and Applications, Symposium on Interactive and Collaborative Computing (ICC'2000). – Wollongong (Australia), 2000.
5. Wampserver 2.0 – http://www.wampserver.com/
6. Глибовець М. М. Розробка системи управління навчального закладу на прикладі НаУКМА / М. М. Глибовець, С. А. Іващенко, О. О. Крусь // Наукові праці: науково методичний журнал. Серія «Комп'ютерні науки». – Т. 57, Вип. 44. – Миколаїв: Вид-во МДГУ ім. Петра Могили, 2006. – С. 214–219.

D. Glomozda

COORDINATION OF USERS INTERACTION IN COLLABORATIVE DISTANT EDUCATION SYSTEM FOR HIGHER EDUCATIONAL INSTITUTION

A prototype of a system connecting an automated educational institution management system with a learning management system is described. Principles of practical implementation of floor control technology to coordinate these systems' users' actions are demonstrated.

УДК 519.8

Бірюков Д. С., Заславський В. А., Євгієнко В. В., Франчук О. В.

МОДЕЛЮВАННЯ ТА ОЦІНКА СЦЕНАРІЇВ ЗАГРОЗ ДЛЯ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

В роботі запропоновано математичну модель сценаріїв загроз для об'єктів критичної інфраструктури та алгоритми оцінки імовірності здійснення загроз.

Сталий розвиток всіх сфер життєдіяльності держави і суспільства безпосередньо залежить від безпеки об'єктів критичної інфраструктури (ОКрІС), вразливість яких протягом останнього десятиріччя стрімко зростає [1]. Причиною є, з одного боку, об'єктивні тенденції розвитку сучасних складних технічних систем (збільшення масштабу, зростання структурної складності, зміна організаційних та виробничих факторів), в таких науковомісних галузях, як енергетика, обчислювальна техніка та телекомунікації, а з іншого – посилення соціальної та економічної залежності від якості, надійності та безпеки функціонування ОКрІС. Також негативно впливає на ситуацію економічна криза, яка спричинила гострий дефіцит фінансових ресурсів. В ряді публікацій за останні роки, наприклад [2, 3], підкреслюється необхідність розвитку методології розв'язання задач аналізу та синтезу безпечних ОКрІС.

У зв'язку з активізацією тероризму в різних сферах діяльності виникає необхідність перегляду заходів та розробки нових підходів до забезпечення системної безпеки, створення фізичного захисту об'єктів критичної інфраструктури, впровадження нових методів контр-тероризму [4–8].

Міжнародний досвід у використанні проектної загрози для захисту об'єктів критичної інфраструктури ґрунтується головним чином на досвіді захисту ядерних матеріалів і ядерних установок та відображений у документах МАГАТЕ, а також державних установ [9–11]. Загальні підходи, сформовані для ядерної галузі, можуть також бути застосовані до інших об'єктів, які потребують високого рівня впевненості у тому, що їх захист є ефективним. Таким чином, високу практичну важливість має створення методів і засобів формалізації та структуризації процесів розробки, оцінки проектної загрози на основі ймовірнісних методів для подальшого формування фізичного захисту об'єктів критичної інфраструктури.

Метою роботи є представлення математичних засобів опису сценаріїв загрози та ймовірнісної оцінки реалізації загроз.

Проектна загроза як об'єкт для подальшої формалізації та структуризації

Важливими об'єктами критичної інфраструктури є АЕС та об'єкти ядерно-енергетичної галузі. Створюючи їх, розробники усвідомлювали необхідність побудови ефективного фізичного захисту, оскільки інциденти та зловмисні дії (здійснення диверсії або розкрадання ядерних матеріалів, радіаційних джерел, радіоактивних речовин, радіоактивних відходів) стосовно цих об'єктів можуть стати причиною цілої низки негативних і навіть катастрофічних наслідків.

Технологія дослідження загроз об'єктам ядерної галузі передбачає створення проектної загрози – документа, в якому наведено властивості та характеристики потенційних внутрішніх і/або зовнішніх порушників, які могли б здійснити спробу несанкціонованого вилучення ядерного матеріалу або диверсії, для протидії яким проектується й оцінюється система фізичного захисту.

У документах МАГАТЕ [11] вказується, що оцінка загрози – це процес аналізу, в результаті якого у документальній формі фіксуються ймовірні мотивації, наміри та можливості потенційних порушників, дії яких могли б викликати небажані наслідки чи для ядерного матеріалу під час його використання, зберігання та транспортування, чи для ядерних установок. Таким чином, оцінка загрози має імовірнісний характер, а отже прийняття рішень щодо проектної загрози і формування фізичного захисту здійснюється в умовах ризику, беручи до уваги імовірнісну оцінку здійснення протиправних дій з боку порушників. Значимість протиправних дій також характеризується їх наслідками, тобто рівнем впливу на інтереси населення, держави, ключових груп та міжнародного співробітництва.

Проблема убезпечення ОКрІС

Для задач убезпечення ОКрІС характерними є такі риси.

Представлення об'єкта (КрІС і окремих ОКрІС) та предмета (сценарії загроз, системи фізичного захисту, фактори і об'єкти, що впливають на безпеку КрІС) дослідження *у вигляді системи* з виділенням *структури і взаємозв'язків* між елементами. ОКрІС є крупномасштабними системами зі складною внутрішньою структурою і належать до таких ключових галузей, як державне управління, оборона, енергетика, промисловість, телекомунікації, транспорт, охорона здоров'я, фінансово-банківська система.

Для ОКрІС все частіше застосовується термін «системи, що складаються з систем», що означає необхідність створення багаторівневих ієрархічних моделей, які дають змогу використовувати, як складові, вже існуючі моделі. Інтеграція реальних систем приводить до інтеграції їхніх моделей безпеки. Прикладом реалізації такої побудови моделі є ієрархічна структура і багаторівнева вкладеність, використана в роботі [9].

Високий рівень взаємозв'язку окремих інфраструктур і ОКрІС, що наглядно продемонстровано в [10], де на прикладі студентського містечка Массачусетського інституту технологій (Massachusetts Institute of Technology) показано, що найбільш проблемні точки можуть залишитись непоміченими, якщо інфраструктури розглядаються окремо.

Невизначеність. Аналіз безпеки здійснюється на основі логіко-імовірнісних методів, а для окремих ОКрІС, наприклад, АЕС, розроблено і успішно застосовується спеціальне програмне забезпечення [14]. Характерною особливістю терористичних загроз є «непередбачуваність» сценарію атаки, відсутність статистичних даних і розуміння логіки дій терористів [4–6].

Прийняття рішень в реальному часі. Виникнення нових загроз потребує безперервних інформаційного моніторингу ситуації, підтримки процесів прийняття і узгодження рішень в умовах обмежених ресурсів, розв'язання задач із убезпечення в реальній обстановці, зважаючи на активізацію негативних дій [0].

Також проблема убезпечення ОКрІС пов'язана з *високою ціною відмови*, що потребує введення надлишкових елементів у структуру системи, забезпечення диверсифікації ризику і парирування відмов «з загальної причини» на основі багатоверсійних технологій і різнотипного резервування [15, 16].

Моделювання сценаріїв загроз ОКрІС

В даному параграфі для дослідження безпеки складних систем різної природи (СС) запропоновано модель складної системи, що складається з неоднорідних (таких, що мають неідентичні множини станів) елементів з багатьма станами (СНБС), та алгоритм обчислення імовірнісних показників стану СНБС за заданими показниками елементів (за фіксованої реалізації побудови підсистем).

Безпека розглядається як властивість системи і може характеризуватись (як якісно, так і кількісно) рядом показників, залежно від природи системи.

Об'єктом дослідження є СС (системи взаємопов'язаних факторів). Предмет дослідження – засоби дослідження та убезпечення.

Необхідно зазначити, що безпека ОКрІС характеризується станом об'єкта (системи). На практиці часто виділяють скінченне число станів (рівнів якості виконання функціональних задач, а також можливі режими відмов). Такий підхід

призводить до використання моделей структурно-складних систем, що складаються з неоднорідних (таких, що мають неідентичні множини станів) підсистем та елементів (СНБС). Алгоритм обчислення імовірнісних характеристик СНБС запропоновано в [16].

Побудова моделі здійснюється шляхом виконання таких кроків:

– визначення елементів сценаріїв (елементи, що мають потенційний вплив на реалізацію загрози);
– визначення множини можливих станів таких елементів;
– формування *сценаріїв* загрози (визначення ланцюгів, що складаються з пар: «елемент – заданий стан»), які призводять до реалізації загрози;
– формування *графу сценаріїв загроз* (структура, що включає всі сценарії);
– оцінка ймовірностей станів елементів;
– оцінка ймовірності реалізації сценаріїв загроз.

Для опису *загрози* використовується модель системи із елементів з багатьма станами.

Визначаються елементи, які входять до сценаріїв загроз (елементи, суттєві з точки зору безпеки). Це можуть бути люди (терористичні групи, обслуговуючий персонал, військові тощо), засоби захисту (сервер, програмне забезпечення) та інші об'єкти, що впливають (можуть вплинути) на реалізацію загрози. Позначимо множину таких елементів $I = \{1, 2, ..., n\}$.

Визначаються можливі значення стану елементів $i \in I$, що впливають на стан загрози. Нехай для елемента $i \in I$ визначено m_i (задане скінчене число) різних станів, що впливають на реалізацію сценарію загрози. Позначимо множину станів елементу $i \in I$ через $S_i = \{s_i^{(1)}, s_i^{(2)}, ..., s_i^{(m_i)}\} \subset \mathbb{N}$. Для кожного елементу $i \in I$ множина S_i містить індекси, яким відповідають властиві для даного елементу стани безпеки (небезпеки).

Припускається, що стан елементу $i \in I$ описується дискретною випадковою величиною x_i. Позначимо $p_i^{(s)}$ – ймовірність перебування елементу $i \in I$ в стані $s \in S_i$, тобто, $p_i^{(s)} = \mathrm{P}\{x_i = s\}$, $s \in S_i$.

Припущення

– величини x_i, $i \in I$ стохастично незалежні;
– ймовірності $p_i^{(s)} = \mathrm{P}\{x_i = s\}$, $s \in S_i$ задані.

Формування одиничних сценаріїв загрози

Умови реалізації загрози будемо описувати *сценарієм* – множиною пар «елемент – стан».

Для графічного позначення елементів сценарію будемо використовувати такий спосіб (рис. 1).

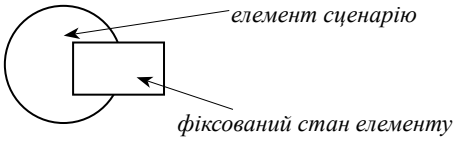

Рис. 1. Схематичне позначення елементу сценарію

Таким чином, проводячи паралель з визначенням ПЗ: «потенційні правопорушники» – елементи сценарію, а «характеристики потенційних правопорушників» – певні значення стану елементів сценарію, за яких сценарій реалізується.

Сценарій – множина пар: вершина графу, певне (фіксоване) значення змінної, що відповідає вершині (рис. 2).

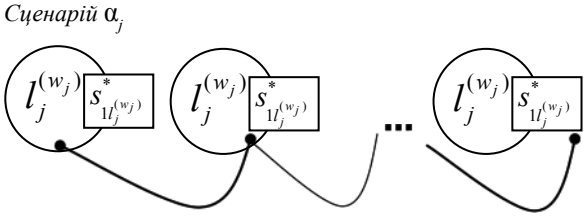

Рис. 2. Схематичне позначення сценарію

Визначається набір сценаріїв, що призводять до реалізацій загрози. Позначимо $\alpha_j, j \in J = \{1, 2, ..., h\}$ – сценарії. Тоді $\alpha_j = \{(i, s_{ij}^*)\}_{i \in I_j}$, де $I_j = \{l_j^{(1)}, l_j^{(2)}, ..., l_j^{(w_j)}\} \subseteq I$ – множина вершин графу, які задіяні в сценарії α_j, а s_{ij}^* – фіксоване значення змінної x_i для сценарію α_j.

Логічна умова реалізації загрози за сценарієм α_j може бути подана у вигляді наступної ФАЛ:

$$\bigcap_{i \in \alpha_j} \mathrm{I}_{[x_i = s_{ij}^*]}. \qquad (1)$$

Логічна умова реалізації всіх загроз за набором сценаріїв $\{\alpha_j\}_{j \in J}$, може бути подана у вигляді наступної ФАЛ:

$$f(x_1, x_2, ..., x_n) = \bigcup_{j \in J} \bigcap_{i \in \alpha_j} \mathrm{I}_{[x_i = s_{ij}^*]}. \qquad (2)$$

Функція $f(x_1, x_2, ..., x_n)$ приймає значення 1, якщо хоча б один сценарій реалізовано, і значення 0, якщо, відповідно, жоден сценарій не реалізовано. Тоді ймовірність реалізації хоча б одного сценарію загрози може бути записана у вигляді:

$$\mathrm{P}\{f(x_1, x_2, ..., x_n) = 1\} = \mathrm{P}\{\bigcup_{j \in J} \bigcap_{i \in \alpha_j} \mathrm{I}_{[x_i = s_{ij}^*]}\}. \qquad (3)$$

Сценарії утворюють систему зі складною структурою, оскільки одні і ті самі елементи входять до декількох сценаріїв.

Формування комплексного сценарію загрози

Структуру системи будемо задавати графом $G = (V, E)$, де множина вершин $V = \{v_i, i \in I\}$

відповідає елементам сценаріїв, множина ребер $E=\{(v_j,v_i),\ j\in I_i^0,\ i\in I\}$ – зв'язкам між елементами сценаріїв.

Оцінка ймовірності здійснення сценаріїв загроз ОКрІС

З метою перетворення ФАЛ заданої у вигляді в ІФ необхідно провести логіко-ймовірнісні перетворення, застосувавши алгоритм розрізання [7].

$$\begin{aligned}\mathrm{P}\{f(x_1,x_2,...,x_n)=1\}&=1-\mathrm{P}\{\overline{\bigcup_{j\in J}\bigcap_{i\in\alpha_j}\mathrm{I}_{[x_i=s_{ij}^*]}}\}=\\&=1-\mathrm{P}\{\overline{\bigcap_{j\in J}\bigcap_{i\in\alpha_j}\mathrm{I}_{[x_i=s_{ij}^*]}}\}.\end{aligned}\qquad(4)$$

Позначимо $K=\{k_1,k_2,...,k_r\}\subseteq I$ – множина елементів, що входять одночасно в декілька сценаріїв. Таким чином сценарії є взаємозалежними, і справедливим буде:

$$\begin{aligned}&\mathrm{P}\{f(x_1,x_2,...,x_n)=1\}=1-\mathrm{P}\{\bigcap_{j\in J}\overline{\bigcap_{i\in\alpha_j}\mathrm{I}_{[x_i=s_{ij}^*]}}\}\neq\\&\neq 1-\prod_{j\in J}\mathrm{P}\{\overline{\bigcap_{i\in\alpha_j}\mathrm{I}_{[x_i=s_{ij}^*]}}\}=1-\prod_{j\in J}(1-\prod_{i\in\alpha_j}\mathrm{I}_{[x_i=s_{ij}^*]}).\end{aligned}$$

Верхня та нижня оцінки ймовірності сценарію загрози

Обчислення верхньої та нижньої границі для ймовірності здійснення загрози здійснюються з застосуванням мінімальних шляхів та розрізів графу сценаріїв загроз.

Нехай маємо h^* перерізів графу $G=(V,E)$, які позначено β_h, $h\in H=\{1,2,...,h^*\}$. Нижня границя може бути отримана з нерівності:

$$\begin{aligned}\mathrm{P}\{f(x_1,x_2,...,x_n)=1\}&\geq\prod_{h\in H}(1-\mathrm{P}\{\overline{\bigcap_{i\in\beta_h}\bigcap_{s\in S_i^+}\mathrm{I}_{[x_i=s]}}=1\})\geq\\&\geq\prod_{h\in H}\Big(1-\prod_{i\in\beta_h}\mathrm{P}\{\mathrm{I}_{[x_i=s,\,s\in S_i^+]}=0\}\Big)=\\&=\prod_{h\in H}\Big(1-\prod_{i\in\beta_h}(1-\prod_{s\in S_i^+}\mathrm{P}\{x_i=s\})\Big),\end{aligned}\qquad(5)$$

де $S_i^+=\{s\in S_i\mid(i,s)\in\alpha_j\}$.

Верхня границя обчислюється з використанням сценаріїв $\alpha_j, j\in J$:

$$\begin{aligned}\mathrm{P}\{f(x_1,x_2,...,x_n)=1\}&\leq 1-\prod_{j\in J}(1-\mathrm{P}\{\bigcap_{i\in\alpha_j}\mathrm{I}_{[x_i=s_{ij}^*]}=1\})\leq\\&\leq 1-\prod_{j\in J}\Big(1-\prod_{i\in\alpha_j}\mathrm{P}\{\mathrm{I}_{[x_i=s_{ij}^*]}=1\}\Big)=\\&=1-\prod_{j\in J}\Big(1-\prod_{i\in\alpha_j}\mathrm{P}\{x_i=s_{ij}^*\}\Big).\end{aligned}\qquad(6)$$

Оцінки (5) та (6) швидко обчислюються, і є корисними за великої кількості сценаріїв з елементами, що повторюються.

Імітаційне моделювання

Оцінку ймовірності здійснення загрози можна отримати, використавши метод імітаційного моделювання Монте-Карло [14] та наступний рекурсивний алгоритм обходу графу сценаріїв загрози $G=(V,A)$. Процедура обходу запускається при $i=n+1$ і має вигляд:

Крок 1. Для вершини e_i виконати крок 2.

Крок 2. Для всіх вершин e_k, $k\in I_i^0$ виконати крок 3, якщо $I_i^0=\varnothing$, то перейти на крок 4.

Крок 3. Якщо для елементу, що відповідає вершині e_k ще не обчислені $\pi_k^{(s)}(x_k(t),t)$, $t\in\mathrm{T}$, $s\in\Xi_k$, то запустити виконання процедури для вершини e_k.

Крок 4. Обчислити імовірнісні характеристики $\pi_i^{(s)}(x_i(t),t)$, $t\in\mathrm{T}$, $s\in\Xi_i$, стану виходу підсистеми $i\in I$.

Точне значення ймовірності сценарію загрози

Використавши алгоритм розрізання відносно основного елементу [7], обчислюються точні значення ймовірності здійснення загрози.

Застосувавши формулу повної ймовірності, можемо представити ймовірність події «всі сценарії не реалізовані» у вигляді

$$\begin{aligned}\mathrm{P}\{f(x_1,x_2,...,x_n)=0\}&=\sum_{s_1\in S_{k_1}}\sum_{s_2\in S_{k_2}}...\sum_{s_r\in S_{k_r}}\prod_{k\in K}\mathrm{P}\{x_k=s_k\}\cdot\\&\cdot\mathrm{P}\{f(x_1,x_2,...,x_n)=0\mid x_k=s_k,k\in K\}.\end{aligned}$$

Використавши перетворення з формули (3) запишемо:

$$\begin{aligned}&\mathrm{P}\{f(x_1,x_2,...,x_n)=0\}=\\&=\sum_{s_1\in S_{k_1}}\sum_{s_2\in S_{k_2}}...\sum_{s_r\in S_{k_r}}\prod_{k\in K}\mathrm{P}\{x_k=s_k\}\cdot\\&\cdot\mathrm{P}\{\bigcap_{j\in J}\overline{\bigcap_{i\in\alpha_j}\mathrm{I}_{[x_i=s_{ij}^*]}}=1\mid x_k=s_k,k\in K\}.\end{aligned}$$

Важливість елементів сценарію вплив на здійснення загрози

Елементи сценарію по-різному впливають на його здійснення. Важливість кожного з елементів корисно оцінити кількісно. Для цього пропонується використати таку формулу обчислення:

$$w_i=\frac{\sum_{s\in S_{ij}^*}\mathrm{P}\{f(x_1,x_2,...,x_n)=1\mid x_i=s\}\mathrm{P}\{x_i=s\}}{\mathrm{P}\{f(x_1,x_2,...,x_n)=1\}}.$$

Таким чином, загальну схему етапів дослідження безпеки на основі моделі СБС можна показати у вигляді рис. 3.

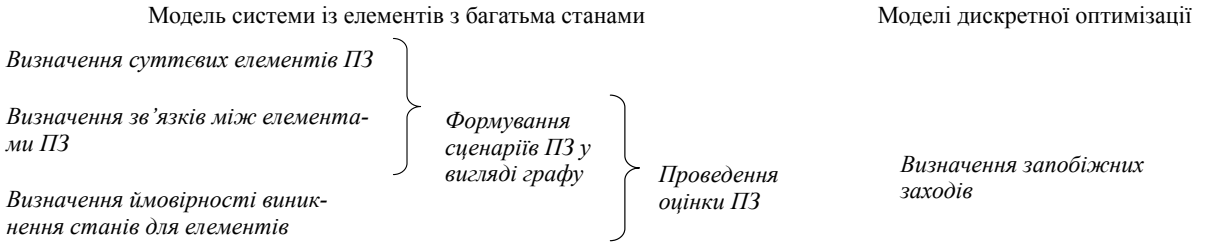

Рис. 3. Етапи дослідження в моделі безпеки

Висновки

Розв'язання задач моделювання сценаріїв загроз пов'язано з важливою практичною проблемою протидії тероризму.

В роботі запропоновано модель з багатьма станами для формалізації та оцінки проектної загрози. Розроблені та представлені методи логіко-імовірнісних перетворень для даної моделі. На основі розроблених математичних засобів здійснюється оцінка ймовірності реалізації загрози.

Безпеку недостатньо визначити на якісному рівні (висока, задовільна, низька і т. п.) – необхідно мати можливість оцінювати її кількісно для різних варіантів реалізації системи.

Варто наголосити:

- проектна загроза повинна бути структурованою (чітко описаною), що неможливо без залучення методів системного аналізу, математичних моделей та інформаційних технологій;
- імовірнісна оцінка проектної загрози може бути здійснена на основі застосування моделей систем із елементів з багатьма станами та логіко-імовірнісних методів;
- імовірнісна оцінка проектної загрози дасть змогу раціонально розподілити ресурси під час створення ефективних систем фізичного захисту.

1. Горбулін В. П., Качинський А. Б. Системно-концептуальні засади стратегії національної безпеки України / В. П. Горбулін, А. Б. Качинський. – К. : ДЦ «НВЦ» Євроатлантикінформ», 2007. – 592 с.
2. Johnson C.W. Understanding the interaction between public policy, managerial decision-making and the engineering of critical infrastructures // Reliab. Eng-ng & Sys. Safety. – 92(9). – 2007. – P. 1141–1154.
3. Kröger W. Critical infrastructures at risk: a need for a new conceptual approach and extended analytical tools / W. Kröger // Reliab. Eng-ng & Sys. Safety. – 93(12). – 2008. – P. 1781–1787.
4. Keeney R. L. Modeling values for anti-terrorism analysis / R. L. Keeney // Risk Analysis. – 27(3). – 2007. – P. 585 – 596.
5. Ushakov I. Counter-terrorism: protection resources allocation, part 2 / I. Ushakov // Reliability : Theory and Applications. – 2006. – No. 2. – P. 71–78.
6. Оценка террористического риска и принятие решений о целесообразности построения систем защиты от террористического воздействия / В. П. Петров, Д. О. Резников, В. И. Куксова и др. // Проблемы безопасности при чрезвычайных ситуациях : ОИ/ ВИНИТИ. – 2007. – Вып. 1. – С. 89–105.
7. Рябинин И. А. Надежность и безопасность структурно-сложных систем / И. А. Рябинин. – СПб. : Изд-во С.-Петерб. ун-та, 2007. – 276 с.
8. Соложенцев Е. Д. Сценарное логико-вероятностное управление риском в бизнесе и технике / Е. Д. Соложенцев. – СПб. : Бизнес-пресса, 2004. – 342 с.
9. Baiardi F. Hierarchical, model-based risk management of critical infrastructures / F. Baiardi, C. Telmon, D. Sgandurra // Reliab. Eng-ng & Sys. Safety. – 94(9). – 2009. – P. 1403–1415.
10. Patterson S. A. Identification of critical locations across multiple infrastructures for terrorist actions / S. A. Patterson, G. E. Apostolakis // Reliab. Eng-ng & Sys. Safety. – 92(9). – 2007. – P. 1183 –1203.
11. Оцінка загрози ядерного тероризму: проектна загроза / С. І. Кондратов, Ю. М. Скалецький, В. І. Кравцов та ін.; за заг. ред. акад. НАН України В. П. Горбуліна. – К. : ДП «НВЦ» Євроатлантикінформ», 2006. – 76 с.
12. Закон України «Про фізичний захист ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання» 19.10.2000, №2064-III.
13. Фізичний захист ядерного матеріалу та ядерних установок INFCIRC/225/Rev.4, МАГАТЕ, 1999.
14. Імовірнісний аналіз безпеки атомних станцій (ІАБ) : Навч. посібник / В. В. Бєгун, О. В. Горбунов, І. М. Каденко та ін. – К., 2000. – 568 с.
15. Многоверсионные системы, технологии, проекты / В. С. Харченко, В. Я. Жихарев, В. М. Илюшко, Н. В. Нечипорук; под. ред. В. С.Харченко. – Харьков : Нац. аэрокосм. ун-т «ХАИ», 2003. – 486 с.
16. Модели и алгоритмы оптимизации надежности сложных систем / В. Л. Волкович, А. Ф. Волошин, В. А. Заславский, И. А. Ушаков ; Под ред. акад. В. С. Михалевича. – К. : Наукова думка, 1992. – 312 с.
17. Бірюков Д. С. Про обчислення показників надійності складних системи з багатьма станами / Д. С. Бірюков // Вісн. Київ. ун-ту. Сер. : фіз.-мат. наук. – 2005. – Вип.3. – С. 193–199.

D. Biryukov, V. Zaslavskii, V. Evgienko, O. Franchuk

THREAD SCENARIOS MODELING AND ASSESSMENT FOR CRITICAL INFRASTRUCTURE

Mathematical model of thread scenarios for critical infrastructure facilities and algorithms for probabilistic assessment of thread realization are proposed.