УДК 004.942

МОДЕЛІ, МЕТОДИ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ДЛЯ СППР ЩОДО БЕЗПЕКИ

В.В. Бєгун, В.Ф. Гречанінов, А.О. Морозов
Институт проблем математических машин и систем НАН Украины
e-mail: begunw@ukr.net

Гаслом ДСНС є слоган: «Запобігти, врятувати, допомогти». Це гасло відображує глобальну стратегію рятувальних підрозділів у всьому світі. Нажаль, в Україні цей слоган поки тільки гасло, запобігти надзвичайні ситуації (НС) поки що не виходить. Щоб запобігти НС потрібно *навчитися* з усієї множини можливих НС, виділити найбільш імовірні, які можуть виникнути за обставин, що склалися на поточний час. З цього слідує простий висновок, що перехід на технологію регулювання безпеки на основі принципів «запобігання» потребує якісного виконання 2-х процесів: *постійного моніторингу* та завчасного *прогнозування* виникнення можливих НС. Але, прогнозування можливе тільки на основі моделювання процесів, або на основі, знову ж таки, якісних експертних оцінок. Ось такий логічний ланцюжок й приводить до необхідності впровадження сучасних інформаційних технологій (ІТ) у сферу безпеки, створенню СППР тощо.

Технологія на основі принципів «запобігання» у тому чи іншому ступені впроваджена у більшості країн світу, описана у багатьох наукових працях [1-6], повністю впроваджена й в Україні у ядерній галузі. Її ефективність доведена наукове й практично, вона базується на парадигмі ризик-орієнтованого підходу (РОП) й може бути реалізована з невеликими фінансовими витратами в усіх галузях виробництва та, навіть, для запобігання природних катастроф [5-6]. Перешкоди її впровадження у нашій державі розглянуті у [7], основна з них пов’язана з корупційною складовою та недоліками освіти з напряму безпеки. Так, поняття «моделі безпеки» поки що відсутнє у наших навчальних програмах ВНЗ, на відміну скажімо США, де посібник з цього напряму впроваджено наприкінці 70-х років минулого століття [8]. Відсутня й практика погодження посібників цього напряму з ДСНС, точніше відмінена з початку 2000-х років.

Отже, моделі безпеки – необхідна умова створення ІТ з безпеки. Розглянемо деякі вимоги та особливості таких моделей. В першу чергу, має вирішуватися питання щодо типу моделей: якісна, кількісна – детерміністична, імовірнісна, імітаційна та ін. Питання далі – який метод має бути використано для моделювання, невизначеності методу та спосіб їх оцінок, точність та адекватність моделі. З розвитком ІТ великим помічником авторів стають інтернет-пошукові системи, типу «Google». Будь яка бажаюча людина одним кліком може знайти сотні-тисячі сторінок інформації з теми, що цікавіть. Але *інформація не є знанням*, й, у цьому існує не тільки користь, але й величезна небезпека. Людина – автор, думає що щось знає з теми, робить публікацію, чи, навіть, «монографію», не замислюючись над процесом, з причин його складнощі та незнання деталей чи обставин. Прикладів таких чимало. Наприклад, у сфері охорони праці (це безпека на виробництві) є «вчений» на особистому рахунку якого біля 200 монографій й навчальних посібників з різних галузей виробництва і знань! За його особистим висловлюванням, він може потрапити у Книгу Рекордів Гіннеса як самий плідний «вчений» світу! На наш погляд, цього не може бути, тому що протирічить просто здоровому глузду, це безвідповідальність та безкарність. Ще приклад – у минулому році викладач Інституту харчових технологій успішно (!) захистив дисертацію з питань технологічного контролю параметрів турбогенератора АЕС й т.і. Нажаль, такими є реалії нашої держави, тому стосовно моделювання процесів безпеки в Україні потрібно висунути ще одну

обов'язкову вимогу – *компетентність автора щодо безпеки*. Так, у світовій практиці ядерної галузі є вимоги до експерта (фахівця): вища спеціальна освіта, досвід роботи за напрямом й ліцензія або науковий ступінь. Але ж, у більшості випадків інших галузей, це ігнорується, й, це ще більша небезпека, ніж помилка фахівця чи, навіть уся небезпека, що моделюється. Наслідком некомпетентної моделі є омана, що може призвести до катастрофи. До речи, катастрофа ЧАЕС розпочалася з програми «випробувань», розробленою «науковцями» інституту з Донецька (Донтехенерго).

Другим питанням щодо моделей з безпеки є вибір методології та методу. Так, після затвердження концепції РОП [9] та плану її впровадження [10], в Україні почали з'являтися методики з визначення рівня ризику вже нормативно, чи навіть законодавчо, затверджені . Наприклад, методики з визначення рівня ризику корупції, паводку [11], та інші засновані на методі FMEA (Failure Mode and Effects Analysis), або у перекладі «аналіз видів відмов та їх наслідків – АВВН» [12]. Перша методика офіційно затверджена ще у минулому році, але не використовується, на наш погляд, саме з цієї причини – недосконалості методу. Насправді, метод FMEA частіше використовується як метод попереднього (якісного) аналізу, щоб визначити ризики категорій «А» та «В» з метою їх подальшого аналізу іншим методом. Наступним недоліком цієї методики є невелика кількість градацій ризику – усього три діапазони, що навіть не відповідає стандарту. Це призвело до унеможливлювання її практичного застосування й, як наслідок, потреби нової розробки. До речи, на наш погляд, кожна сучасна офіційна методика повинна бути представлена з програмним забезпеченням (ПЗ), чого не має у наведених прикладах. Неможливо зробити адекватні оцінки за цією методологією, дуже великі невизначеності отримуємо у підсумку, що зводить нанівець весь аналіз. Отже, при виборі типу моделі стосовно методу FMEA може бути наступна рекомендація – цього аналізу достатньо, якщо результатом є знехтуваний або малий ризик, інакше потрібен більш детальний аналіз.

Також, дуже важливим є питання вибору типу методу моделювання: детерміністичний – ймовірнісний. Помилки цього типу можуть мати найбільш фатальний наслідок, тому що дуже просто й непомітно губиться адекватність моделі. Фахівцям з безпеки добре відомий ГОСТ 12.3.047, де на основі світового досвіду зібрані найбільш адекватні моделі вибухонебезпечних процесів. Усі моделі детерміністичні, легко перетворюються у відповідне ПЗ (студенти роблять програми у якості лабораторних робіт), адекватність перевірена світовим досвідом, але ж чомусь не використовуються службами ДСНС. До речи, для більшості моделей цього стандарту ПЗ розроблено як для систем Windows, Linux, так й для Android. Тобто, скажімо, наслідки розливу цистерни небезпечної речовини є можливість порахувати як на стаціонарних комп'ютерах, так й на смартфонах. Але, часто простота моделі визиває недовіру, або спрощення призводить до неможливості показати «новизну». Зауважимо, що у вітчизняній практиці, також на вищому науковому рівні, є помилки й цього типу. Наприклад, розпад радіоактивних ізотопів моделюється ланцюгами Маркова, як цілком незалежні випадкові події, незважаючи на давно відомі таблиці радіоактивних перетворень, які розміщені на сайті МАГАТЕ.

Коли більшість подій, що характеризують процес, мають стохастичну природу, прийнято проводити аналіз на основі імовірнісної моделі. Імовірнісні моделі та імовірнісний аналіз безпеки (ІАБ) широко й порівняно давно використовуються у моделюванні безпеки складних систем, АЕС тощо [13]. Що стосується застосування методу у інших галузях, скажемо, медицині, то існують тільки окремі спроби. Розроблені моделі створені на основі «дерев відмов». Дерево відмов (ДВ) представляє собою

графічну модель різних паралельних та послідовних поєднань базисних подій (БП), що призводять до реалізації раніше визначеної небажаної події. З математичної точки зору це розімкнутій граф, вершинами якого є те чи інше сполучення подій. У техніці ДВ – це математичні ймовірнісні моделі систем, які враховують можливі відмови всіх елементів, що входять у систему, їх взаємозв'язок та взаємозалежність, та дозволяють розрахувати ймовірність відмови системи [13]. Моделювання технічних систем, навіть таких складних систем, як АЕС, дещо простіше, оскільки порівняно легко прослідити вплив кожної БП (відмови) на роботоздатність кожної підсистеми, в яку входять елементи, що моделюються. Ця обов'язкова процедура імовірнісного моделювання, звичайно виконується за допомогою згаданого методу FMEA. Процедура FMEA у цьому випадку – це якісний аналіз системи, що застосовується для визначення «впливових» подій, які обов'язково мають бути включені в імовірнісну модель ДВ, тобто у цьому випадку це попередній аналіз. Велике значення для імовірнісних моделей має статистика, на основі якої створюється саме моделі БП, визначається їх елементарна статистика, математичне очікування, закон розподілу, дисперсія тощо. Для моделей безпеки технічних систем, важливо враховувати світовий досвід, тобто використовувати Байєсовські оцінки.

Для моделювання можливих помилок людини (людський чинник - ЛЧ) у імовірнісних моделях звичайно використовується широко відома у техніці методологія THERP (Technique for Human Error Rate Prediction). Звісно, що ця методологія призначена для технічних систем, тому у роботах з моделювання інших систем роблять наступні припущення: 1) імовірність базової помилки (Human Error Probability - HEP) фахівця високої кваліфікації (вища спеціальна освіта, достатній досвід) має порядок: $P = 1 \cdot 10^{-3}$ та 2) помилки досвідчених фахівців у різних сферах діяльності відбуваються за схожими сценаріями. Підсумкова імовірність помилок залежить від інших факторів та обставин, як то: складність задачі, достатності часу, ергономіки робочого місця, рівня стресу та інше. Імовірність колективної помилки при роботі в бригаді також має моделюватися, що можливо за методологією THERP. Імовірності усіх подій, що враховуються у моделі розраховується на основі статистичних даних об'єкту, що моделюється, за припущенням нормального їх розподілу. Існують й інші методи моделювання ЛЧ, наприклад, на основі дерева рішень та інші. Вибір методу залежить від типу об'єкту та компетенції автора моделі, при цьому, вітчизняної методики не існує, хоча і є вимога обов'язковості моделювання ЛЧ у нормативних документах. Вітчизняного ПЗ для моделювання складних систем імовірнісними методами теж не існує. Ось такі наші реалії.

Про можливість створення саме СППР та ІТ з безпеки є також достатня кількість публікацій [2,4,14,15]. Більш того така спроба була ще на початку 2000-х [15], на комп'ютерах того покоління. Оскільки завдання, що ставилося затвердженою програмою не вирішено, маємо право стверджувати про допущені системні помилки, на наш погляд, з наведених причин. Саме з метою недопущення повтору, нові проекти [1-3,9,10] передбачають розроблення галузевих положень управління ризиком. При такому підході буде забезпечена їх достатня компетентність, передбачається публічне обговорювання проектів і методик управління ризиком, що, сподіваємось, частково виключить корупційну складову. Підтримка ЄС у наближенні до кращих європейських практик здійснюється по багатьох напрямах [5], освіти тощо, що також дає надію на сприятливе завершення розпочатих робіт.

Висновки. Впровадження сучасних ІТ у сферу безпеки в Україні дуже потрібне, давно пора розпочати проектування АСУ єдиної системи цивільного захисту з впровадженням кращій світової практики. Можливо потрібно затвердити на державному рівні вимоги щодо компетентності розробників, або/та процедури погодження методик

перед їх затвердженням. Кожна методика має бути з програмним забезпеченням. Відомо, що впровадження нової парадигми управління безпекою внесена в угоду про асоціацію, але створення системи тільки під примусом ЄС малоймовірне, потрібна добра воля Уряду.

Література

1. В.В. Бєгун, В.Ф. Гречанінов, В.П. Клименко, П.П. Кропотов. Галузеве керівництво з розробки та реалізації політики управління ризиками. Збірник тез II-ої Міжнародної науково-практичної конференції "Актуальні проблеми моделювання ризиків і загроз виникнення надзвичайних ситуацій на об'єктах критичної інфраструктури" 26-28 травня 2016, Київ, Україна. - С. 195-201. [Електронне видання]. - Режим доступу: http://undicz.dsns.gov.ua/files/2016/8/31/Zbirnyk_tez_konferencii.pdf

2. Основи комплексної автоматизованої системи управління техногенною безпекою. Гречанінов В.Ф. Коробко А.Д. Сучасний стан цивільного захисту України: перспективи та шляхи до Європейського простору: матеріали 18 Всеукраїнської науково-практичної конференції рятувальників. − Київ: ІДУЦЗ, 2016. – С.-105-109.

3. Морозов А.О., Гречанінов В.Ф., Бєгун В.В. Управління безпекою в епоху інформаційного суспільства. Вісник НАН України, №10, 2015 р. С. 34-41.

4. Морозов А.О., Косолапов В.Л. Інформаційно-аналітичні технології підтримки прийняття рішень на основі регіонального соціально-економічного моніторингу. – К.: Наукова думка, 2002.

5. PPRD East 2 в Україні: http://pprdeast2.eu/en/strany-partnery/ukraine/.

6. Шевчук В.В., Іванік О.М. Комплексна методика моделювання впливу небезпечних геологічних процесів на функціонування трубопровідно-транспортних природно-техногенних систем. Патент України №42098 від 06.02.2012 р.

7. В. Бєгун. Основне призначення РОП - підтримувати ризики небезпечного об’єкту на прийнятному рівні. // Пожежна і техногенна безпека – К.: ДСНС України, 2017. - № 3. – С. 19-21.

8. Хенли Э. Дж., Кумамото Х. Надежность технических систем и оценка риска / Пер. с англ. Сыромятникова В.С., - М., 1984.

9. Розпорядження КМУ «Про схвалення Концепції управління ризиками виникнення надзвичайних ситуацій техногенного та природного характеру» від 23.01.2014 № 37 р. [Електронний ресурс]. – Режим доступу: http://www.mns.gov.ua

10. Розпорядження КМУ «Про затвердження плану заходів щодо реалізації концепції управління ризиками виникнення надзвичайних ситуацій техногенного та природного характеру». від 25.05.2015 № 419 р. [Електронний ресурс]. – Режим доступу: http://www.mns.gov.ua

11. Методологія оцінювання корупційних ризиків у діяльності органів влади. Затверджено Рішення Національного агентства з питань запобігання корупції 02.12.2016 № 126. Зареєстровано в Міністерстві юстиції України 28 грудня 2016 р. за № 1718/29848

12. ГОСТ 27.310-95. Надежность в технике. Анализ видов, последствий и критичности отказов. Основные положения.

13. Вероятностный анализ безопасности атомных станций / В.В. Бегун, О.В. Горбунов, И.Н. Каденко [и др.]. – К.: Випол, 2000. – 558 с**.**

14. О.Г. Додонов, О.В. Нестеренко, М.М. Будько. Архітектура автоматизованих інформаційно-аналітичних систем органів державної влади. Математичні машини і системи, 2003, № 3, 4, с.138-146

15. Програма створення Урядової інформаційно-аналітичної системи з питань надзвичайних ситуацій на 2000-2002 роки. Затверджено постановою Кабінету Міністрів України від 16 грудня 1999 р. N 2303.