УДК 621.039:006.4.2:002

О. Ю. Погосов, О. В. Дерев'янко

Одеський національний політехнічний університет, м. Одеса, Україна

Фізичний захист АЕС та інформаційна безпека як необхідні умови зниження ризиків ядерних і радіаційних аварій

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 АЕС, 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. Запропоновано, у межах загальної формалізації Хатчісона, введення в алгоритми аналізу додаткових функціональних залежностей від показників, характерних для АЕС. Звернуто увагу на доцільність використання регресійного аналізу впливу специфічних обставин, притаманних сучасним умовам експлуатації АЕС.

Ключові слова: ядерна та радіаційна безпека, фізичний захист АЕС, інформаційна безпека атомних енергоблоків.

А. Ю. Погосов, О. В. Деревянко

Физическая защита АЭС и информационная безопасность как необходимые условия снижения рисков ядерных и радиационных аварий

Проанализированы факторы снижения риска ядерных и радиационных аварий на АЭС с учетом специфических условий, связанных с информационной безопасностью в системе физической защиты атомных электростанций. Рассмотрена связь гетерогенных факторов, которые могут влиять на риск возникновения аварий на АЭС, возможность и пути дальнейшего повышения адекватности моделирования динамики защиты информации с ограниченным доступом, непосредственно касающейся функционирования автоматизированного комплекса инженерно-технических средств физической защиты АЭС. Предложено, в рамках общей формализации Хатчисона, включение в алгоритмы анализа дополнительных функциональных зависимостей от показателей, характерных для АЭС. Обращено внимание на целесообразность использования регрессионного анализа влияния специфических обстоятельств, характерных для современных условий эксплуатации АЭС.

Ключевые слова: ядерная и радиационная безопасность, физическая защита АЭС, информационная безопасность атомных энергоблоков.

Аварії на атомних електростанціях можуть мати характер ядерних подій (аварії реактивнісного типу, пов'язані з некерованістю ядерної реакції ділення ядерного пального) та радіаційних подій (аварії, пов'язані з викидами радіоактивних речовин і впливом іонізуючої радіації на довкілля). Ризик цих подій визначається багатьма факторами, серед яких можна виділити техногенні та антропогенні. Щодо антропогенного впливу, ядерна та радіаційна небезпека може бути наслідком втручання зловмисників у технологічний процес з використанням, зокрема, комп'ютерних засобів порушення адекватного управління в разі недостатнього рівня інформаційної безпеки. Як системні фактори можна вказати також соціально-психологічні та політико-економічні (політичні, фінансові, терористично-диверсійні тощо). Пом'якшення чи унеможливлювання дії всіх цих факторів та мінімізація ризику аварій на АЕС — важливе державне стратегічне завдання, яке випливає з економічної та науково-технічної проблеми: АЕС економічно виправдані та потрібні для нормального розвитку промисловості країни, але тільки за умови технічного забезпечення на максимально можливому рівні ядерної та радіаційної безпеки енергоблоків атомних електричних станцій.

Вказана проблема вирішується різними шляхами. Зокрема, як показує світовий досвід багаторічної експлуатації АЕС, її можна уникнути завдяки сукупному використанню організаційних заходів і відповідних технологій. Останні десятиріччя особлива увага приділяється впровадженню на АЕС та удосконаленню технологій запобігання та протидії антропогенним факторам негативного впливу на об'єкти атомної енергетики. Факторами негативного впливу є застосування потенційно небезпечної техніки людиною із зловмисною метою або, в деяких випадках, ненавмисний негативний вплив людини на техніку. Для попередження або компенсації тих чи інших антропогенних факторів, що обумовлюють ризик аварій на АЕС, існують відповідні технології захисту, що передбачають не тільки традиційну озброєну охорону, але й використання спеціальних (невійськових) технічних засобів та методів, які базуються на науково обґрунтованих підходах, науково-технічних розробках та апаратних засобах. Одним з таких сучасних підходів, ефективність якого визнана і наукою, і практикою, є фізичний захист об'єктів атомної енергетики з використанням складних інформаційних, зокрема комп'ютерних, технологій. Це положення узагальнено в рекомендаціях МАГАТЕ [1].

Відповідно до міжнародних юридичних документів і вимог Закону України «Про фізичний захист ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання», система фізичного захисту ядерних енергоустановок (що функціонує, зокрема, у складі енергоблоків АЕС) охоплює інформаційно забезпечені інженерно-технічні заходи (застосування конструкцій та апаратів, зокрема з програмним забезпеченням), які вживаються з метою створення умов, спрямованих на мінімізацію можливості здійснення диверсії, крадіжки або іншого неправомірного вилучення радіоактивних матеріалів, зменшення ймовірності інших протиправних дій відносно ядерних об'єктів, що забезпечують промисловість електричною енергією [2].

Фізичний захист атомних електростанцій, технологія експлуатації яких передбачає використання ядерних енергетичних установок (і напрацювання, як побічних продуктів, радіоактивних матеріалів), синергетично пов'язаний з елементами забезпечення ядерної і радіаційної безпеки АЕС. Апаратне та програмне обмеження несприятливих дій

на АЕС є одним з дієвих інструментів фізичного захисту цих об'єктів від зловмисних антропогенних посягань. Більше того, ефективний фізичний захист АЕС розглядається як важливий комплекс заходів забезпечення не лише ядерної та радіаційної безпеки, але і як основа екологічної, економічної та інших видів безпеки, стратегічно важливих для держави і суспільства. Тому фактори забезпечення достатнього рівня надійності фізичного захисту АЕС, зокрема фактори інформаційної безпеки, яка стосується кібернетичного (тобто пов'язаного з керуванням) впливу, на сучасному етапі розвитку атомної енергетики стали предметом найпильнішого розгляду як в економічному, соціально-психологічному, юридичному, організаційному та практичному аспектах, так і з точки зору природних і технічних наук (в першу чергу), оскільки основою фізичного захисту може бути лише науково обґрунтована, кібернетично забезпечена та інформаційно захищена матеріально-технічна база.

Проблема забезпечення інформаційної безпеки й апаратного (комп'ютеризованого) фізичного захисту АЕС виникає як частина загальної зазначеної проблеми і вирішується на стику багатьох галузей знань, до яких, перш за все, належать фізика, математика, кібернетика, інформатика, криптографія. Загальнотеоретичні аспекти цієї частини проблеми фізичного захисту в атомній електроенергетиці обумовлюють необхідність як глибокого знання базових енерготехнологічних процесів, властивих роботі основного й допоміжного устаткування АЕС, так і необхідність розуміння особливостей інформаційних технологій у роботі станцій для виконання науково-технічних досліджень та розробок, спрямованих на вирішення комплексних завдань безпеки АЕС. Для підготовки фахівців з фізичного захисту енергоблоків АЕС 2016 року відкрита навчальна спеціалізація за фахом «Фізична ядерна безпека» на кафедрі «Атомні електричні станції» Інституту енергетики і комп'ютерно-інтегрованих систем управління Одеського національного політехнічного університету.

Як показує огляд науково-технічної літератури, в частині інформаційного забезпечення фізичної безпеки АЕС є низка поки що достатньою мірою не досліджених питань, до яких належить і питання ефективної протидії комп'ютерно-інтегрованим організованим загрозам (невипадковим, таким, що здійснюються за допомогою комп'ютерної техніки) — як зовнішнім, так і, можливо, внутрішнім. Згідно зі ст. 18 Закону [2], до першочергових вимог фізичного захисту АЕС належить, серед іншого, створення умов для захисту інформації з обмеженим доступом, бо інформаційна безпека, зокрема комп'ютерно-інтегрована безпека (така, що організується і впроваджується як протидія комп'ютерно-інтегрованим загрозам), є важливою складовою фізичної безпеки таких ядерних об'єктів, як АЕС, та потребує використання високотехнологічних, відповідних до нових загроз, інженерно-технічних методів та засобів.

Згідно з чинним законодавством, зокрема з «Вимогами до комплексу інженерно-технічних засобів системи фізичного захисту ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання» [3], технічні засоби системи фізичного захисту ядерних енергетичних установок АЕС об'єднується в інформаційно-керуючу систему для виконання завдань із фізичного захисту об'єктів атомної енергетики — автоматизований інформаційно-керуючий комплекс [4]. Автоматизований інформаційно-керуючий комплекс є важливою кібернетичною складовою частиною системи фізичного захисту будь-якої атомної станції. Такий комплекс має забезпечувати затримку та ускладнення і подальше унеможливлення протиправних дій правопорушників, якщо таке матиме місце, а також забезпечувати непошкодження реєстрації та надійне збереження інформації щодо функціонування обладнання, яке використовується на АЕС. Отже, безпека інформаційних технологій на АЕС є актуальною частиною фізичної безпеки атомних енергоблоків. Таке положення визначає безпрецедентно складне комплексне науково-технічне завдання — удосконалення програмно-технічних засобів захисту інформаційних ресурсів забезпечення фізичного захисту об'єктів атомної енергетики.

Останнім часом дослідженням за цією тематикою приділяється все більша увага [5—8]. Водночас аналіз опублікованих даних свідчить про те, що в математичному моделюванні, яке має складати аналітичну базу кібернетичних методів та засобів протидії актам здійснення загроз, спрямованим проти інформаційної безпеки АЕС, внутрішня специфіка АЕС як об'єктів захисту поки не враховується достатньою мірою, що робить відповідні технічні рішення недостатньо досконалими.

Метою викладених у статті досліджень є аналіз можливостей зниження ризику ядерних та радіаційних аварій на АЕС і, зокрема, аналіз можливості врахування специфічних факторів, пов'язаних з інформаційною безпекою в системі фізичного захисту атомних електростанцій, беручи до уваги синергетичний зв'язок захисту сигнальної інформації, яка використовується в керуванні потенційно небезпечним обладнанням АЕС.

Для досягнення зазначеної мети потрібно проаналізувати:

зв'язок гетерогенних факторів, що можуть впливати на ризик ядерних та радіаційних аварій у сучасній атомній енергетиці і, зокрема, значимість адекватного поводження з оперативною сигнальною інформацією в організації фізичного захисту задля забезпечення безпеки АЕС;

можливість і шляхи подальшого підвищення адекватності моделювання динаміки захисту інформації з обмеженим доступом, що стосується функціонування автоматизованого комплексу інженерно-технічних засобів фізичного захисту АЕС.

Синергетичний вплив факторів на ядерну та радіаційну безпеку АЕС. Системний вплив різноманітних (гетерогенних) факторів на безпеку АЕС і важливу роль інформаційної безпеки відображено на рис. 1.

Наведені на рис. 1 фактори, хоча і є гетерогенними, пов'язані між собою діями оперативного персоналу та певним поводженням з інформацією в межах цих дій. Зауважимо, що робота потенційно небезпечного в ядерному та радіаційному відношенні обладнання (у разі порушення якої може статися некерована ядерна реакція, неконтрольоване вивільнення тепла, розгерметизація реакторного контуру і радіоактивне забруднення) залежить від процедур керування на підставі сигнальної інформації — інформації, яку отримують, аналізують та використовують для формування керуючих сигналів (сигнали є матеріальними носіями інформації).

Сигнали, зокрема техногенного походження (від контрольно-вимірювальних приладів), обробляють в інформаційно-обчислювальному комплексі АЕС. Оброблені сигнали (трансформовані в командні сигнали) надходять на виконавчі механізми технологічного обладнання. Зловмисне втручання в систему аналізу сигналів та систему формування інформаційних сигналів, важливих для керування потенційно небезпечним обладнанням АЕС, або незловмисні (халатні або неуважні) дії підвищують

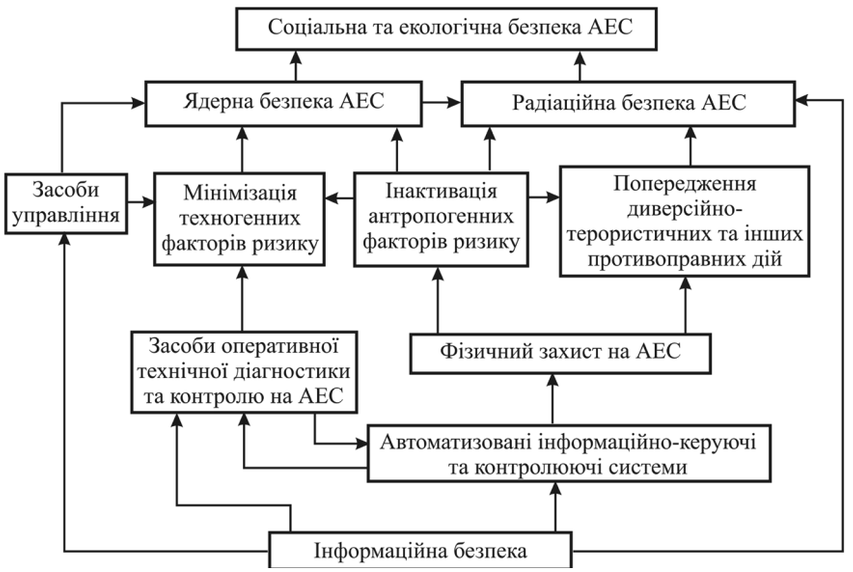

Рис. 1. Схема дії гетерогенних факторів та їх з'язків для забезпечення комплексної (всебічної) безпеки АЕС та системна роль інформаційної безпеки

ризик виникнення аварійних ситуацій. Неадекватне (технологічно незапланованe) втручання в сигнальну інформацію може мати і характер диверсії.

Врахування фактора захисту інформації для фізичної безпеки АЕС. Недооцінювання фактора захисту інформації, яка так чи інакше використовується в процесі вирішення задач керування на АЕС на рівні окремих технологічних систем, може підвищувати ризик ядерних та радіаційних інцидентів і аварій. І навпаки, ефективний захист обладнання протидією інформаційно-технологічним порушенням чи інформаційним атакам методами роботи з сигнальною (комп'ютерною) інформацією знижує ризик ядерних та радіаційних інцидентів і аварій.

До методів роботи з сигнальною інформацією належить, зокрема, використання інформаційно захищених експертних систем та систем підтримки оператора. В сучасних умовах фізичний захист — це не тільки інженерні споруди механічної протидії зовнішньому наземному чи повітряному порушнику, а й комп'ютерна електроніка та програмні засоби протидії зовнішньому та внутрішньому порушнику. Потенційний порушник може мати доступ (або намагатися його отримати) до систем керування технологічними процесами через комп'ютерну техніку. Для цього необов'язково застосовувати механічні інструменти та прилади, можна діяти навіть дистанційно, використовуючи електротокові сигнали та електромагнітні поля для комп'ютеризованого втручання в системи керування, передавання інформаційних сигналів через електромагнітний простір.

Адекватне поводження з сигнальною інформацією (охорона технологічно важливої інформації та протидія інформаційним перешкодам і атакам) з урахуванням показаних зв'язків є важливим фактором забезпечення всебічної (комплексної) безпеки АЕС.

До заходів суто технічного (апаратного, програмного) захисту інформації належить діяльність, спрямована на запобігання порушенню цілісності, блокуванню та (чи) витоку інформації технічними каналами, тобто каналами, що в загальному випадку являють собою сукупність носія інформації, середовища його поширення та засобу технічної розвідки. Проте лише пасивне приховування інформації (унеможливлення або суттєве утруднення несанкціонованого одержання інформації) не завжди є достатнім заходом, і виникає потреба в активній протидії технічній розвідці — несанкціонованому здобуванню інформації за допомогою технічних засобів та аналізу здобутої інформації. Активна форма приховування інформації разом з пасивними заходами може базуватися на методиках, що поєднують різні шляхи та методи створення таких матеріальних носіїв (фізичного поля чи речовини), які ускладнюють здобування інформації або спричиняють невизначеність її змісту [6]. До активної форми приховування інформації належить організоване дезінформування зловмисників — спосіб технічного захисту інформації, що полягає у формуванні свідомо хибної інформації для унеможливлення несанкціонованого доступу до істинної інформації з обмеженим доступом [9, 10].

Всі ці заходи — організаційні (пропускний режим, передбачена інструкціями послідовність дій, обмеження доступу фізичних осіб у певні зони та приміщення тощо), апаратні та програмні — мають сприяти, в кінцевому підсумку, підвищенню ефективності технічного захисту інформації. Ефективність технічного захисту інформації вважається достатньою, якщо за допомогою застосовуваних методик, технічних методів, відповідних способів, автоматизованих засобів та інженерно-фізичних споруд, використовуваних на АЕС, досягається відповідність встановленим вимогам щодо безпеки функціонування енергоблоків станції, які експлуатуються чи вводяться в експлуатацію в близькому майбутньому.

Комп'ютеризовані засоби фізичного захисту, дія яких спрямована, зокрема, на протидію комп'ютеризованим інформаційним атакам (загрозам), для адекватного реагування на інформаційні загрози, мають функціонувати в режимах з програмною підтримкою з боку комп'ютерних експертних систем. Це потрібно також і для ефективного спрацювання на упередження несанкціонованих інформаційних втручань. Робота експертних систем ефективна в тому разі, якщо такі системи є адаптивними та самонавчальними автоматичними програмованими системами, а це забезпечується за допомогою програмного (математичного) моделювання заздалегідь очікуваних (передбачуваних) процесів, з періодичною корекцією та модернізацією математичного забезпечення та програмних кодів. Відповідна корекція та модернізація потребують

врахування специфічних для АЕС факторів, пов'язаних з інформаційною безпекою в системі фізичного захисту, на які не було зважено раніше.

Моделювання процесів протидії інформаційним загрозам для кібернетичного захисту АЕС. У моделюванні процесів, притаманних процедурам фізичного захисту АЕС і функціонуванню систем інформаційної та кібернетичної безпеки, в першому наближенні зазвичай використовується логістична крива, що визначається рівнянням Ферхюльста [11, 13]. Ще 15—20 років тому вважалося, що має місце експоненційне зростання інтенсивності намагань спричинити той чи інший збиток об'єктам атомної енергетики внаслідок зловмисного оперування технологічно важливою інформацією. Але в дійсності експоненційне зростання інтенсивності кібератак (тобто атак з використанням інформаційно-кібернетичних технологій) рано чи пізно закінчується [5]. Інтенсивність активних дій підтримується на деякому рівні, властивому системі «спроба нападу — захист», який можна назвати ємністю захисного демпфера.

Логістична крива в загальному випадку описує зростання зовнішніх кібератак і відповідає аналітичній залежності

$$\frac{dN}{dt} = r\left(1 - \frac{N}{N_c}\right)N\,, \qquad (1)$$

де $N=N(t)$ — потенційна кількість вдалих реалізацій загроз як функція часу; $\frac{dN}{dt}$ — похідна від $N(t)$, яка описує потенційну швидкість реалізації зловмисниками вдалих інформаційних атак, або інтенсивність атак; N_c — середня кількість активних інформаційних об'єктів, до яких можуть бути здійснені загрози; r — показник легкості реалізації тієї чи іншої загрози через певну вразливість об'єкта. Показник r визначається умовами експоненційного зростання із залежності, характерної для початкового етапу зростання $N(t)$:

$$\frac{dN}{dt} = rN\,. \qquad (2)$$

Для подальшого розгляду можливості удосконалення логістичної математичної моделі заради спрощення вигляду виразу (1) позначимо інтенсивність кібератак $x(t)$. Вважатимемо, що припиненню експоненційного зростання $x(t)$ відповідає умовно початковий час $t=0$. Від цього часу, із збільшенням інтенсивності $x(t)$, посилюється і дія зовнішніх та внутрішніх протидіючих факторів, що зменшують швидкість (інтенсивність) кібератак. Спираючись на дослідження в галузі загальної теорії динаміки відбивання будь-яких атак у системі «нападник — захисник» [5], інтенсивність кібератак можна розглядати як функціональну залежність

$$x_i(t) = \frac{K_i}{1 + \frac{K_i - x_i^0}{x_i^0} e^{-r_i^m (t - t_0)}}\,. \qquad (3)$$

Динаміка поведінки цієї функціональної залежності (рис. 2) обумовлена трьома параметрами: x_i^0, K_i та r_i^m. Перший з них (x_i^0) визначає початкове значення кількості атак за певний час, інакше кажучи — інтенсивності чи «щільності» кібератак x_i при $t=t_0$; другий вказує на рівень насичення, до якого прагне $x_i(t)$, тобто на граничну для даного об'єкта кількість намагань дії; третій (r_i^m) задає крутизну початкового зростання функціональної

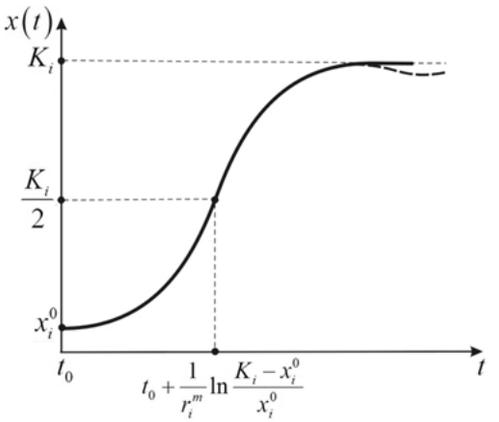

Рис. 2. Ілюстрація впливу показників x_i^0, K_i и r_i^m на форму (кривизну) модельної логістичної кривої при моделюванні динаміки від кібератак на АЕС та відповідного захисту

залежності, верхній індекс m використано як позначку максимальної крутизни графіка.

Щоб з'ясувати математичний і фізико-технічний (важливий для забезпечення безпеки об'єкта) зміст коефіцієнтів r_i^m та K_i, звернемо увагу на те, що залежність питомої швидкості приросту інформаційних (зокрема кібернетичних) атак на об'єкт від щільності активно реалізовних технічних можливостей захисту об'єкта, яка має вигляд $r_i(x_i) = r_i^m - \gamma x_i$, є розкладанням питомої швидкості зростання атак на об'єкт у ряд Тейлора.

Розкладання виконується по степенях, залежних від щільності активізації апаратно-програмних можливостей захисних засобів x_i, і представлене нульовим та першим степенями. Компонента цього розкладання, яка відповідає нульовому степеню, $r_{i_0} = r_i^m$, не залежить від щільності x_i, а компонента, яка відповідає першому степеню, $r_{i_1} = -\gamma x_i$, залежить від щільності x_i, причому при $x_i \to 0$ $r_{i_0} \to 0$. Саме тому за малої початкової щільності x_i^0 первинне зростання можливостей захисту буде майже експоненційним з показником експоненти r_i^m. Отже, цей параметр є нічим іншим, як захисним потенціалом об'єкта, що підлягає фізичному захисту.

Таким чином, якщо потенціал можливого захисту об'єкта в період, який передував сучасному етапу розвитку атомної енергетики, описувався експоненційно зростаючою кривою (потенціал швидко нарощувався), то в подальший період, за теперішнього розвитку атомної енергетики, другий доданок у знаменнику формульної залежності для логістичної кривої прагне до нуля, в результаті чого числові розв'язки $x_i(t)$ асимптотично наближаються до K_i (рівень можливостей прагне до стабілізації). У розглянутій моделі комплексний параметр K_i характеризує ємність потенціалу об'єкта, що підлягає захисту, та виражається відповідною даній ємності граничною кількістю відбивання кібератак.

Отже, тільки досліджуючи динаміку зростання захищеності об'єкта за розширений період часу стає очевидним її S-подібний характер. Верхня межа зростання потенціалу захищеності, яка відповідає K_i, є верхньою асимптотою логістичної кривої (межею зростання захисних можливостей), причому ця межа з часом може зазнавати змін. Як показує аналіз, адекватно (відповідно до умов поточного часу) обираючи величини x_i^0, K_i и r_i^m, можна більш чи менш

задовільно описувати динаміку змін апаратно-програмних можливостей кібератак та захисту від них конкретного об'єкта. Проте рівняння логістичного зростання треба розглядати лише як одну з можливих математичних моделей опису динаміки відбивання кібератак на АЕС. Таку модель можна розглядати як базову — вона доволі примітивна і не враховує деяких перспективних специфічних умов функціонування складних об'єктів, зокрема енергоблоків АЕС.

Отриману залежність кількості зовнішніх атак від часу можна використовувати в аналітичному чи чисельному моделюванні ефективності відбивання кібератак, спрямованих на об'єкти, що потребують фізичного захисту, якщо не брати до уваги їх нестаціонарність [5]. Але специфікою інформаційної безпеки і фізичного захисту АЕС, на думку авторів, є те, що, аналізуючи поведінку цієї модельної функції, треба враховувати нестаціонарність у часі кожного з операндів отриманого виразу (оскільки вони залежать від інших, змінних у часі, показників). Тому зважаючи на сучасну та прогнозовану в ближньому майбутньому специфіку функціонування АЕС потрібно внести корективи до наведеної моделі (3): всі показники в отриманій базовій залежності розглядати як змінні і, крім того, як функції кількох незалежних аргументів.

Зауважимо, що результати наших досліджень, звірені з результатами досліджень в галузі нелінійної динаміки [11], показують, що наведений логістичний закон добре описує динаміку зростання здійснених атак лише тоді, коли немає заходів та засобів протидії загрозі. Математична модель (3) виявляє і певні інші недоліки, якщо взяти до уваги деякі соціальні процеси, які призводять, скажімо, до запізнення реагування на кібератаки. Так, тангенс куту нахилу дотичної (яким ідентифікується інтенсивність кібератак) після моменту часу t=0, прийнятому за початок відліку (область сучасності), зростаючи у ближній перспективі, може не тільки зменшуватися до нульового значення, але й стати від'ємним. Відповідно, модельна S-подібна крива може трансформуватися. Теоретично на форму графіків залежностей, наведених на рис. 2, впливатиме конкретний вибір незалежних аргументів модельної функціональної залежності. Практично цьому можуть сприяти, наприклад, фактор міжнародної зацікавленості в глобальній безпеці атомної енергетики та відповідні заходи щодо зменшення невідбитих кібератак на об'єкти атомної енергетики. Безумовно, ці обставини мають бути враховані в процесі моделювання як специфічні реалії завдань сьогодення в атомній енергетичній галузі.

Для розуміння шляхів подальшого коректного перегляду описаної початкової моделі треба звернути увагу на вказані недоліки, які можуть проявити себе за межами ближньої часової перспективи, і перейти до відповідної ускладненої форми аналітичної моделі. За можливості, у подальших розробках, після накопичення нових емпіричних даних, треба звернутись до моделювання на якнайширшому часовому інтервалі. Задля впровадження більш реалістичного моделювання для розв'язання задач протидії інформаційним та кібернетичним загрозам щодо АЕС, у часовій перспективі можна, на наш погляд, використовувати залежність Хатчісона [13]

$$\frac{dN}{dt} = r\left(1 - \frac{N(t-\tau)}{K}\right)N(t),$$

де τ — час запізнювання реагування на надходження реалізованих інформаційно-кібернетичних загроз.

Розв'язок цього рівняння вказує не на монотонне зростання кількості реалізованих загроз, хоча і зі зниженням інтенсивності, а на зниження цього показника в певному майбутньому періоді; отже, можна очікувати періодичного коливального процесу — загрози можуть розповсюджуватися хвилями, період яких залежить від часу запізнення, а інтенсивність — від коефіцієнта вразливості. З практичної точки зору, запізнення в захисті інформації може виникати, наприклад, за потреби навчання користувачів систем безпеки, фахівців та осіб, що приймають рішення про впровадження та модернізацію таких систем [14]. Люди, від яких залежить безпека АЕС, особливо старшого віку, можуть мати труднощі з професійним перенавчанням або легковажно ставитися до сприймання нових, реально виникаючих загроз, доки не усвідомлять необхідність врахування ризиків у перспективі, пов'язаних з науково-технічним прогресом. Це суттєвий фактор, оскільки сучасною тенденцією, специфічною для АЕС, є збільшення середнього віку персоналу, яким укомплектовані станції [12]. Крім того, запізнювання реагування може виникати внаслідок безтурботності, недооцінки ризиків (відсутності підвищення особистої культури безпеки), що є суто психологічно-інтелектуальною особливістю людини і вагомим антропогенним фактором. Активні дії щодо захисту сигнальної інформації (наприклад, підготовка дезінформації), як і організаційно-соціальні заходи (наприклад, перенавчання), теж неминуче призводять до запізнення реагування, хоча й відмінного в часі.

Час запізнення і коефіцієнт вразливості (відношення кількості «вдалих» атак до загальної кількості атак) з урахуванням специфіки об'єктів атомної енергетики не можна вважати незалежними змінними в моделюванні процесів. Отже, подальше удосконалення моделі для кібернетичного, комп'ютеризованого забезпечення безпеки АЕС [15] має полягати в розгляданні аргументів залежності, представленої у вигляді формалізації Хатчісона як функцій дійсно незалежних змінних або умовно незалежних (некорельованих між собою) факторів. Ці фактори, по-перше, повинні бути виражені чисельно; по-друге, вони є функціями або функціоналами; по-третє, вони характерні саме для умов експлуатації АЕС. До таких багатофакторних функціоналів-показників можна віднести залишковий ресурс експлуатації енергоблока, потужність енергоблока, коефіцієнт встановленої потужності, ймовірність пошкодження активної зони ядерного реактора, ймовірність безаварійної експлуатації енергоблока в цілому, деякі техніко-економічні та геофізичні (в зоні розташування АЕС) показники тощо. Для дослідження значимості тих чи інших факторів може бути використаний регресійний аналіз, а для виявлення їх незалежності — кореляційний аналіз. Регресійний аналіз та кореляційний аналіз щодо впливу такого роду специфічних факторів, притаманних експлуатації енергоблоків АЕС, можуть скласти окремі напрями подальших досліджень за розглянутою тематикою.

Висновки

1. Проаналізовано зв'язок гетерогенних факторів, що можуть впливати на ризик ядерних та радіаційних аварій в сучасній атомній енергетиці. Зокрема, показано значимість впливу відповідного захисту оперативної сигнальної інформації в системі організації фізичного захисту для забезпечення безпеки АЕС. Розглянуто обмеження щодо використання

логістичної залежності Ферхюльста в описі динаміки протидії кібератакам у системі фізичного захисту АЕС.

2. Проаналізовано можливість і шляхи подальшого підвищення адекватності моделювання динаміки захисту інформації з обмеженим доступом, показано, що адекватність моделювання безпосередньо стосується результативного функціонування автоматизованого комплексу інженерно-технічних засобів фізичного захисту АЕС. Звернено увагу на потребу врахування запізнення реагування, притаманного динаміці поновлення та освоєння персоналом АЕС апаратно-програмних засобів інформаційної безпеки.

3. Для реалізації завдань з протидії інформаційним загрозам щодо безпеки АЕС запропоновано включати в алгоритми аналізу, в межах загальної формалізації Хатчісона, додаткові функціональні залежності від показників, характерних для атомної енергетики. Закцентовано на доцільності використання регресійного аналізу впливу специфічних факторів, притаманних сучасним умовам експлуатації АЕС.

Список використаної літератури

1. Рекомендации по физической ядерной безопасности, касающиеся физической защиты ядерных материалов и ядерных установок (INFCIRC/225/REVISION 5). Вена : МАГАТЭ, 2012. 69 с. (Серия изданий МАГАТЭ по физической ядерной безопасности, № 13).

2. Про фізичний захист ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання : Закон України від 19.10.2000 № 2064-III. *Відомості Верховної Ради України (ВВР)*. 2001. № 1. Ст. 1.

3. Вимоги до комплексу інженерно-технічних засобів системи фізичного захисту ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання : Наказ Державної інспекції ядерного регулювання України 05.12.2011 № 176. URL : http://zakon3.rada.gov.ua/laws/show/z1505-11

4. ДСТУ 2226–93. Автоматизовані системи. Терміни та визначення. К. : Ін-т проблем математичних машин і систем Національної академії наук України, 1993. 48 с.

5. Кононович І. В. Динаміка кількості інцидентів інформаційної безпеки. *Інформатика та математичні методи в моделюванні*. Одеса, 2014. Т. 3, № 3. С. 35—43.

6. Конеев И. Р., Беляев А. В. Информационная безопасность предприятия. СПб.: БХВ-Петербург, Проспект, 2003. 160 с.

7. Кононович В. Г., Кононович І. В., Стайкуца С. В., Цвілій О. О. Визначення ідентичності об'єктів у системі соціальної та інформаційної безпеки. *Сучасний захист інформації*. 2015. № 1. С. 19—27.

8. Габидулин Э. М., Кшевецкий А. С., Колыбельников А. И. Защита информации. М. : МФТИ, 2011. 225 с.

9. Про внесення змін до Закону України «Про інформацію». *Відомості Верховної Ради України (ВВР)*. 2011. № 32. Ст. 313.

10. ДСТУ 3396.2–97 Захист інформації. Технічний захист інформації. Терміни та визначення. К. : Держ. служба спец. зв`язку та захисту інформації України, 1997. 20 с.

11. Кононович В. Г., Кононович І. В., Копитін Ю. В., Стайкуца С. В. Вплив затримки прийняття заходів із захисту інформації на ризики інформаційної безпеки. *Безпека інформації*. 2014. Т. 20, № 1. С. 83—91.

12. Карпов В. В. Цена российского атомщика. *Атомная стратегия*. С. 8—10.

13. Долгий Ю. Ф., Сурков П. Г. Математические модели динамических систем с запаздыванием: Учеб. Пособие. Екатеринбург : Изд-во Урал. ун-та, 2012. 122 с.

14. Бобок И. И., Кобозева А. А., Максимов М. В., Максимова О. Б. Проверка целостности записей камер видеонаблюдения в режиме реального времени на объектах атомной енергетики. *Ядерна та радіаційна безпека*. 2016. Вип. 2 (70). С. 68–72.

15. Клевцов А. Л., Трубчанинов С. А. Компьютерная безопасность информационных и управляющих систем АЭС: кибернетические угрозы. *Ядерна та радіаційна безпека*. 2015. Вип. 1 (66). С. 54—58.

References

1. Nuclear Security Recommendations on Physical Protection of Nuclear Materials and Nuclear Facilities (INFCIRC/225/REVISION 5), Vienna, IAEA, 2012, 69 p. (IAEA Nuclear Security Series No. 13).

2. Law of Ukraine "On Physical Protection of Nuclear Facilities, Nuclear Materials, Radioactive Waste, Other Radiation Sources" No. 2064-III dated 19 October 2000 [Zakon Ukrainy "Pro fizychnyi zakhyst yadernykh ustanovok, yadernykh materialiv, radioaktyvnykh vidkhodiv, inshykh dzherel ionizuiuchoho vyprominiuvannia" vid 19.10.2000 No. 2064-III], Bulletin of the Verkhovna Rada of Ukraine, 2001, No. 1, Art. 1. (Ukr)

3. Requirements for the Set of Engineering and Technical Means for Physical Protection of Nuclear Facilities, Nuclear Materials, Other Radiation Sources, Order of State Nuclear Regulatory Inspectorate of Ukraine No. 176 dated 05 December 2011 [Vymohy do kompleksu inzhenerno-tekhnichnykh zasobiv systemy fizychnoho zakhystu yadernykh ustanovok, yadernykh materialiv, radioaktynykh vidkhodiv, inshykh dzherel ionizuiuchoho vyprominiuvannia, Nakaz Derzhavnoi inspektsii yadernoho rehuliuvannia Ukrainy 05.12.2011 No. 176], available at: http://zakon3.rada.gov.ua/laws/show/z1505-11 (Ukr)

4. DSTU 2226-93. Automated Systems. Terms and Definitions. [Avtomatyzovani systemy. Terminy ta vyznachennia], Kyiv, Institute of Mathematical Machines and Systems Problems, National Academy of Sciences of Ukraine, 1993, 48 p. (Ukr)

5. *Kononovych, I. V.* (2014), "Changes in the Number of Information Security Incidents" [Dynamika kilkosti intsydentiv informatsiinoi bezpeky], Informatics and Methematical Methods in Modelling, Odesa, V. 3, No. 3, pp. 35–43. (Ukr)

6. *Konieiev, I. R., Beliaiev, A.V.* (2003), "Enterprise IT" Security [Informatsionnaia bezopasnost predpriiatiia], Saint Petersburg, Prospekt, 160 p. (Rus)

7. *Kononovych, V. H., Kononovych, I. V., Staikutsa, S. V., Tsvilii, O. O.* (2015), "Determining the Identity of Objects in the Social and Information Security System" [Vyznachennia identychnosti obiektiv u systemi sotsialnoi ta informatsiinoi bezpeky], *Modern Information Security*, No. 1, pp. 19–27. (Ukr)

8. *Gabidulin, E. M., Kshevetskyi, A. S., Kolybelnikov, A. I.* (2011), "Information Security" [Zashchita informatsii], Moscow, MFTI, 225 p. (Rus)

9. On Amending the Law of Ukraine "On Information" [Pro vnesennia zmin do Zakonu Ukrainy "Pro informatsiiu"], Bulletin of the Verkhovna Rada of Ukraine, 2011, No. 32, Art. 313. (Ukr)

10. DSTU 3396.2-97. Information Security. Technical Protectionof Information. Terms and Definitions. [Zakhyst informatsii. Tekhnichnyi zakhyst informatsii. Terminy ta vyznachennia], Kyiv, State Service of Special Communications and Information Protection of Ukraine, 1997, 20 p. (Ukr)

11. *Kononovych, V. H., Kononovych, I. V., Kopytin, Yu. V., Staikutsa, S. V.* (2014), "Impact of Delayed Taking of Measures on Information Protection and Information Security Risks" [Vplyv zatrymky pryiniattia zakhodiv iz zakhystu informatsii na ryzyky informatsiinoi bezpeky], Information Security, 2014, V. 20, No. 1, pp. 83–91. (Ukr)

12. *Karpov, V. V.* "The Price of Russian Nuclear Scientist" [Tsena rosiiskogo atomshchika], Atomic Strategy, pp. 8-10. (Rus)

13. *Dolgii, Yu. F., Surkov, P. G.* (2012), "Mathematical Models of Denamic Systems with Delay" [Matematicheskiie modeli dinamicheskikh sistem s zapazdyvaniiem], Manual, Yekaterinburg, Ural University Publishing House, 122 p. (Rus)

14. *Bobok, I. I., Kobozeva, A. A., Maksimov, M. V., Maksimova, O. B.* (2016), "Cheking the Integrity of CCTV Footage at Nuclear Facilities References", [Proverka tselosnosti zapisei kamer videonabliudeniia v rezhyme realnogo vremeni na obiektakh atomnoi energetiki], Nuclear and Radiation Safety Journal, No. 2 (70), pp. 68–72. (Rus)

15. *Klevtsov, A. L., Trubchaninov, S. A.* (2015), "Computer Security of NPP Instrumentation and Control Systems: Cyber Threats" [Kompiuternaia bezopasnost informatsionnykh i upravliaiushchikh sistem AES: kiberneticheskiie ugrozy], Nuclear and Radiation Safety Journal, No. 1 (66), pp. 54–58. (Rus)

Отримано 28.12.2016.