdunarodnoe ahentstvo po atomnoi enerhyy - International Atomic Energy Agency.
3. Park, J. K., Suh, Y. S., & Park, C. (2016). Implementation of cyber security for safety systems of nuclear facilities. *Progress in Nuclear Energy*, *88*, 88–94.
4. Poresky, C., Andreades, C., Kendrick, J., & Peterson, P. (2017). *Cyber Security in Nuclear Power Plants: Insights for Advanced Nuclear Technologies.* (UCBTH-17-001). CA.
5. Berg, H.-P. (2017). Cybersecurity of critical infrastructures such as nuclear facilities. *ENERGETIKA*, *63*(4), 141–145.
6. Pohosov, O. Yu., & Derevianko, O. V. (2017). Fizychnyi zakhyst AES ta informatsiina bezpeka yak neobkhidni umovy znyzhennia ryzykiv yadernykh i radiatsiinykh avarii. [Physical protection of NPPs and information security as necessary conditions for reducing the risks of nuclear and radiation accidents]. *Yaderna ta radiatsiina bezpeka - Nuclear and radiation safety*, 3(75), 50–55 [In Ukraine]
7. Chumak, D. V., & Klevtsov, O. L. (2015). Komp‘iuterna bezpeka na yadernykh obiektakh v Ukraini: oblasti vzaiemodii mizh yadernoiu bezpekoiu ta zakhyshchenistiu. [Computer security at nuclear facilities in Ukraine: areas of interaction between nuclear safety and security] *Yaderna ta radiatsiina bezpeka - Nuclear and radiation safety*, 3(67), 60–64. [In Ukraine]
8. Shkarlet, S., Lytvynov, V., Dorosh, M., Trunova, E., & Voitsekhovska, M. (2019). The Model of Information Security Culture Level Estimation of Organization. *Advances in Intelligent Systems and Computing*, *1019*, 249–258.
9. Lytvynov, V. V., Kazymyr, V. V., Stetsenko, I. V., Trunova, O. V., & Skiter, I. S. (2017). *Metody analizu ta modeliuvannia bezpeky rozpodilenykh informatsiinykh system* [Methods of analysis and modeling of security of distributed information systems]. Natsionalnyi tekhnolohichnyi universytet. [In Ukraine]
10. Lytvynov, V. V., Stoianov, N., Skiter, I. S., Trunova, O. V., & Hrebennyk, A. H. (2018). Zakhyst korporatyvnykh merezh vid atak z vykorystanniam kontent-analizu hlobalnoho informatsiinoho prostoru. [Protection of corporate networks from attacks using content analysis of the global information space]. *Tekhnichni nauky ta tekhnolohii - Technical sciences and technologies*,1(11), 115–130. [In Ukraine]
11. *Computer security at nuclear facilities : reference manual : technical guidance.* (2011). International Atomic Energy Agency.
12. International Electrotechnical Commission. (2009). *Nuclear power plants — Instrumentation and control important to safety — Classification of instrumentation and control functions.* (IEC 61226.).
13. International Electrotechnical Commission. (2014). *Nuclear power plants — Instrumentation and control systems — Requirements for security programmes for computerbased system.* (IEC 62645).
14. *Cyber Security in the Energy Sector. Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector* (E03341). (2017). Energy Expert Cyber Security Platform (EECSP).
15. Technical Committee for Standardization "Information Technology" (TC 20) at Derzhspozhyvstandart of Ukraine and the International Research and Training Center (2004). Informatsiini tekhnolohii. *Nastanovy z keruvannia bezpekoiu informatsiinykh tekhnolohii (IT). Chastyna 2. Keruvannia ta planuvannia bezpeky IT* [nformation Technology. Information Technology (IT) Security Management Guidelines. Part 2. IT security management and planning] (41033) (DSTU ISO . DSTU ISO/TR 13335-2:2003). DP «UkrNDNTs».

16. Technical Committee for Standardization "Information Technology" (TC 20) with the participation of the Technical Committee for Standardization "Banking and Financial Systems". (2016). *Informatsiini tekhnolohii. Metody zakhystu. Systemy upravlinnia informatsiinoiu bezpekoiu. Vymohy* [Information Technology. Methods of protection. Information security management systems. Requirements] (DSTU ISO/IEC 27001:2015). DP «UkrNDNTs».
17. Technical Committee for Standardization "Information Technology" (TC 20). (2014). *Informatsiini tekhnolohii. Metody bezpeky. Systemy menedzhmentu informatsiinoiu bezpekoiu. Vymohy* [Information Technology. Security methods. Information security management systems. Requirements] (17. DSTU ISO/IEC 27001:2013). DP «UkrNDNTs».
18. Turner, P. L., Adams, S. S., & Hendrickson, S. M. (2017). Enhancing Power Plant Safety through Simulated Cyber Events. Submitted to the American Nuclear Society's. У *10th International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human Machine Interface Technologies* (с. 301–313). American Nuclear Society (ANS).
19. *Program on Technology Innovation: Analysis of Hazard Models for Cyber Security, Phase I* (000000003002004995). (2015). EPRI.
20. *Program on Technology Innovation: Cyber Hazards Analysis Risk Methodology, Phase II: A Risk Informed Approach.* (000000003002004997). (2015). EPRI.