УДК. 621.039:004.09

Д. В. Чумак, О. Л. Клевцов

Державний науково-технічний центр з ядерної та радіаційної безпеки, м. Київ, Україна

Комп‘ютерна безпека на ядерних об’єктах в Україні: області взаємодії між ядерною безпекою та захищеністю

Розглянуто проблематику комп’ютерної та інформаційної безпеки у площині фізичного захисту, а також нормативно-правове забезпечення комп’ютерної безпеки на ядерних об’єктах в Україні. 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.

Ключові слова: АЕС, комп’ютерна безпека, інформаційна безпека, ядерна безпека, захищеність, фізичний захист, інформаційні та керуючі системи, кібернетичні атаки.

Д. В. Чумак, А. Л. Клевцов

Компьютерная безопасность на ядерных объектах в Украине: области взаимодействия между ядерной безопасностью и защищенностью

Рассматрены проблематика компьютерной и информационной безопасности в плоскости физической защиты, а также нормативно-правовое обеспечение компьютерной безопасности на ядерных объектах в Украине. Основной акцент сделан на компьютерной безопасности информационных и управляющих систем (ИУС), важных для ядерной безопасности. Приведен пример интегрированного подхода к рассмотрению требований к ядерной безопасности и защищенности с учетом взаимодействия сфер обеспечения защищенности ИУС и ядерной безопасности. Представлены рекомендации и планы на будущее по совершенствованию компьютерной безопасности на ядерных объектах в Украине.

Ключевые слова: АЭС, компьютерная безопасность, информационная безопасность, ядерная безопасность, защищенность, физическая защита, информационные и управляющие системы, кибернетические атаки.

Активний процес комп’ютеризації та інформатизації атомної галузі зумовлює потребу в підвищенні рівня комп’ютерної безпеки на ядерних об’єктах. Міжнародна спільнота неодноразово висловлювала серйозну занепокоєність щодо вразливості до кібернетичних загроз ядерних та радіоактивних матеріалів, а також відповідних установок. Міжнародне агентство з атомної енергії (МАГАТЕ) відмічає, що досвід, отриманий від дії вірусу «Стакснет», продемонстрував реальну небезпеку кібератак для ядерних об’єктів, та наголошує, що подібні події негативно впливають на рівень ядерної безпеки та захищеності.

Із збільшенням частки виробітку електроенергії атомними енергоблоками в Україні, комп’ютерна безпека на ядерних об’єктах в Україні потребує додаткових заходів щодо її посилення, про що свідчать такі фактори:

підвищення загрози використання кіберпростору з метою проведення терористичних атак на ядерні об’єкти, зокрема у зв’язку з ситуацією на сході країни;

активне застосування на ядерних установках комп’ютерних інформаційних та керуючих систем (ІКС) в управлінні технологічними процесами або їх контролі, потенційна вразливість ядерних установок до кібернетичних загроз;

потенційна небезпека несанкціонованого викрадення, знищення або спотворення важливої інформації через комп’ютерні мережі, що може призвести до негативних наслідків для ядерного об’єкта;

підвищення загрози з боку внутрішніх правопорушників;

негативна світова тенденція збільшення випадків несанкціонованого доступу до елементів критичної інфраструктури, зокрема до об’єктів атомної енергетики.

Основні терміни. Наразі в Україні розпочато розробку єдиного підходу до визначень ключових термінів кібернетичної тематики, що потребує внесення змін до відповідних законів з цього напряму. В українському законодавстві *інформаційна безпека* визначається як стан захищеності життєво важливих інтересів людини, суспільства і держави, за котрого відвертається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання й порушення цілісності, конфіденційності та доступності інформації [1]. Але, враховуючи основний фокус статті на ядерній тематиці, користуватимемося довідковим керівництвом МАГАТЕ щодо комп’ютерної безпеки на ядерних установках № 17 (NSS 17) [2], за яким *інформаційна безпека* (*information security*) — збереження конфіденційності, цілісності та доступності інформації; *комп’ютерна безпека* (*computer security*) — специфічний аспект інформаційної безпеки, який стосується комп’ютерних систем, мереж і цифрових систем.

Зауважимо, що в Україні нормативно-правова база з комп’ютерної безпеки, особливо в ядерній сфері, потребує подальшого розвитку на відміну від бази з інформаційної безпеки, яка має належне нормативно-правове забезпечення. У статті більше уваги приділяється інформаційній безпеці та перспективам розвитку нормативно-правових аспектів забезпечення комп’ютерної безпеки на національних ядерних об’єктах.

Комп’ютерна безпека відіграє все важливішу роль у досягненні основних цілей *ядерної захищеності* (*nuclear security*), зокрема у запобіганні та виявленні викрадення, саботажу (диверсії), несанкціонованого доступу, незаконного

передавання або інших зловмисних дій відносно ядерних матеріалів, інших радіоактивних речовин або пов'язаних з ними установок, і реагуванні на такі дії [2]. У свою чергу, цілі комп'ютерної безпеки — це, зазвичай, захист характеристик конфіденційності, цілісності та доступності електронних даних або готовності комп'ютерних систем і процесів [2]. Таким чином, визначаючи та захищаючи відповідні дані або системи, які впливають на ядерну безпеку та захищеність на ядерних установках, можна підвищити безпеку експлуатації ядерних об'єктів.

Міжнародна спільнота визнає комп'ютерну та інформаційну безпеку як інтегровані частини захищеності. Зазначимо, що і в Україні існує подібний підхід. Оскільки в Україні захищеність ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання визначена як відповідність рівня фізичного захисту ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання законодавству [3], у цій статті питання забезпечення комп'ютерної та інформаційної безпеки розглядається в площині фізичного захисту. Акцент робиться на комп'ютерній безпеці ІКС, адже наразі на ядерних установках саме вони виконують основну роль в управлінні технологічними процесами або їх контролі. ІКС визначається як система, що призначена для ініціювання роботи однієї чи кількох інших систем або технологічного устаткування та/або для безпосереднього управління ними та/або для одержання, обробки, зберігання, відображення та/або реєстрації даних про технічний стан конструкцій, систем, елементів, їх властивості та/або функціонування.

Більшість сучасних ІКС — це комп'ютерні системи, а отже, вони потенційно уразливі до впливу кібернетичних загроз. Кібернетична атака на ІКС, важливу для ядерної безпеки, може негативно вплинути на реалізацію технологічних процесів і в кінцевому підсумку призвести до порушення безпеки ядерної установки. Оскільки забезпечення захищеності ІКС ядерних установок є задачею надзвичайно серйозною та пов'язаною з ядерною безпекою, вимоги до ядерної безпеки та захищеності доцільно розглядати в комплексі.

На ядерних установках система фізичного захисту та ІКС є автономними, тому деякі загрози, особливо ті, які несуть за собою Інтернет та локальні мережі, не становлять особливої небезпеки. Проте кібернетичні загрози, пов'язані з програмним та апаратним забезпеченням для систем фізичного захисту та ІКС, — загрози небезпечні, тому на них слід звертати увагу, розглядаючи проблематику комп'ютерної безпеки на ядерних об'єктах. Серед таких загроз потрібно виділити:

шкідливі закладки в програмному забезпеченні (ПЗ) власної розробки або в покупному ПЗ;

негативний вплив на ПЗ ІКС з боку засобів розробки ПЗ;

закладки в технічних засобах (hardware trojans);

внесення шкідливих програм або даних з портативних пристроїв або із зовнішніх носіїв даних у процесі експлуатації;

негативний вплив з боку контрольно-перевірочної апаратури;

шкідливі дії персоналу АЕС або сторонніх організацій;

некоректне оновлення ПЗ ІКС на АЕС.

Інформаційна безпека та комп'ютерна безпека як елементи національної безпеки. У Законі України «Про основи національної безпеки України» з-поміж основних загроз національним інтересам України в інформаційному секторі названо комп'ютерну злочинність та комп'ютерний тероризм, а також розголошення інформації, яка становить державну таємницю, або розголошення іншої інформації з обмеженим доступом.

Створення належної нормативної бази для протидії цим загрозам в Україні не завершено, але роботи в цьому напрямі проводяться. Минулого року Кабінетом Міністрів України ухвалено рішення про необхідність розробити та схвалити закон щодо комп'ютерної безпеки. Проект закону, після розгляду Кабінетом Міністрів України, перебуває на стадії доопрацювання. Урядом затверджено план захисту державної інформації і державних інформаційних ресурсів [4], у рамках якого реалізуються заходи щодо захисту від кібернетичних загроз. За планом, у 2015–2016 роках передбачається організувати та провести оцінку стану захищеності державних інформаційних ресурсів об'єктів, що належать до критичної інформаційної інфраструктури держави, і удосконалити законодавство з протидії правопорушенням проти державних інформаційних ресурсів та інформаційно-телекомунікаційних систем об'єктів критичної інформаційної інфраструктури держави [4]. Наразі в Україні захист критичної інфраструктури регламентується численними внутрішньовідомчими нормативно-правовими актами.

Серед основних законів, які формують національну політику щодо інформаційної безпеки, назвемо такі:

Закон України «Про інформацію» від 02.10.1992 № 2657-XII [5];

Закон України «Про державну таємницю» від 21.01.1994 № 3855-XII [6];

Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР [7];

Закон України «Про ратифікацію Конвенції про кіберзлочинність» від 07.09.2005 № 2824-IV [8].

У зв'язку з викликами національній безпеці через події на сході країни, прийнято рішення Ради національної безпеки і оборони України про проведення невідкладних заходів щодо забезпечення національної безпеки, суверенітету й територіальної цілісності України [9]. Відповідно до цього рішення, а саме пункту 6, Міністерству внутрішніх справ України наказано забезпечити посилену охорону об'єктів енергетики та критичної інфраструктури. Відповідно до Закону України «Про фізичний захист ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання» [3], Національна гвардія України забезпечує охорону та оборону всіх українських атомних електростанцій, Державного спеціалізованого підприємства «Чорнобильська АЕС» та об'єкта «Укриття», Інституту ядерних досліджень НАНУ, Національного наукового центру «Харківський фізико-технічний інститут» та ін.

Нормативно-правова база в частині захищеності інформаційних та керуючих систем, важливих для безпеки ядерних установок. У керівних матеріалах МАГАТЕ [2] наведено класифікацію загроз комп'ютерним системам на ядерних об'єктах в аспекті ядерної захищеності:

атаки для збору інформації, вчинені з метою планування та виконання подальших злочинних дій;

атаки, спрямовані на відімкнення або погіршення роботи одного або кількох комп'ютерів, критично важливих для фізичного захисту або безпеки установки;

порушення нормальної роботи одного або кількох комп'ютерів у поєднанні з іншими паралельними режимами атаки, такими як фізичне вторгнення в задані місця.

Ці загрози є серйозними ризиками для роботи ядерних установок, оскільки можуть бути використані зловмисниками, щоб приховати проникнення на ядерний об'єкт та вчинення протиправних дій. Тому для протидії цим загрозам на ядерних об'єктах повинен функціонувати відповідний комплекс заходів щодо забезпечення комп'ютерної безпеки у рамках фізичного захисту.

Оскільки комп'ютерна безпека та інформаційна безпека є складовими елементами ядерної захищеності, заходи з реалізації цілей комп'ютерної та інформаційної безпеки, головним чином, відображені в тій частині ядерного законодавства України, що стосується фізичного захисту.

В Україні основою фізичного захисту є Закон України «Про фізичний захист ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання» [3]. У цьому законі встановлено першочергові вимоги та завдання фізичного захисту, одним з яких, зокрема, є організація роботи з обміну інформацією про стан фізичного захисту та її збереження, а також зазначено про необхідність створення умов для захисту інформації з обмеженим доступом. Категоризацію такої інформації наведено в Законі України «Про доступ до публічної інформації» [10]. У документі [11] визначено, що інформація про систему фізичного захисту ядерних установок, ядерних матеріалів, об'єктів поводження з радіоактивними відходами, іншими джерелами іонізуючого випромінювання є державною таємницею. Перевірка порядку забезпечення захисту інформації щодо фізичного захисту об'єктів, доступ до якої обмежується, здійснюється в рамках постанови Кабінету Міністрів України № 327 [12].

Чинні в Україні нормативно-правові документи насамперед спрямовані на забезпечення інформаційної безпеки. Щодо норм, правил та стандартів, які б регламентували вимоги безпосередньо до комп'ютерної безпеки ядерних установок, то на даний час в Україні вони відсутні. Проте в 2015 році передбачено введення в дію нового нормативного документа «Вимоги з ядерної та радіаційної безпеки до інформаційних і керуючих систем, важливих для безпеки атомних станцій», який розроблено за безпосередньої участі фахівців ДНТЦ ЯРБ. У ньому запропоновано подвійну класифікацію ІКС та їх елементів (технічних засобів і програмного забезпечення) з метою гармонізації класифікації систем та елементів АЕС, наведеній у НП 306.2.141 [13], — базовому нормативному документі України з безпеки АЕС, з класифікацією функцій за міжнародними стандартами.

Згідно з НП 306.2.141 [13], ІКС АЕС можуть належати до одного з трьох класів безпеки:

класу 2* — елементи, відмови яких є вихідними подіями, що за умов проектного функціонування систем безпеки та з урахуванням кількості відмов, що нормуються в цих системах для проектних аварій, призводять до пошкодження тепловидільних елементів у межах, установлених для проектних аварій, або елементи систем безпеки, відмови яких призводять до невиконання цими системами своїх функцій;

класу 3 — елементи систем, важливих для безпеки, що не ввійшли до класів 1 і 2, або елементи, що виконують функції радіаційного захисту персоналу й населення;

клас 4 — елементи нормальної експлуатації АС, що не впливають на безпеку і які не ввійшли до класів 1, 2, 3.

У документі «Вимоги з ядерної та радіаційної безпеки до інформаційних і керуючих систем, важливих для безпеки атомних станцій» введено категоризацію функцій ІКС АЕС. За аналогією до стандарту МЕК 61226 [14], функції ІКС класифікуються за категоріями А, В, С залежно від їх ролі в забезпеченні й підтримці безпеки, а також залежно від можливих наслідків, спричинених невиконанням або помилковим виконанням функції, а всі ІКС поділено на важливі для безпеки й такі, що не впливають на безпеку.

Важливими для безпеки є ІКС, які виконують хоча б одну з функцій, віднесених до категорії А, В або С. Інші ІКС відносять до таких, що не впливають на безпеку.

Кожна ІКС, важлива для безпеки, належить до одного з трьох класів безпеки, які позначаються сполученням цифри, зазначеної в НП 306.2.141 [133], і букви (у круглих дужках), яка вказує на найвищу з категорій функцій, виконуваних цією ІКС, а саме:

до класу безпеки 2(А), якщо серед цих функцій принаймні одна має категорію А;

до класу безпеки 3(В), якщо серед цих функцій відсутні функції категорії А, але принаймні одна з них має категорію В;

до класу безпеки 3(С), якщо серед цих функцій відсутні функції категорії А і В, але принаймні одна з них має категорію С.

ІКС належить до класу 4, якщо жодна з виконуваних нею функцій не класифікована за категоріями.

Документ «Вимоги з ядерної та радіаційної безпеки до інформаційних і керуючих систем, важливих для безпеки атомних станцій» регламентує, перш за все, вимоги з ядерної та радіаційної безпеки ІКС АЕС. Проте він також містить деякі вимоги, що стосуються фізичного захисту та комп'ютерної безпеки ІКС АЕС (рис. 1).

Рис. 1. Взаємодія між ядерною безпекою та фізичним захистом

Зокрема, в частині забезпечення фізичного захисту документ містить вимоги до захисту технічних засобів ІКС АЕС від несанкціонованого доступу. Згідно з цими вимогами, для запобігання можливості навмисного або ненавмисного виведення з роботи, втручання в роботу, псування або розкрадання, які можуть створити загрозу безпеці, передбачаються:

фізичний захист від несанкціонованого доступу всередину технічних засобів, до кабельних з'єднувачів, затискачів та інших елементів для зовнішніх підключень;

захист від несанкціонованої зміни програмного забезпечення, баз даних і архівів;

негайне сповіщення персоналу про будь-яку спробу несанкціонованого доступу до технічних засобів, програмного забезпечення, баз даних або архівів.

У проекті мають бути передбачені заходи захисту від несанкціонованого використання РЩУ, а оперативний персонал у приміщенні БЩУ негайно сповіщається про будь-яку подібну спробу.

* Зазначимо, що ІКС АЕС не належать (і не можуть належати) до класу безпеки 1.

Згідно з вимогами до комп'ютерної безпеки ІКС АЕС, регламентованими у документі «Вимоги з ядерної та радіаційної безпеки до інформаційних і керуючих систем, важливих для безпеки атомних станцій», програмне забезпечення, що бере участь у виконанні функцій категорій А, В і С, захищають від небажаного та небезпечного втручання в його роботу, а також від несанкціонованої зміни через зовнішні комп'ютерні мережі та/або в разі використання нерезидентних носіїв даних.

ПЗ, яке бере участь у виконанні функцій, що належать до категорії А, повністю ізолюють від взаємодії із зовнішніми комп'ютерними мережами.

ПЗ, яке бере участь у виконання функцій, що належать до категорій В і С, ізолюють від доступу до мережі Інтернет.

Будь-які зміни у ПЗ можуть вноситися тільки після відповідної авторизації; несанкціонована зміна програмного забезпечення вручну або з використанням зовнішніх носіїв даних має унеможливлюватися.

Має унеможливлюватися і негативний вплив вжитих заходів захисту від кібернетичних загроз на виконання програм та/або характеристик виконання функцій, які реалізуються програмними засобами або з використанням програмних засобів.

Вочевидь, ці вимоги до комп'ютерної безпеки ІКС АЕС носять загальний характер. Подальшим завданням (зокрема, для ДНТЦ ЯРБ) є розробка в Україні нормативного документа, який би містив детальні вимоги до комп'ютерної безпеки комп'ютерних систем ядерних установок з урахуванням документів МАГАТЕ (зокрема, NSS 17 [2]) та міжнародних стандартів (зокрема, МЕК 62645 [15]).

Зауважимо, що розглянуті вимоги до комп'ютерної безпеки ІКС АЕС дещо відрізняються від підходів, зазначених у [2] та [15]. Згідно з NSS 17 [2] та МЕК 62645 [15], жорсткість вимог з комп'ютерної безпеки не залежить ні від напряму, ні від категорій виконуваних ІКС функцій, ні від класу безпеки ІКС АЕС.

У NSS 17 [2] використовується класифікація ІКС за *рівнем* комп'ютерної безпеки (security level), а МЕК 62645 [15] введено ідентичну класифікацію за *ступенем* комп'ютерної безпеки (security degree*). Жорсткість вимог визначається залежно від відповідного рівня або ступеня компьютерної безпеки.

Зупинимося детальніше на класифікації, використаній у [15]. Градація рівнів захищеності системи з необхідним набором вимог відповідає максимальним наслідкам успішної кібернетичної атаки на цю систему з урахуванням ядерної безпеки та експлуатаційних характеристик АЕС. МЕК 62645 [15] визначає три ступеня комп'ютерної безпеки: S1, S2 та S3. Класифікація [15] стосується тільки ІКС АЕС та не розповсюджуються на інші комп'ютерні системи АЕС. Проте до вказаних ступенів комп'ютерної безпеки можуть бути віднесені не тільки ІКС, але й, наприклад, системи управління фізичним захистом. Крім того, кількість ступенів комп'ютерної безпеки може бути збільшена для встановлення вимог з комп'ютерної безпеки по відношенню до інших комп'ютерних систем, мереж та окремих комп'ютерів, що не беруть участь у реалізації технологічних процесів.

Оскільки стандарт МЕК 62645 [15] обмежується саме ІКС АЕС, запропоновано встановити певний зв'язок між ступенями комп'ютерної безпеки та категоріями функцій, виконуваних ІКС АЕС.

Ступені комп'ютерної безпеки визначаються для ІКС так:

ІКС, що виконують функції ядерної безпеки категорії А, — ступінь комп'ютерної безпеки S1;

ІКС, потрібні для роботи в режимі реального часу (без зазначення категорій ядерної безпеки), та ІКС, що виконують функції ядерної безпеки категорії В, — не нижче ступеня комп'ютерної безпеки S2;

ІКС, що виконують функції ядерної безпеки категорії С, — ступінь комп'ютерної безпеки S3 або вище, залежно від максимально шкідливих наслідків;

ІКС, що відповідають за експлуатацію та технічне обслуговування АЕС, — ступінь комп'ютерної безпеки S3.

Системі може бути призначено жорсткіший, ніж рекомендований, ступінь комп'ютерної безпеки, якщо максимальні наслідки шкідливої дії на будь-яку з виконуваних нею функцій вважаються еквівалентними до відповідних жорсткіших ступенів комп'ютерної безпеки.

Як бачимо, в стандарті МЕК 62645 [15] зроблено спробу встановити опосередкований зв'язок між ядерною безпекою та комп'ютерною безпекою. В Україні доцільно в процесі розробки нових нормативних документів, що містять детальні вимоги до комп'ютерної безпеки ІКС АЕС, застосовувати аналогічний підхід до класифікації ІКС АЕС з комп'ютерної безпеки, використовуючи ступені комп'ютерної безпеки та враховуючи категорії виконуваних ними функцій.

Висновки

Проаналізувавши проблематику комп'ютерної безпеки в Україні, зокрема на ядерних об'єктах, потрібно наголосити на необхідності пріоритетного розвитку нормативно-правового регулювання в цій галузі. На відміну від інформаційної безпеки, рівень якої в Україні достатньо високий, комп'ютерна безпека (особливо в ядерній галузі) потребує додаткової уваги.

Наявні документи з комп'ютерної безпеки на ядерних об'єктах не охоплюють усіх аспектів проблематики та містять загальні вимоги. Подальшим завданням є розробка в Україні нормативних документів з детальними вимогами до комп'ютерної безпеки ІКС АЕС та інших комп'ютерних систем ядерних установок. Для створення належного регулятивного контролю за комп'ютерною безпекою АЕС в Україні доцільно використовувати міжнародні документи.

ДНТЦ ЯРБ наразі проводить відповідні дослідження для створення національних стандартів комп'ютерної безпеки АЕС та відповідних комп'ютерних систем. Розробляючи ці стандарти, вимоги до комп'ютерної безпеки ядерних установок доцільно розглядати в комплексі з вимогами до ядерної безпеки.

Список використаних джерел

1. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007—2015 роки» від 09.01.2007 № 537-V // Відомості Верховної Ради України (ВВР). — 2007. — № 12. — Ст. 102.

2. Комп'ютерна безпека на ядерних установках : Довідкове керівництво : технічні керівні матеріали. — Відень : МАГАТЕ, 2011. — (IAEA nuclear security series, ISSN 1816−9317; No. 17; ISBN 978−92-0−120110-2).

* Терміни «security level» і «security degree» абсолютно ідентичні, але на даний час перевага надається терміну «security degree».

3. Закон України «Про фізичний захист ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання» // Відомості Верховної Ради України (ВВР). — 2001. — № 1. — Ст. 1.

4. Про затвердження плану заходів щодо захисту державних інформаційних ресурсів : Розпорядження Кабінету Міністрів України від 05.11.2014 № 1135-р // Урядовий кур'єр. — 2014. — № 228.

5. Закон України «Про інформацію» від 02.10.1992 № 2657-XII // Відомості Верховної Ради України (ВВР). — 1992. — № 48. — Ст. 650.

6. Закон України «Про державну таємницю» від 21.01.1994 № 3855-XII // Відомості Верховної Ради України (ВВР). — 1994. — № 16. — Ст. 93.

7. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР // Відомості Верховної Ради України (ВВР). — 1994. — № 31. — Ст. 286.

8. Закон України «Про ратифікацію Конвенції про кіберзлочинність» від 07.09.2005 № 2824-IV // Відомості Верховної Ради України (ВВР). — 2006. — № 5–6. — Ст. 71.

9. Про невідкладні заходи щодо забезпечення національної безпеки, суверенітету і територіальної цілісності України : Рішення Ради Національної безпеки і оборони України від 01.03.2014, введено в дію указом Президента України від 02.03.2014 № 189/2014 // Офіційний вісник України. — 2014. — № 19. — Стор. 31, ст. 593.

10. Закон України «Про доступ до публічної інформації» від 13.01.2011 № 2939-VI // Відомості Верховної Ради України (ВВР). — 2011. — № 32. — Ст. 314.

11. Звід відомостей, що становлять державну таємницю : Затверджено наказом Служби безпеки України від 01.03.2001 № 52 // Офіційний вісник України. — 2005. — № 34. — Стор. 172, ст. 2089. — Код акту 33414/2005.

12. Про затвердження Порядку проведення державної перевірки систем фізичного захисту ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання та планів взаємодії у разі вчинення актів ядерного тероризму : Постанова Кабінету Міністрів України від 12.03.2003 р. № 327 // Офіційний вісник України. — 2003. — № 11. — Стор. 506, ст. 490. — Код акту 24676/2003.

13. Загальні положення безпеки атомних станцій : НП 306.2.141–2008 // Офіційний вісник України. — 2008. — № 9. — Стор. 28, ст. 226. — Код акту 42114/2008.

14. *IEC 61226*. Nuclear power plants — Instrumentation and control important to safety — Classification of instrumentation and control functions. — Geneva : International Electrotechnical Commission, 2009. — 26 p.

15. *IEC 62645*. Nuclear power plants — Instrumentation and control systems — Requirements for security programmes for computer-based system. — Geneva : International Electrotechnical Commission, 2014. — ISBN 978–2-8322–1810-5.

References

1. Law of Ukraine "On Basic Principles for the Development of an Information–Oriented Society in Ukraine for 2007–2015" [Zakon Ukrainy "Pro osnovni zasady rozvytku informatsiinoho suspilstva v Ukraini na 2007–2025 roky] No. 537–V of 09 January 2007, Bulletin of the Verkhovna Rada of Ukraine (VVR), 2007, No. 12, Art. 102. (Ukr)

2. Computer Security at Nuclear Facilities: Reference Manual: Technical Guidance [Kompiuterna bezpeka na yadernykh ustanovkakh: Dovidkove kerivnytstvo: tekhnichni kerivni materialy], Vienna, International Atomic Energy Agency, 2011, (IAEA Nuclear Security Series, ISSN 1816–9317; No. 17), ISBN 978–92–0–120110–2.

3. Law of Ukraine "On Physical Protection of Nuclear Facilities, Nuclear Materials, Radioactive Waste and Other Radiation Sources" [Zakon Ukrainy "Pro fizychnyi zakhyst yadernykh ustanovok, yadernykh materialiv, radioaktyvnykh vidkhodiv, inshykh dzherel ionizuiuchoho vyprominiuvannia], Bulletin of the Verkhovna Rada of Ukraine (VVR), 2001, No. 1. Art. 1. (Ukr)

4. On Approving Action Plan on Protection of the State Information Resources: [Pro zatverdzhennia planu zakhodiv schodo zakhystu derzhavnykh informatsiinykh resursiv] Resolution of the Cabinet of Ministers of Ukraine No. 1135–r of 05 November 2014, Governmental Courier, 2014, No. 228. (Ukr)

5. Law of Ukraine "On Information" [Zakon Ukrainy "Pro informatsiiu], No. 2657–XII of 02 October 1992, Bulletin of the Verkhovna Rada of Ukraine (VVR), 1992, No. 48, Art. 650. (Ukr)

6. Law of Ukraine "On State Secret" [Zakon Ukrainy "Pro derzhavnu taiemnytsiu], No. 3855–XII of 21 January 1994, Bulletin of the Verkhovna Rada of Ukraine (VVR), 1994, No. 16, Art. 93. (Ukr)

7. Law of Ukraine "On Information Protection in Information and Telecommunication Systems" [Zakon Ukrainy "Pro zakhyst informatsii v informatsiino-telekomunikatsiinykh systemakh] No. 80/94–VR of 05 July 1994, Bulletin of the Verkhovna Rada of Ukraine (VVR), 1994, No. 31, Art. 286. (Ukr)

8. Law of Ukraine "On Ratification of the Convention on Cyber Crime" [Zakon Ukrainy "Pro ratyfikatsiiu Konventsii pro kiberzlochynnist"], No. 2824–IV of 07 September 2005, Bulletin of the Verkhovna Rada of Ukraine (VVR), 2006, No. 5–6, Art. 71. (Ukr)

9. On Urgent Measures to Ensure National Security, Sovereignty and Territorial Integrity of Ukraine [Pro nevidkladni zakhody schodo zabezpechennia natsionalnoi bezpeky, suvernitetu i terytorialnoi tzilisnosti Ukrainy], Decision of the National Security and Defense Council of Ukraine of 01 March 2014 put in force by President's Decree No. 189/2014 of 02 March 2014, Official Journal of Ukraine, 2014, No. 19, p. 31, Art. 593. (Ukr)

10. Law of Ukraine "On Access to Public Information" [Zakon Ukrainy "Pro dostup do publichnoi informatsii"], No. 2939–VI of 13 January 2011, Bulletin of the Verkhovna Rada of Ukraine (VVR), 2011, No. 32, Art. 314. (Ukr)

11. Summary of State Secret Information [Zvit vidomostei, scho stanovliat derzhavnu taiemnytsiu], Approved by Order of the Security Service of Ukraine No. 52 of 01 March 2001//Official Journal of Ukraine, 2005, No. 34, p. 172, Art. 2089. Act code 33414/2005. (Ukr)

12. On Approving the Procedure of the State Inspection of the Physical Protection Systems at Nuclear Facilities, Nuclear Materials, Radioactive Waste, Other Radiation Sources and Interaction Plans in Case of Nuclear Terrorism Acts [Pro zatverdhennia Poriadku provedennia derzhavnoi perevirky system fizychnoho zakhystu yadernykh ustanovok, yadernykh materialiv, radioaktyvnykh vitkhodiv, inshykh dzherel ionizuiuchoho vyprominiuvannia ta planiv vzaiemodiiu razi vchynennia aktiv yadernoho teroryzmu], Resolution of the Cabinet of Ministers of Ukraine No. 327 of 12 March 2003, Official Journal of Ukraine, 2003, No. 11, p. 506, Art. 490, Act Code 24676/2003. (Ukr)

13. General Safety Provisions for NPP [Zahalni polozbennia bezpeky atomnykh stantsii], NP 306.2.141–2008, Official Journal of Ukraine, 2008, No. 9, p. 28, p. 226. Act Code 42114/2008. (Ukr)

14. *IEC 61226*. Nuclear Power Plants — Instrumentation and Control Important to Safety — Classification of Instrumentation and Control Functions, Geneva, International Electrotechnical Commission, 2009, 26 p.

15. *IEC 62645:2014/COR1:2015* Corrigendum 1 — Nuclear power plants — Instrumentation and control systems, Requirements for security programmes for computer–based system, Geneva, International Electrotechnical Commission.

Отримано 22.06.2015.