УДК 004.05.7:681.3.07

В. М. Бурлаков, В. Г. Кононович, І. В. Кононович

СИНЕРГІЯ ТА ТЕМПОДИНАМІКА ВДОСКОНАЛЕННЯ МОДЕЛІ КІБЕРНЕТИЧНИХ ЗАГРОЗ ЯДЕРНИХ ОБ’ЄКТІВ

Анотація: Метою роботи є створення синергійної моделі проектних загроз інформаційній, кібернетичній та ядерній безпеці критично важливих об’єктів ядерної енергетики України Для досягнення мети вирішуються завдання: формулювання принципів побудови проектної моделі кіберзагроз автоматизованим системам технологічного й адміністративного управління, важливих для забезпечення ядерної безпеки; складання переліку проектних кіберзагроз із урахуванням цільової діяльності підприємства, особливостей і вразливостей об’єктів ядерної сфери; розроблення формалізованої дискретної математичної моделі періодичного вдосконалення переліку проектних кіберзагроз.

Ключові слова: інформаційна безпека, кібербезпека, ядерна безпека, критично важливі об’єкти, проектні загрози, модель динамічної системи, циклічне управління.

Опис проблеми

Набуття чинності закону України «Про основні засади забезпечення кібербезпеки України» вимагає вирішення задач кібербезпеки критично важливих об’єктів (далі – КВО) енергетики, зокрема атомних електричних станцій (далі – АЕС). Нормативною базою ядерної галузі визначено вимоги забезпечення безпеки АЕС за рахунок послідовної реалізації стратегії глибоко ешелонованого захисту, заснованого на застосуванні системи технічних та організаційних заходів бар’єрного захисту [1]. Вимоги щодо послуг і функцій ефективного забезпечення інформаційної безпеки інформаційних та керуючих систем, важливих для безпеки АЕС, знайшли своє відображення у [2]. На черзі – забезпечення кібернетичної безпеки на основі синергійних моделей проектних загроз інформаційній, кібернетичній та ядерній безпеці критично важливих об’єктів ядерної енергетики України.

Огляд існуючих моделей проектних загроз ядерної безпеки

У доповіді на Всесвітньому економічному форумі 2016 року щодо кібербезпеки цивільних ядерних об’єктів (ЯО) зазначено: «Виклики кібербезпеки стали одною з ключових проблем для операторів КВО в усіх секторах. Стрімкий прогрес у нарощувані потенціалу проактивних кібероперацій та різке зростання кількості інцидентів кібербезпеки на КВО вимагають невідкладних відповідних заходів. … Кожен силовий блок на АЕС оснащений декількома підсистемами АСУ ТП (АСУ технологічними процесами), які необхідно інтегрувати між собою, а також

забезпечити безпеку й сумісність з корпоративним програмним забезпеченням (далі – ПЗ), яке відповідає за процеси управління та збору даних [3]».

В [4] відмічено з одного боку важливу роль МАГАТЕ з питань формування переліку проектних загроз ЯО, а з іншого зазначено, що «до 2009 року серед документів МАГАТЕ не було жодного, який було б присвячено питанням кібербезпеки». В Україні захист інформації тільки розпочинав набирати свого значення [5].

Досягнутий рівень науки і техніки, комп’ютеризації, автоматизації та телекомунікацій на жаль супроводжується новими загрозами й вразливостями для ядерної безпеки (далі – ЯБ). Наукові праці вітчизняних вчених, серія документів МАГАТЕ та інших організацій, що опубліковані після 2014 року, проводять принцип комплексування кібербезпеки з фізичною ядерною безпекою [6 – 8]. МАГАТЕ почало активне врахування питань кібербезпеки при визначенні проектних загроз (NSS 10). Іншими словами – головна ціль системи кібербезпеки, серед іншого, це захист від кіберзагроз системи забезпечення ЯБ. Неврахування синергійного підходу, який останнім часом відзначив свій розвиток [9, 10], до моделі загроз, аналізу ризиків, єдиної методології оцінювання безпеки систем технологічного та адміністративного управління у стандартах ядерного сектору не дозволяє продукувати відповідні політики, адекватні підходи та заходи із забезпечення кібербезпеки та фізичної ядерної безпеки (кіберфізичної ядерної безпеки). Набуває своєї актуальності вимога додати ще один бар’єр – розподілений інформаційно-кібернетичний бар’єр, що доповнить глибоко ешелонований захист АЕС. Труднощі, що виникають при отриманні гармонізованих між собою моделей проектних загроз, вимагають глибокої наукової і методичної проробки.

Метою роботи є створення синергійної моделі проектних кіберзагроз ядерної безпеки АЕС та динамічної математичної моделі циклічних процесів вдосконалення номенклатури загроз із врахуванням оновлених пріоритетів інформаційної, кібернетичної та ядерної безпеки.

Для досягнення поставленої мети були сформульовані та вирішені наступні задачі: формулювання принципів побудови проектної моделі кіберзагроз автоматизованим системам технологічного й адміністративного управління, важливим для забезпечення ядерної безпеки; складання синергійного переліку кіберзагроз із урахуванням факторів цільової неперервної діяльності підприємства, особливостей вразливостей об’єктів ядерної сфери; розробка дискретної нелінійної математичної моделі циклічного процесу вдосконалення номенклатури проектних кіберзагроз.

Основна частина

1. Принципи побудови моделі проектних кіберзагроз

Зважаючи на специфіку, особливості і високу потенційну небезпечність ЯО, на всіх етапах «життєвого циклу» необхідно дотримуватись таких принципів, більшість з яких закріплені нормативно-законодавчими актами або є результатом наукових досліджень:

1. «Дотримання принципів культури безпеки досягається шляхом встановлення пріоритету ЯБ над економічними та виробничими цілями … і пов’язані з необхідністю всебічної оцінки безпеки [1, 11]». Відповідно цілі кібербезпеки мають бути підпорядковані цілям ЯБ, а прийняття рішень повинно здійснюватись виключно в інтересах ЯБ, а вже потім в інтересах забезпечення неперервності бізнесу та інших цілей. «Необхідно, щоб цілі (кібер)безпеки були узгоджені з визначеними цілями призначення [див. 10]» ЯО, із задачами ЯБ, а також з відомостями щодо фізичного середовища ядерних установок (ЯУ).

2. Принципи апробованості програмних й інженерно-технічних практик, консервативного підходу та врахування нових науково-технічних даних. Принципу апробованості відповідають, наприклад, галузеві СОУ щодо інформаційної безпеки Національного банку України, побудовані на базі міжнародних стандартів серії ISO/IEC 2700x. Вони можуть бути зразками для СОУ АЕС. Проектування конструкцій, систем, елементів, ПЗ, засобів кібербезпеки повинно здійснюватись на основі консервативних підходів [1].

3. Принципи актуальності та ефективності. Мета системи кібербезпеки «гарантувати, що автоматизовані системи та комунікаційні мережі, необхідні для надійного постачання електроенергії у країні, **розумно** захищені від атак із різноманітних ймовірних джерел загроз, а також підтримується життєздатність та ефективність такого захисту». Це досягається комплексним впровадженням різних захисних заходів, організаційних і технічних, управлінських та юридичних, застосованих у правильний час і у правильному місті і лише після всебічного вивчення об’єктів захисту та ризиків, які з ним пов’язані [4].

4. Принцип антропо-центричності. Середовище безпеки включає всі закони, політики безпеки організацій, досвід, спеціальні навики та знання, для яких вирішено, що вони мають відношення до безпеки та загроз безпеки. До уваги слід приймати всі різновиди загроз, але найбільшу увагу приділяють загрозам, які пов’язані з навмисними чи ненавмисними діями людини. Саме останні загрози несуть непоправимі наслідки на КВО [10].

5. Принцип комплексності, інтеграції та конвергенції видів безпек з ядерною безпекою АЕС. Трансграничність атак, складність внутрішньої ІТ- інфра-

структури ЯО та висока інтенсивність потоків даних вимагають комплексного та всеохоплюючого підходу до кібербезпеки, який принципово виходить за рамки тільки лише реагування на інциденти. Перед усім встановлюється взаємозв’язок безпеки АЕС з фізичною безпекою. Вимога 8 з [12] встановлює: «Заходи із забезпечення безпеки, фізичної ЯБ та механізми для державної системи обліку та контролю ядерного матеріалу повинні розроблятись та здійснюватись на комплексній основі таким чином, щоб одні не здійснювались на шкоду другим».

Одночасно діє вимога 64 з [12]: «Взаємовплив систем захисту та систем управління на АЕС повинен бути попередженим за допомогою поділу, шляхом виключення взаємозв’язків або забезпечення відповідної функціональної незалежності». Обговорюється інтеграція безпеки ПО в систему фізичної ЯБ [13], агентство розробляє додаткові керівні матеріали з фізичної ЯБ, які стосуються комп’ютерної безпеки. У матеріалах конференції МАГАТЕ [14, 15] відмічені три напрями забезпечення кібербезпеки, які є важливими складовими забезпечення безпеки ЯО:

- кібербезпека АСУ ТП ЯО. Модель кіберзагроз АСУ ТП має характерні риси для КВО і, крім того, враховує специфіку, особливості, задачі ЯБ та цільової діяльності ЯО. Методична, нормативна та технічна база цього напряму в Україні вже має певні напрацювання і деякі випробувані зразки. Позначається [15], що в цьому напрямку є проблеми недостатньої обізнаності щодо загроз та засобів захисту як у ядерній галузі в цілому, так і у спеціалістів, що експлуатують АСУ ТП на АЕС. Має місце нездатність професіоналів в області кіберпростору і спеціалістів, які проектують та експлуатують ЯУ, знайти спільну мову та ефективно співробітничати. Тим більше, що відсутня постійна практика такого співробітництва [15];

- кібербезпека інформаційних та керуючих систем. Слід розрізняти системи телеметричного контролю для збору й аналізу даних та автоматизовані системи, а нині інформаційно-телекомунікаційні системи, для адміністративного управління (наприклад, системи документообігу, бухгалтерські системи тощо). Тут придатна модель загроз типового державного підприємства з поправками на встановлений режим. Головне у тому, щоб врахувати віртуальні не прямі зв’язки з фізичним захистом та захистом АСУ ТП. Наприклад, дані про переміщення ядерного матеріалу можуть зберігатись у базі даних адміністративного управління;

- кібербезпека систем фізичного захисту ЯО. Важливість даного напряму тільки починає усвідомлюватись спеціалістами за мірою автоматизації фізичного захисту. Для ефективного забезпечення безпеки набуває свого значення ще один бар’єр – розподілений інформаційно-кібернетичний бар’єр, що має доповнити

глибоко ешелонований захист АС. Гостра проблема полягає в тому, що спеціалісти з кібербезпеки повинні освоїти уявлення про системи ФЯБ й особливості проектування та функціонування АСУ ТП ЯО. А проектувальникам та експлуатаційному персоналу ЯУ, відповідно – освоїти уявлення щодо заходів забезпечення кібербезпеки. Взаємний обмін обізнаністю має привести до відсутності конфліктів між заходами фізичної ЯБ (далі – ФЯБ) та кібербезпеки, включаючи заходи з реагування на несанкціоновані дії, заходи з обслуговування та управління системами тощо. Крім того, поставлена задача з розробки методик й інструментів, спрямованих на об’єднання процесів аналізу вразливостей у обох сферах забезпечення безпеки ядерних об’єктів. Потрібно виявляти програмно-технічні засоби, ланцюги обладнання та мережі, способи фізичного доступу до них, через які здійснюються трансграничні кібератаки, і включати такі ланцюги у перелік елементів захисту систем ФЯБ.

6. Принцип функціональної повноти заходів захисту. У матеріалах конференції МАГАТЕ виділено три напрями забезпечення кібербезпеки, важливі для забезпечення безпеки ЯО (див. принцип 5). Але ці три напрями не складають функціонально повної системи забезпечення кібербезпеки АЕС. На відміну від задач і об’єктів інформаційної безпеки АЕС об’єктом забезпечення кібербезпеки стає кіберпростір. Його важливі складові: це локальні інформаційно-комунікаційні системи та телекомунікаційна системи.

Значну частину кіберпростору займають телекомунікаційні системи та мережі, які створили по суті телекомунікаційне середовище, а також мережу Інтернет. Телекомунікаційне середовище створює певні проблеми безпеки і є джерелом загроз. Кібератаки здійснюються через телекомунікаційні системи, прямо, чи опосередковано через флеші, або через мобільні телефони, підключені з метою підзарядки до апаратних засобів локальної обчислювальної мережі АЕС.

2. Вразливості ядерного об’єкта від кіберзагроз

«Аналіз останніх інцидентів виявляє ряд основних тенденцій. У відношенні до ЯУ переважають кіберзагрози підвищеної складності, використовуються інструменти кібершпигунства та цілеспрямовано обираються цілі серед критичних систем та співробітників ЯО. Сучасне деструктивне ПЗ є багатомодульним і легко модифікується. Кібератаки стали постійними загрозами підвищеної небезпеки, їх життєвий цикл» досяг декількох років. Крім звичайних загроз сформовано загрози специфічних інцидентів на ЯО». Автори доповіді [3] виділяють такі причини росту вразливостей кібербезпеки КВО: масштабний і все ще триваючий перехід на цифрові системи управління виробничими та технологічними процесами (ВТП); практика підключення офісних і навіть промислових корпоративних мереж до Інтернет, а в подальшому – до Інтернету речей; повсюдне розповсю-

дження мобільного зв’язку; використання віддаленого управління; проблема контролю та довіри до постачальників обладнання систем управління, контролю, комунікацій та ПЗ. До цього додамо, що телекомунікаційні системи та мережі поки що є «постачальниками» анонімності, не гарантована в реальному часі ідентичність кожної з транзакцій і неспростовність від участі в обміні.

КВО ядерної енергетики характеризуються виключно високим рівнем інфраструктурної складності «інформаційних систем ядерних установок, які включають сотні систем управління ВТП та багато тисяч датчиків на кожну АЕС [3]». Це створює організаційну і техногенну загрозу безпеці ядерних КВО.

Унікальні і такі, що не мають аналогів для кожного об’єкта атомної енергетики, архітектурні рішення у сфері забезпечення кібербезпеки та мережевої безпеки суттєво обмежують можливості застосування попереднього досвіду та кращих практик.

3. Модель порушника кібербезпеки та класифікація загроз

Кібератаки та напади на АСУ ТП здійснюються за допомогою програмно-технічних засобів, телекомунікаційних мереж та Інтернет. Специфікою потенційних кібератак у ядерній галузі «може бути: практика регулювання діяльності ЯО, що склалася; технічні особливості їх функціонування, зокрема, необхідність неперервного функціонування технологічних процесів протягом тривалого часу; відокремленість та закритість ядерної галузі; недостатня обізнаність працівників ЯО щодо кіберзагроз та їх потенційних наслідків для безпеки радіоактивних матеріалів та ЯУ а також хибна думка про захищеність ЯО від кіберзагроз» тим, що вони та їх АСУ ТП фізично відокремлені від інформаційних мереж. «Крім того, на ядерних об’єктах автоматизованими являються системи фізичного захисту ЯО, обліку та контролю ядерних матеріалів, різні системи документообігу та бухгалтерського обліку [15]». Кібератака може привести до припинення функціонування АСУ ТП, до виконання її функцій з параметрами, які не спостерігаються операторами або до нештатного виконання команд оператора.

Протиправні дії у відношенні до об’єктів, які підлягають захисту, можуть скоїти різні зловмисники. Їх розподіляють на рівні від «технічно не грамотних фанатів-одинаків до добре озброєних злочинних груп, які володіють знаннями та технологіями, що потрібні для управління ЯУ, які мають можливість віддаленого доступу до управління системами об’єкта захисту та які діють у змові з персоналом АЕС».

«Проектні загрози» ЯБ та сценарії їх здійснення повинні аналізуватись для кожного конкретного об’єкта із врахуванням соціальної та криміногенної обстановки, інформаційних та кіберзагроз безпеки, які визнані на рівні держави

та галузі, степеню ризику для потенційних наслідків аварій та можливих шляхів впливу на елементи ЯУ з метою викликати ядерний інцидент.

«Кібератаки можуть здійснюватись віддалено, або з території ЯО. В останньому випадку зловмиснику необхідно отримати фізичний доступ до елементів ЯУ або приєднати носій із зловмисним ПЗ до елементів установки. Простіше за все зробити це при сприянні персоналу ЯО або підрядних організацій [15]». Можливе зараження зловмисним ПЗ через електронну пошту.

В Україні і міжнародній спільноті «відсутня універсальна таксономія та класифікація кібернетичного впливу на ЯУ та й на інші типові об’єкти. Сучасні АСУ ТП класифікують з урахуванням їх впливу на безпеку АЕС. За впливом АСУ ТП, як елемента АЕС, на безпеку зазвичай класифікують за чотирма класами. Проектні загрози потрібно розподіляти за цими класами. За своїми цілями кібернетичні загрози (КЯБ) поділимо на розвідувальні, підготовчі, знищувальні або аварійні, терористичні, а також на крадіжку ядерних матеріалів, на порушення бізнес-процесів ЯО або руйнування іміджу об’єкта, як надійно захищеного від зловмисних впливів, на завдання фінансових, репутаційних чи моральних збитків, на доступ, знищення, модифікацію, блокування чи копіювання інформації або комбіновані. Орієнтовний перелік загроз КЯБ складено на основі аналізу інцидентів з безпекою, проведеного вітчизняними та зарубіжними спеціалістами [15, 16 та іншими]. Перелік може стати базою для множини *проектних загроз*.

4. Номенклатура проектних загроз кібернетичної ядерної безпеки

Для забезпечення ЯБ на ЯО проектуються і створюються системи ЯБ, які включають обладнання, ПЗ, персонал та регламенти. Початковими даними для проектування таких систем є результати аналізу вразливостей та загроз ЯО, включаючи опис сценаріїв здійснення загроз.

А. *Загрози з метою спровокувати аварію з неприйнятними радіаційними наслідками*:

1) кібератаки на АСУ ТП ядерної установки, які направлені на: спотворення (змінення) або блокування управляючих команд; блокування доступу оператора до інформації щодо стану ЯО або спотворення такої інформації; перепрограмування промислових контролерів. Все це також з метою ініціювання аварії або створення умов для виникнення аварійної ситуації;

2) кібератаки на автоматизовані системи ФЯБ, систему фізичного захисту та систему обліку й контролю ядерних матеріалів, включно, з метою: порушення функціонування системи фізичного захисту (ФЗ) та/або обліку та контролю для скоєння диверсій; віддаленого відключення засобів контролю й управління доступом до приміщень з елементами, які захищаються; зміни налаштувань вимірювальних систем, які застосовуються для обліку й контролю ядерних матеріалів;

3) кібератаки на АСУ ТП ЯО, доступ, знищення або фальсифікація даних для можливості зловмисникам здійснити диверсію;

4) загроза отримання віддаленого доступу до автоматизованої системи та управління елементами системи ФЗ за допомогою програмного забезпечення для створення VPN, яке застосовується постачальником системи ФЗ, IP-адрес обладнання системи ФЗ, імен користувачів та паролів, що використовуються за умовчанням або встановлення безпосереднього зв’язку з іншими мережами;

5) загроза отримання даних щодо доступу. Ця інформація може буди отримана у різний спосіб, включаючи кібератаки на постачальників обладнання, підкуп, оману або шантаж персоналу. Далі, шляхом віддаленого управління елементами ФЗ зловмисники можуть забезпечити собі безперешкодний прохід у зони ЯО, що охороняються, для скоєння диверсії або крадіжки та вихід із них, одночасно заблокувавши прохід для персоналу. Можливі маніпуляції з камерами відеоспостереження;

6) загроза компрометації (наприклад, кібератаки, маніпуляції або фальсифікації) комп’ютеризованих систем, які використовуються для забезпечення ФЗ, ядерної безпеки, а також обліку та контролю ядерних матеріалів, для саботажу або диверсій [16].

Б. *Загрози крадіжки ядерних матеріалів*:

1) кібератаки на автоматизовані системи ФЯБ, систему ФЗ та систему обліку й контролю ядерних матеріалів, включно, з метою: порушення функціонування системи ФЗ та/або обліку та контролю для підготовки крадіжки радіоактивних матеріалів; зокрема, віддалене відключення засобів контролю й управління доступом до приміщень з елементами, які захищаються; зміни налаштувань вимірювальних систем, які застосовуються для обліку й контролю ядерних матеріалів;

2) кібератаки на автоматизовані інформаційні системи ЯО: доступ, знищення або фальсифікація даних, зокрема даних щодо інвентарної кількості ядерних матеріалів, для можливості здійснити крадіжку та приховати факт крадіжки на якомога більший термін;

3) загроза несанкціонованого доступу до системи документообігу ЯО з метою розвідки відомостей щодо графіка проведення техобслуговування елементів системи ФЗ, інформаційного та кібернетичного захисту, транспортування ядерних матеріалів, порядку дій персоналу по виявленню та припиненню несанкціонованих дій;

4) загроза компрометації корпоративної мережі шляхом розсилки у внутрішній мережі підприємства фішингових повідомлень, через які може бути завантажено шкідливе ПЗ, здатний викрасти креслення та схеми ЯУ. Далі така інформація дозволить правопорушникам виявляти способи диверсії або крадіжки;

5) загроза компрометації комп’ютеризованих систем, важливих для забезпечення ФЗ, ЯБ, а також обліку та контролю ядерних матеріалів, для несанкціонованого вилучення при використанні та зберіганні ядерних та інших небезпечних матеріалів [16].

В. *Загальні та інші загрози:*

1) загроза довіри до десятків і сотень ІТ – постачальників і необхідність забезпечення цілісності ланцюжків поставок ІТ – продукції, особливо для АСУ ТП, через практичну неможливість здійснення всеохоплюючої повної перевірки контролерів, дистанційних терміналів, маршрутизаторів, програмних застосувань і програмних комплексів по управлінню технологічними процесами тощо, на прихований функціонал, шкідливе ПЗ забезпечення або помилки.

2) загроза проникнення шкідливого ПЗ. Точка входу може бути одна, а розповсюджується це ПЗ по всій системі або мережі.

3) загроза отримання інформації або державних інформаційних ресурсів, що підлягають захисту згідно законодавства, персональних даних персоналу АЕС, даних щодо постачальників та продукції, що поставляється, звітної інформації, інших документів, які містять інформацію з обмеженим доступом.

5. Моделювання темподинаміки вдосконалення переліку проектних загроз

Процес створення переліку проектних загроз повторюється циклічно задля його вдосконалення, вираховування нових загроз і науково-технічних досягнень. Цикл включає етапи: визначення задач безпеки; визначення процесів цільової діяльності (експлуатаційних технологічних процесів); складання переліку і визначення цінності об’єктів захисту; складання переліку зловмисників і засобів нападу на захист; складання, власне, переліку загроз та ризику їх реалізації; складання переліку засобів і організаційних заходів безпеки тощо.

Відомо, що соціальні, економічні, політичні тощо процеси є нелінійними, рефлексивними і залежать від багатьох зворотних зв’язків. *Мета задачі моделювання* полягає у якісному визначенні за яких умов процес вдосконалення переліку проектних загроз може сам стати загрозою процесові забезпечення кібербезпеки.

Прототипом для такої моделі буде система менеджменту якості, в аспекті постійного поліпшення її результативності на основі процесно-орієнтованого підходу, вимоги до якої сформульовані у стандарті ДСТУ/ISO 9001:2015. Для зниження відхилень процесів застосовують в управлінні, наприклад, концепцію PDCA (плануй (Plan), роби (Do), перевіряй (Check), дій (Act)). Основними елементами циклу PDCA є: P – визначення цілей та прийняття рішення щодо необхідних змін (розробка плану); D – здійснення змін (втілення плану); C – оцінка та аналіз результатів (контроль виконання плану); A – проведення необхідних дій, якщо результати не відповідають запланованим, або стандартизація дій

у випадку успіху (коригування плану). Цикли PDCA та процесу вдосконалення переліку проектних загроз (ВППЗ) інтерпретуються взаємно однозначно. У циклічній схемі управління процесом ВППЗ є певне запізнювання, проявляються різні нелінійні явища. Ці явища можуть негативно впливати на надійність системи ВППЗ і всієї системи управління кібербезпекою. Подібна задача вирішувалась стосовно циклічного управління кібербезпекою в [17] і стосовно управління колективною та індивідуальною свідомістю громадян у [18]. «Ефективність людської дії здебільшого залежить від правильного управлінського рішення, що, у свою чергу, залежить від інформаційного моделювання ситуації, від пошуку потрібної інформації та її переробки. Лавиноподібне зростання інформаційних потоків, в яких змішувались потрібна і непотрібна інформація («інформаційні шуми»), у значній мірі утруднив поведінку людини та висунув на передній план вибірковий пошук потрібної інформації з наступною її редукцією для прийняття тих чи інших рішень [19, с. 142]».

У процесі ВППЗ збирається, обробляється і генерується інформація щодо загроз, механізмів захисту, дій персоналу тощо. Інформація поступає у вигляді документів, повідомлень, які утворюють дискретний потік. Тому модель має формуватись за допомогою, так званих, дискретних відображень. Оберемо найпростіші нелінійні дискретні відображення, які вперше дослідив Фейгенбаум [20]. Будемо розглядати деякий аналітичний процес управління від моменту часу, коли на початку циклу управління в момент t_0 на вхід управляючого елемента системи подавався вектор вхідних сигналів $\mathbf{X}_0 = \{x_{01}, x_{02}, ...\}$, обчислено результат $\mathbf{S}_0$, на виході управляючого елемента системи маємо вектор вихідних сигналів $\mathbf{Y}_0(S_0)$. Припустимо, що сума $\mathbf{S}$ та вихідний сигнал $\mathbf{Y}_0(S_0)$ запам’ятовується у системі.

Функціонал перетворень в управляючому циклі нам невідомий. Щоб вивчити вклад управляючого елемента в процес управління, будемо вважати, що, у найпростішому випадку, всі інші перетворення в управляючому елементі однозначні і мають адитивний характер. Тоді, в кінці циклу управління в момент часу t_1, після закінчення перехідних процесів, маємо вектор вхідних сигналів $\mathbf{X}_1 = \{x_{11}, x_{12}, ...\}$, встановлюється сума S_1, на виході управляючого елемента системи маємо вихідний сигнал $Y_1(S_1)$. При цьому, $S_1 = S_0 + s_{in}$, де s_{in} – зміна суми S під впливом потоку управління. Задамо найпростіше нелінійне правило переходу від $Y_0(S_0)$ до $Y_1(S_1)$ таким чином, щоб зміна суми S за один крок в одному управляючому елементі циклу записувалася так:

$$S_1 = \frac{dy}{dS} = \alpha S_0 \left(1 - S_0\right) + s_{in}. \qquad (1)$$

Провівши ітераційні перетворення, у загальному вигляді отримуємо формулу

$$S_{n+1} = \alpha S_n \left(1 - S_n\right) + s_{in}, \tag{2}$$

де n – номер ітерації, яке має смисл дискретного модельного часу; α – параметр, який називають коефіцієнтом росту.

Таким чином, отримано одномірне дискретне відображення із вхідним потоком. Якщо $s_{in} = 0$, то маємо одномірне дискретне відображення, яке наливають *логістичним відображенням* і яке ретельно проаналізоване у численних публікаціях [21]. Зокрема відомо, що при невеликих значеннях α ($0 < \alpha < 1$) $S_n \to 0$ при $n \to \infty$, незалежно від вибору початкового значення S_0. Існують нерухомі точки, для яких справедлива рівність

$$S^* = \alpha S^* \left(1 - S^*\right). \tag{3}$$

При $\alpha < 1$ квадратне рівняння (3) має один невід’ємний корінь $S^* = 0$. Нерухома точка стійка. При $\alpha > 1$ невід’ємних коренів два: $S^* = 0$ і $S^* = (\alpha - 1) / \alpha$. При $\alpha = 1$ нерухома точка $S^* = 0$ втрачає стійкість, а нова нерухома точка стає стійкою. При цьому, із збільшенням α виникають коливання. Управляючий елемент буде видавати по черзі два рішення. При подальшому збільшенні α виникають наступні біфуркації подвоєння періоду за сценарієм Фейгенбаума та детермінований хаос.

Тепер розглянемо найпростішу модель циклового інформаційного процесу управління, який складається з двох етапів:

- аналізу інформаційного потоку даних ВППЗ (відбір потрібної інформації, редукція, консолідація, переробка) – x_{in}. Інтенсивність дискретного інформаційного потоку управляючого елемента цього етапу позначимо за x;

- прийняття рішень та обробки вихідного інформаційного потоку для корекції заходів захисту (формування та видача управлінського рішення) – x_{out}. Інтенсивність дискретного інформаційного потоку управляючого елемента цього етапу позначимо за y.

Врахуємо прямі та зворотні зв’язки між управляючими елементами циклу за допомогою коефіцієнтів двох типів.

Коефіцієнти p, q характеризують синтаксичну обробку інформації (формати, списки, таблиці тощо). Коефіцієнти k_{ij} характеризують семантичну обробку інформації, коли робляться висновки, нові рішення, виникає нова інформація. Після простих перетворень наша математична модель динамічної системи $\Phi(x, y)$ приводиться до такого вигляду:

$$\Phi\left(x, y\right) = \begin{cases} x_{n+1} = x_n - k_{xy} p x_n^2 + k_{yx} q y_n^2 + x_{in} \\ y_{n+1} = y_n + k_{xy} p x_n^2 - \left(k_{yx} + k_{out}\right) q y_n^2 \end{cases}, \tag{4}$$

де x, y – динамічні змінні, які визначають інтенсивність інформаційних елементів

потоку на етапах обробки інформації; k_{ij} – перехідні коефіцієнти, що характеризують динамічну взаємодію етапів обробки інформації; p, q – розподільчі коефіцієнти, x_{in} – інтенсивність інформаційних елементів потоку, що поступають на перший етап обробки; причому, $\{k_{ij}\}$ и $\{p, q\} \in (0,1)$, $\{x, y\} \in R$, $x_{in} = const \in R^+$.

Наявність у системі двох груп коефіцієнтів (k_{ij} та p, q) має конкретну фізичну інтерпретацію: коефіцієнти k_{ij} описують відносну величину редукції і консолідації інформації за синтаксичними ознаками, наприклад, форматами відомостей і повідомлень, та задають долю інформаційного потоку, який переходить з одного етапу на сусідній. Частина інформаційного потоку переходить на попередній етап обробки для виправлення неточностей, врахування зауважень тощо. Коефіцієнти p, q описують розподіл елементів інформаційного потоку за їх видами по семантичним ознакам, наприклад, за змістом. Перехід між етапами обробки у нелінійній системі визначається добутком коефіцієнтів обох груп.

Методи дослідження дискретних відображень проаналізовані у численних публікаціях [22, 21]. Напрямком подальших досліджень є дослідження поведінки динамічної системи та вироблення рекомендацій щодо частоти процедур та тривалості циклу вдосконалення переліку проектних загроз.

Висновки

Створена синергійна модель проектних кіберзагроз ядерної безпеки АС та динамічна математична модель циклічних процесів вдосконалення переліку загроз із врахуванням нових пріоритетів інформаційної, кібернетичної та ядерної безпеки. Складено синергійний перелік кіберзагроз із урахуванням цільової неперервної діяльності підприємства, особливостей вразливостей об’єктів ядерної сфери та кращих практик, технік і технологій безпеки. Розроблена дискретна математична модель вдосконалення переліку проектних кіберзагроз. Напрямом подальших досліджень *планується* знаходження емерджентних властивостей системи оцінки ризиків безпеки на основі синергійної моделі проектних загроз та виведення узагальненого синергійного показника безпеки.

Список використаних джерел

1. НП 306.2.141-2008. Загальні положення безпеки атомних станцій / Норми та правила з ядерної та радіаційної безпеки. – К.: Державний комітет ядерного регулювання України. – 2008. – 62 с.

2. НП 306.2.202-2015. Вимоги з ядерної та радіаційної безпеки до інформаційних та керуючих систем, важливих для безпеки атомних станцій. – К.: Державний комітет ядерного регулювання України. – 2015. – 42 с.;

3. Кибербезопасность гражданских ядерных объектов: оценка угрозы и пути ее преодоления / ПИР-центр // Индекс безопасности № 3 – 4 (118-119) том 22. – С. 63 – 78. (Кибербезопасность гражданских ядерных объектов: оценка угрозы и определение дальнейших шагов / Резюме доклада ПИР-центра на ВЭФ. Москва – Женева, 2016. 4 с. – Режим доступа: pircenter.org/media/content/files/13/14875347670.pdf.)

4. Лукацкий Евгений. Кибербезопасность ядерных объектов / Евгений Лукацкий // Индекс безопасности – № 4 (115), – Том 21. – С 113 - 126.

5. Бурлаков В. М. Модель гармонізованого стандарту захисту інформації в системах управління ресурсами підприємства / В. М. Бурлаков, О. О. Кернасовська // «АСАУ», № 12’(32), 2008. – С. 16 – 24.

6. Бірюков Д. С. Вплив сучасних кіберзагроз на ефективність систем фізичного захисту критично-важливих об’єктів та інфраструктури / Д. С. Бірюков, В. М. Бурлаков // «АСАУ», № 21’(41), 2012. – С. 9 – 17.

7. NST045 (Комп’ютерна безпека для фізичної ядерної безпеки) Computer security for nuclear security, IAEA Nuclear Security Series No. XX 1, IAEA, Vienna, DRAFT, 2016. – 76 p. (Документ переглядає та уточнює NSS 17).

8. NST047 (Методи комп’ютерної безпеки для ядерної безпеки) Computer security techniques for nuclear facilities, IAEA Nuclear Security Series No. XX 1, IAEA, Vienna, DRAFT, 2017. – 124 p.

9. Евсеев С. П. Модель нарушителя прав доступа в автоматизированной банковской системе на основе синергетического подхода / С. П. Евсеев // Науково-технічний журнал «Інформаційна безпека». – Сєвєродонецьк. – 2017.- №2(26). – С. 110 – 120.

10. Евсеев С. П. Методология оценивания безопасности информационных технологий автоматизированных банковских систем Украины / Сергей Евсеев // Украинский научный журнал информационной безопасности. 2016, том 22, вып. 3. – С. 297 – 309.

11. Ястребенецький М.О. Методика оцінки відповідності інформаційних і керуючих систем, важливих для безпеки атомних станцій, вимогам з ядерної та радіаційної безпеки / ГНД. 306.7.02/2.041-2000. – К.: Мін. екології та природних ресурсів України. – 2000. – 43 с.

12. МАГАТЭ SSR-2/1. Безопасность атомных электростанций: Проектирование. Конкретные требования безопасности // Серия норм безопасности МАГАТЕ № SSR-2/1. – МАГАТЭ: Вена, 2018. – 116 с.

13. Park J. A Development Framework for Software Security in Nuclear Safety Systems: Integrating Secure Development and System Security Activities / Jaekwan Park, Yongsuk Sun // Nuclear Engineering find Technology, Vol. 46 No.1 February, 2014. – P. 47-54. https://www.sciencedirect.com/science/article/pii/S1738573315300899.

14. Secure Computer Systems Essential to Nuclear Security, Conference Finds (Press Release) // International Atomic Energy Agency. 8 June 2015. – 3 p. – Режим доступу: https://www.iaea.org/newscenter/news/secure-computersystems-essential-nuclear-security-conference-finds.

15. Михайлова Ольга. Киберугрозы и физическая ядерная безопасность / Михайлова Ольга // Индекс безопасности – № 1 (116), – Том 22. – С 93 - 106.

16. МАГАТЭ (INFCIRC/225/Revision 5). Рекомендации по физической ядерной безопасности, касающиеся физической защиты ядерных материалов и ядерных установок. Рекомендации / Серия изданий по физической ядерной безопасности, № 13. МАГАТЕ № SSR-2/1. – МАГАТЭ: Вена, 2012. – 88 с.

17. Кононович В.Г. Нелінійні моделі циклічного управління кібербезпекою / В. Г. Кононович, І. В. Кононович, А. І. Міхова // «Інформаційні управляючі системи та технології» (ІУСТ – ОДЕСА – 2015). Матеріали Міжнародної науково-практичної конференції, 22 – 24 вересня 2015 р., Одеса / відп. ред. В. В. Вичужанін. –, 2015. (– 336 .с). – С. 171 – 173.

18. Кононович В. Г. Модель системы информационной безопасности консолидированной информации при информационном противоборстве (Раздел 16) / В. Г. Кононович, И. В. Кононович // Информационные технологии и защита информации в информационно-коммуникационных системах: монография / под редакцией В. С. Пономаренко – Х.: Вид-во ТОВ «Щедра садиба плюс», 2015. (– 486 с.) – С. 220 – 233.

19. Информационная безопасность системы организационного управления. Теоретические основы: в 2 т. / Н. А. Кузнецов, В. В. Кульба, Е. А. Микрин и др.; [отв. ред. Н. А. Кузнецов, В. В. Кульба]; Ин-т проблем передачи информ. РАН. – М.: Наука, 2006. Т. 1 – 495 с.

20. М. Фейгенбаум Универсальность в поведении нелинейных систем. (Feigenbaum M. J. Universal Behavior in Nonlinear Systems. — Los Alamos Science. 1980, v. 1, No. 1, pp. 4–27.) Перевод С. Г. Тиходеева. http://ega-math.narod.ru/Nquant/Feigen.htm#note.

21. Малинецкий Г.Г. Математические основы синергетики. Хаос, структуры, вычислительный эксперимент. / Г.Г. Малинецкий. – М.: КомКнига, 2005. – 312 с.

22. Табор М. Хаос и интегрируемость в нелинейных системах / Табор Михал. Пер. с англ. – М.: Эдиториал УРСС, 2001. – 320 с.