https://orcid.org/0000-0002-0045-8586

УДК 004.02[004.9:614.8.084]

В.В. БЄГУН[*]

ЦИФРОВА ЕКОНОМІКА ТА ПИТАННЯ БЕЗПЕКИ ТРЦ УКРАЇНИ

[*]Інститут проблем математичних машин і систем НАН України, м. Київ, Україна

Анотація. *Аналізуються проблеми безпеки торговельно-розважальних центрів (ТРЦ) України та можливість і необхідність включення важливих питань безпеки у державну програму розвитку (цифрового) електронного урядування. Розглянуто стан розвитку електронного урядування в Україні, доведено, що рівень розвитку високий та значно покращився за два минулі роки і відповідає світовим вимогам сьогодення. З точки зору безпеки, розглянуто основні (найкращі) проєкти ТРЦ і на основі даних перевірок державних інспекцій із безпеки описані фактори та обставини ризику для персоналу й відвідувачів ТРЦ. Представлені моделі евакуації під час можливої пожежі й імовірнісна модель виникнення й поширення пожежі. Запропоновані варіанти програмного забезпечення для виконання розрахунків. Як правило, ці сучасні багатофункціональні центри обслуговування населення споруджуються в Україні за рахунок іноземних інвестицій, базуючись на нормах країн інвесторів. Але з причин невідповідності законодавчих основ виникають проблеми з безпеки персоналу та відвідувачів, хазяїв та державних інспекторів із контролю безпеки. Пропонується концепція контролю безпеки на основі даних із надійності систем безпеки об'єктів, яка легко реалізується на комп'ютері. Також розроблена концепція включення розроблених моделей та програм до складу програм державного електронного уряду, оскільки ТРЦ стають об'єктами масової культури з дуже великим числом щоденних відвідувань, яке буде зростати. Наприклад, ТРЦ «Магелан» у м. Києві до початку пандемії відвідувало 30000 людей щодня, ТРЦ «Ocean Plaza» – 60000. Це приблизно від 2 до 5 тисяч людей щогодини. Отже, у випадку пожежі може бути багато жертв, якщо не вдасться вчасно евакуювати людей або приборкати пожежу. Задля запобігання небажаних подій, статистика яких постійно збільшується, пропонується вирішення задач безпеки ТРЦ на сучасному науковому рівні ризик-орієнтованого підходу та сучасному інформаційному рівні. Розглянуто можливий варіант включення питань безпеки ТРЦ в інформаційні технології електронного уряду.*

Ключові слова: *ризик, торговельний центр, контроль безпеки, модель виникнення пожежі, евакуація, оптимізація періоду перевірок.*

Abstract. *The paper analyzes some security problems of several Ukrainian trade and entertainment centers, as well as the possibility and necessity of including important security issues in the state program for the development of e-governance (digital governance). The state of e-governance development in Ukraine has been considered. It has been proved that its level is high and has significantly improved over the past two years, and now meets today's global requirements. From the security point of view, the main (best) projects of trade and entertainment centers have been considered and risk factors and circumstances for the staff and visitors of shopping malls have been described on the basis of the data of inspections carried out by state security inspectorates. Some evacuation models to be used in the event of a fire and a probabilistic model of fire occurrence and spread are provided in the paper. Some software options for performing calculations are also offered. As a rule, these modern multi-functional service centers are built in Ukraine at the expense of foreign investments based on the norms of the investor countries. However, due to the inconsistency of the legal framework, there arise problems with the safety of staff and visitors, owners, and state security inspectors. The work proposes a concept of security control, which can be easily implemented on a computer, based on data on the reliability of object security systems. Since trade and entertainment centers having a large number of daily visits that will go on increasing are becoming mass culture objects, the concept of inclusion of the developed models and programs in the e-government programs has been developed. For example, before the beginning of the pandemic, the Magellan mall in Kyiv was visited by 30,000 people every day and the Ocean Plaza shopping center – by 60,000 people. This is approximately 2,000–5,000 visitors every hour. Therefore, in*

case of a fire, if people are not evacuated in time or the fire is not put out, there may be many victims. To prevent unwanted events whose statistics are constantly increasing, it is offered to solve the safety issues of trade and entertainment centers at the modern scientific level of the risk-oriented approach and the modern information level. The paper also considers a possible option of including security issues of shopping malls in the information technologies of e-government.
Keywords: *risk, shopping center, security control, fire occurrence model, evacuation, optimization of the inspection period.*

DOI: 10.34121/1028-9763-2023-1-60-71

1. Вступ

В Україні існують більше 300 великих торговельних (більш загальне – торговельно-розважальних) центрів (ТРЦ). ТРЦ – це об'єкт (велика будівля), що функціонує з метою побутового обслуговування населення, тому кількість відвідувачів складає до декілька тисяч на добу. Зазвичай це багатоповерхова будівля (8 поверхів – «Гулівер») або будівля великої площі (12,7 га – ТРЦ «Лавина»). ТРЦ будуються за міжнародними стандартами та проєктами. Питання безпеки, як правило, теж вирішені на світовому рівні, дещо з урахуванням національних особливостей інвесторів. У багатьох країнах за класифікацією безпеки вони навіть не попадають у категорію потенційно небезпечних об'єктів (ПНО), але в нашій державі за законодавством ТРЦ відносять до категорії ПНО за багатьма параметрами, як то: наявність легко займистих рідин та горючих газів, велика площа крівлі та ін. Тому навіть після завершення будівництва комплексу за законодавством України потрібно визначати ступінь небезпеки цих об'єктів для персоналу та населення. Потрібно це робити у межах впровадження та розвитку електронного уряду (ЕУ), як це вже зроблено в багатьох сферах життєдіяльності України й всього людства.

Метою статті є висвітлення проблем безпеки життєдіяльності, пов'язаних із функціонуванням нових, але багато розповсюджених в Україні об'єктів сучасної культури й побуту – великих торговельно-розважальних центрів та способів приведення (адаптації) їх функціонування у законодавче поле держави, можливості підтримки безпеки суспільства засобами сучасних цифрових технологій.

2. Аналіз стану розвитку електронного урядування в Україні

Процеси розвитку електронного урядування у XXI столітті вважаються настільки важливими, що ООН розробляє регулярні звіти з цього питання [1], оцінює стан розвитку усіх країн за спеціальними показниками, головний з яких EGDI (Electronic Government Development Index) – Індекс розвитку електронного уряду. EGDI є станом розвитку електронного уряду в державах-членах Організації Об'єднаних Націй (ООН). Поряд з оцінкою моделей розвитку веб-сайтів у країні, індекс розвитку електронного уряду включає характеристики доступу, такі як інфраструктура і рівень освіти, щоб відобразити, як країна використовує інформаційні технології для розширення доступу і залучення свого населення. EGDI є сукупним показником трьох важливих аспектів електронного уряду, а саме: надання онлайн-послуг, телекомунікаційний зв'язок та людський потенціал. Відповідно до звіту показники розвитку країни такі: 1. EGDI – Індекс розвитку електронного уряду (EGDI). 2. ІОП (OSI) – Індекс онлайн послуг. 3. ІТК (ТІІ) – Індекс телекомунікацій. 4. ІЛК (HCI) – Індекс людського капіталу. 5. Рейтинг – узагальнений показник, який вказує місце країни (табл. 1) серед країн світу. Показники 1–4 приймають значення у діапазоні від 0 до 1, мають сенс: чим більше, тим краще; показник 5 – рейтинг визначає місце країни серед 192 країн світу: чим менший, тим краще.

Таблиця 1 – Показники розвитку електронного уряду у 2020 році

Рейтинг	Країна	Регіон	EGDI 2020	ІОП (OSI)	ІТК (TII)	ІЛК (HCI)	Рівень доходу
40	Білорусь	Східна Європа	0,8084	0,7059	0,8281	0,8912	Вище середнього
20	Литва	Північна Європа	0,8665	0,8529	0,8249	0,9218	Високий дохід
53	Туреччина	Західна Азія	0,7718	0,8588	0,628	0,8287	Дохід вище середнього
69	Україна	Східна Європа	0,7119	0,6824	0,5942	0,8591	Дохід нижче середнього

Отже, за даними ООН, ми ще в 2020 році знаходилися серед тієї частини людства, де потрібно чимало зробити для досягнення сталого розвитку держави. Україна знаходилася у першій половині, але показники наших найближчих сусідів були значно кращі. Тобто у світі того ж таки президентського указу «Про країну у смартфоні» роботи було непочатий край. Створили платформу «Дія», де, за задумом, населення може отримати сотні електронних послуг. Найбільш розповсюджені були електронні розрахунки, якими користується переважна більшість українців. Інших повністю автоматизованих послуг не було. В 2022 році Україна перейшла у категорію «високій рівень» розвитку електронного уряду з загальним рейтингом 0,8029 й зайняла 46 місце (з 193 країн), тобто маємо значний приріст розвитку за 2 роки. Впроваджено багато нових сервісів цифрового урядування [2–4]:

• Запущено мобільний застосунок «Дія» – доступ громадян до цифрових документів.

• Створено та запущено Єдиний державний веб-портал електронних послуг – Портал «Дія» (diia.gov.ua).

• Запроваджено Е-систему у сфері будівництва, що має на меті максимальну автоматизацію та прозорість усіх процесів у галузі.

Розвиток цифрової індустрії у світі вимагає рухатися синхронно зі світовим суспільством, і, як бачимо, наша держава має добрі успіхи на шляху реформ щодо впровадження ЕУ. Як записано в основних документах [3], мета реформи – забезпечення доступу громадян і бізнесу до якісних та зручних публічних послуг без корупційних ризиків.

Важливість розвитку ЕУ підтверджує той факт, що це було питанням порядку денного саміту G-20, що пройшов в Індонезії восени 2022 року [4]. У підсумку документ саміту – Декларація складається з 52 пунктів з усіх напрямів діяльності людства. Матеріали саміту – документи: аналізи експертів, звіти, висновки з усіх сторін сучасного життя викладено на 1186 сторінках. Причому, слово «digital» зустрічається 905 разів, та в 12 з 52 пунктах підсумкової декларації, з чого робимо висновок: цифрові технології мають максимальний пріоритет у майбутньому. Ця думка сформульована окремими пунктами: “25. Ми заохочуємо міжнародну співпрацю для подальшого розвитку цифрових навичок і цифрової грамотності, використовуючи позитивний вплив цифрової трансформації…”, “26. Ми виявили, що цифрові технології стають ключем до відновлення та розширення можливостей у різних секторах, у тому числі у створенні стійкої продовольчої системи, сільського господарства, стійких та гідних робочих місць і розвитку людського потенціалу…”. З чого можна зробити висновок (сподівання), що ЕУ та цифрові технології прийдуть і у сферу безпеки.

Так, дуже важливі сфери життєдіяльності держави поки що залишаються без суттєвої наукової та інформаційної підтримки. Це, в першу чергу, стосується сфери безпеки та

військової сфері [5, 6]. Можна навести ступені інформатизації суспільства в Україні за спадом: банківська сфера, торгівля, освіта, ІТ-індустрія, ядерна енергетика, авіаційний транспорт, комунальне господарство, сфера безпеки, військова сфера. Як бачимо, інформатизація присутня там, де є гроші. Але у сфері безпеки це призводить до корупції, у військовій – до необхідності просити допомоги у розвинутих країн (де працюють випускники наших вишів). Як довело життя, потрібно різко змінювати (відновлювати) ситуацію. Отже розглянемо сферу безпеки.

Коротко про суть проблеми. В наукових працях дослідників країни, дисертаціях та дипломних роботах студентів і аспірантів дуже мало праць не тільки про рішення складних прикладних задач у цьому напрямі, але майже відсутні роботи щодо їх постановки. Не впроваджені передові світові технології управління безпекою на основі ризик-орієнтованого підходу (РОП) та стандарти Євросоюзу цього напряму [5–7]. Державний нагляд за безпекою відбувається до цього часу по-старому, методами інспекційного надзору, як у радянські часи.

Дійсно, сам факт відсутності інформаційних технологій (ІТ) у XXI ст. у процедурах оцінки ризику (безпеки) призводить до умов відсутності прозорості [3, 4], і, як наслідок, до корупції. Тому стаття є актуальною, має стати початком важливих та необхідних змін.

3. Аналіз факторів та обставин ризику ТРЦ

Торговельно-розважальний центр – це будівля, яка функціонує з метою обслуговування відвідувачів. Зазвичай це багатоповерхова будівля, що містить у собі:

- комплекс крамниць: одягу, техніки, аптек, продуктів;
- підприємства побутового обслуговування (ательє, ремонт одягу);
- заклади громадського харчування: кав'ярні, ресторани, бари, заклади швидкого харчування;
- розважальні зони: атракціони, кінотеатри, дитячі центри;
- куточки надання послуг зі сфери краси.

Велика кількість відвідувачів повинна відчувати себе комфортно, задля цього ТРЦ облаштовані вбиральнями, ескалаторами, системами клімат-контролю, безкоштовним паркінгом та ін. Варіативність для дозвілля робить ТРЦ осередком масової культури. У роздрібних торгових павільйонах можна знайти все, що завгодно [8, 9]. Так, у ТРЦ «Гулівер» на 8 поверхах налічується понад 250 ексклюзивних і мультибрендових магазинів, в яких продають модний одяг і взуття, вироби зі шкіри, ювелірні прикраси та аксесуари. Торгова площа ТРЦ «Лавина» складає 127 000 м² (12, 7 га). ТРЦ містить понад 400 магазинів, є парковка на 4000 машин [9] (рис. 1).

З точки зору безпеки, ТРЦ є місцем скупчення людей, безпеку яких потрібно гарантувати. Сильне навантаження на електропроводку, джерела відкритого вогню на кухнях закладів та інші подібні фактори несуть небезпеку для зайняття пожежі, тож будь-який ТРЦ повинен бути побудований з урахуванням вимог, викладених у Державних будівельних нормах України (ДБН). Попри це, об'єкт мусить відповідати вимогам державного стандарту [10] (ГОСТ 12.01.004-91), в якому вказано, що пожежна безпека об'єкта мусить забезпечуватися такими системами безпеки (СБ):

- система запобігання пожежі;
- система протипожежного захисту;
- система організаційно-технічних заходів.

Рівні забезпечення пожежної безпеки відвідувачів і матеріальних цінностей, економічні критерії ефективності, проєктування, будівництва до експлуатації об'єкта охарактеризовані в даних системах і спрямовані на виконання таких завдань:

- виключення виникнення пожежі;
- забезпечення пожежної безпеки людей;

• забезпечення пожежної безпеки матеріальних цінностей.

Як випливає з документів ідентифікації безпеки ТРЦ, встановлюють високонадійні системи безпеки (СБ) переважно фірми Siemens, що надає їх хазяям впевненості в безпеці. Але немає систем 100% надійності, причому цей важливий параметр СБ залежить від технічних регламентів їх обслуговування (людського чинника). Звісно, дотримання всіх правил забезпечує мінімізацію вірогідності виникнення пожежі, але це не завжди можливе (досяжне) і, крім того (головне), всі події з порушеннями, які призводять до НС, у більшості мають випадковий характер.

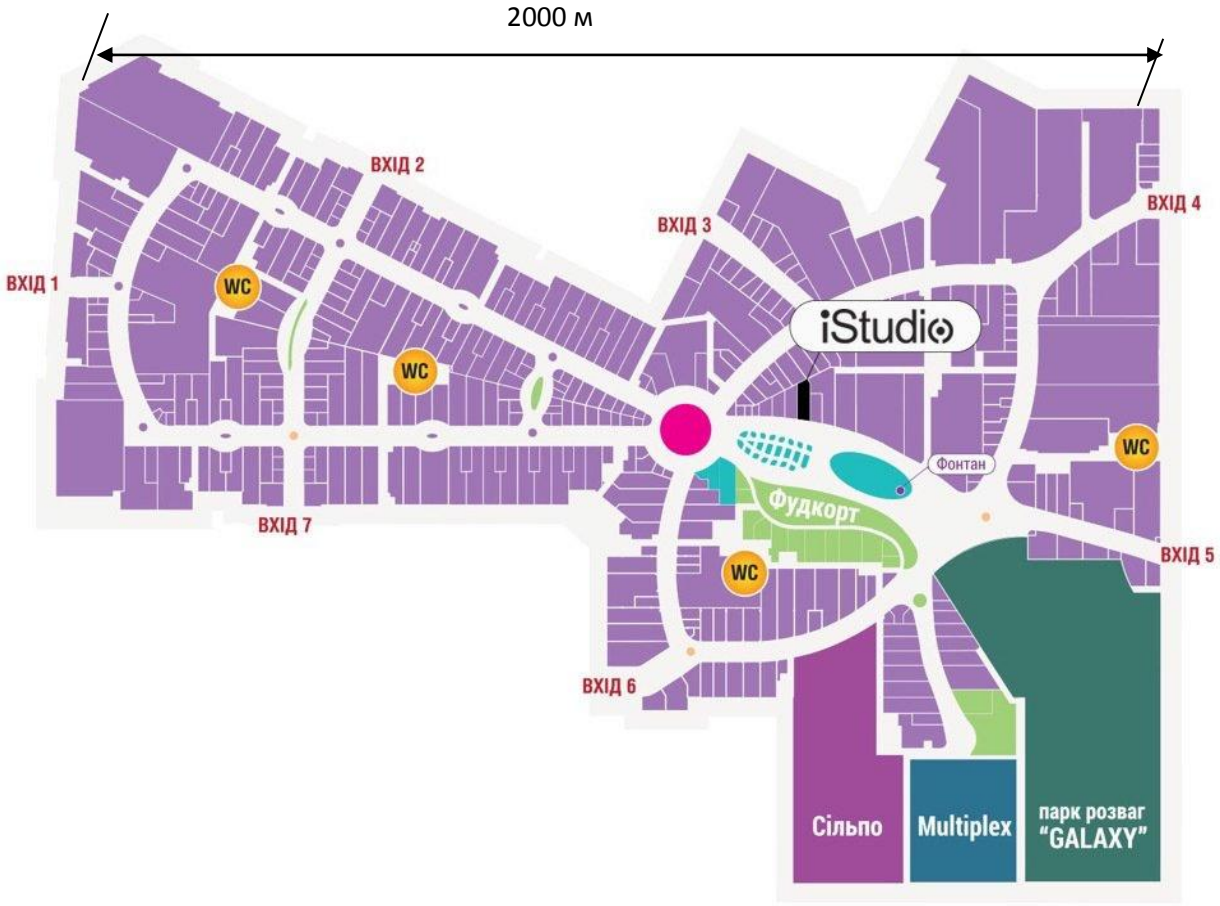

Рисунок 1 – План ТРЦ «Лавина». Світлі лінії є границями крамниць

На сайтах майже всіх ТРЦ є багато даних про товарі й послуги, але дуже рідко зустрічаються дані про безпеку. Навіть навпаки, деякі об'єкти містять інформацію про те, що вони не несуть відповідальності за безпеку відвідувачів. Так, документом «Правила та умови перебування на території ТРЦ» («Гулівер»), затвердженим Наказом ТОВ «ТРИ О» № 02 від 22.10.2020, декларується таке відношення до безпеки: «Власник ТОК (торгово-офісний комплекс), а також призначена ним Адміністрація та (або) залучена ним Служба охорони не несуть відповідальності за будь-яку шкоду, яка може бути заподіяна в ТРЦ майну будь-яких осіб, життю і здоров'ю Відвідувачів, у тому числі заподіяну діями (бездіяльністю) орендарів приміщень і (або) третіх осіб, включаючи дії (бездіяльність) будь-яких Відвідувачів, а також не несе відповідальності за збереження будь-якого майна (речей, документів, грошових засобів та ін.) будь-яких осіб, що знаходяться в ТРЦ, включаючи Відвідувачів (п. 2.3)».

Такий підхід протирічить законодавчим нормам нашої країни з багатьох боків, перш за все: 1) Закону України (ЗУ) про ОПН; 2) ЗУ про державні інспекції та відповідним постановам Кабміну. Але ці протиріччя чомусь не помічені державними структурами верх-

нього рівня. На сайті ДСНС можна знайти акти перевірок деяких ТРЦ із сотнями зауважень щодо невиконання ДБН тощо. При цьому проєктант запевнює у зворотному. Наприклад, сайт відомого проєктанта повідомляє, що виходячи з пріоритету безпеки, така будівля повинна повною мірою відповідати всім будівельним нормам і технічним стандартам, а також мінімізувати (виключати) ризики та наслідки, пов'язані з пожежами, землетрусами та іншими стихійними лихами. Пріоритетну значимість мають такі компетенції, як дотримання всіх нормативних та технічних вимог. Саме тому торговельний центр стає безпечним і привабливим [11]. Але, як вже було сказано, за результатами більшості перевірок інспектори ДСНС України виявляють протилежне. Сотні недоліків, про що часто просто надається припис на закриття. Як бачимо, утворюється протиріччя між власниками і проєктантами, з одного боку, та державною службою безпеки з другого. Тобто виникає конфлікт бізнесу та державних структур, що призводить до нестабільності, напруги в суспільстві. Серед зауважень інспекцій є дуже важливі, які напряму впливають на ризик для відвідувачів та персоналу: про порушення ДБН, правил пожежної безпеки, вимог про евакуацію. Наприклад: «…не проведено визначення розрахункового часу евакуації людей у разі пожежі відповідно до ГОСТ 12.1.004-91». Не перевірено для багатьох ТРЦ, але на основі власного досвіду таких розрахунків [5] та згаданого стандарту можна стверджувати, що для деяких ТРЦ не можна виконати умови стандарту навіть фізично. Не можна пройти сотні метрів у задимленому й темному приміщенні за кілька хвилин. Навіть вдень та зі світлом тяжко знайти один із декількох виходів у великих ТРЦ (рис. 1).

Важливим фактором ризику можуть бути також система клімат-контролю приміщень ТРЦ. Як правило, для цих цілей використовуються кришні кондиціонери типу Rooftop [12] із підводом природного газу поверх покрівлі. Сотні метрів газопроводів, самі Rooftop та умови їх обслуговування теж потрібно розглядати як фактор ризику. Так, у минулому році зафіксовано пожежі великих ТРЦ, які розпочиналися саме з покрівлі (Стамбул, Химки) з причин помилок персоналу під час обслуговування цих систем. З цього видно, що недостатнє навчання персоналу теж має розглядатися як обставини ризику.

4. Розрахунок (моделювання) часу евакуації

Визначення розрахункової тривалості евакуації людей із приміщень, будівель і споруд проводиться з застосуванням спрощеної аналітичної моделі руху людського потоку за додатком А.4 ДСТУ 8828:2019 (ГОСТ 12.1.004-91). Загальний алгоритм розрахунку евакуації приміщень у процесі експлуатації відбувається відповідно до плану евакуації (рис. 2) і складається з таких кроків:

1. Визначити можливі маршрути евакуації (за кількістю основних та запасних входів - виходів).
2. Розбиття маршрутів евакуації на розрахункові ділянки.
3. Знаходження тупикових початкових та диктуючих ділянок, шляхів прямування.
4. Визначення розрахункової довжини та ширини ділянок.
5. Визначення щільності потоку.
6. Визначення часу руху на ділянці та маршруті евакуації в цілому.

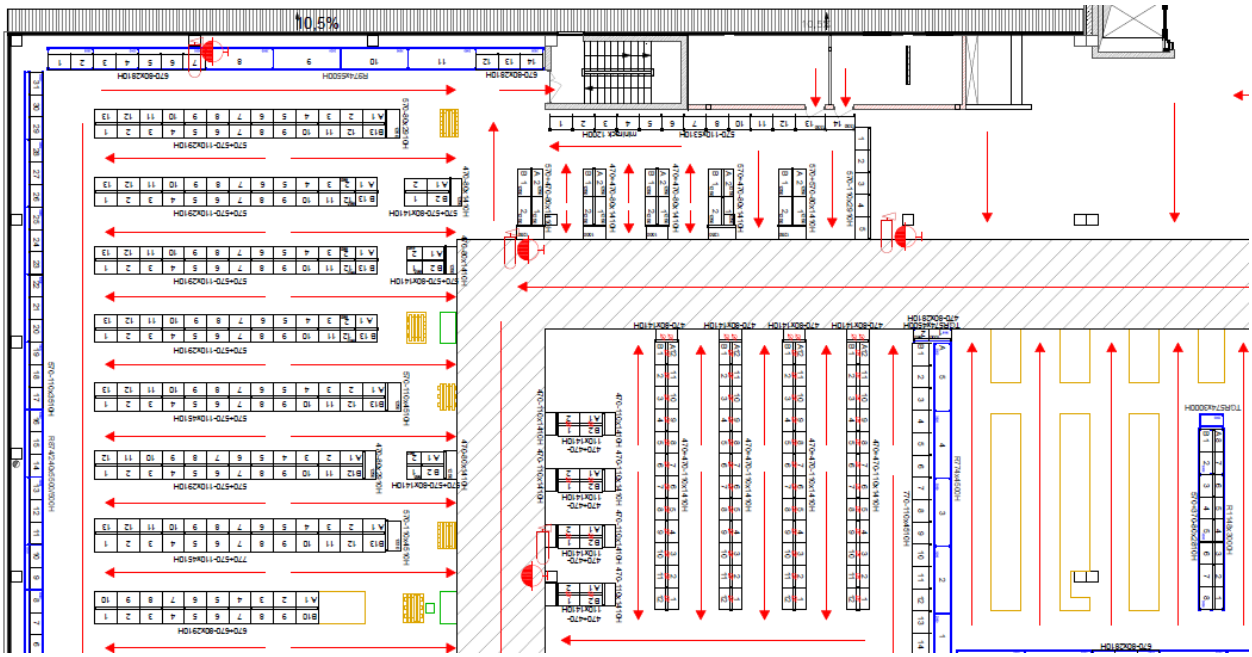

Рисунок 2 – Фрагмент плану евакуації ТРЦ

Усі ці кроки зовсім не прості, наприклад, навіть у порівняно невеликого ТРЦ ($S <= 20000\,m^2$) при розрахунках відповідно до стандарту виділено (i) більше 200 розрахункових ділянок. Очевидно, що для об'єкта типу ТРЦ «Лавина» таких ділянок буде тисячі. Розрахунок для кожної ділянки однотипний. Потрібно визначити початкову кількість людей на ділянці N_1, інтенсивність людського потоку q_B, час проходження ділянки t_B. Отже, для автоматизації процесу розроблена програма (рис. 3). Для повної автоматизації потрібно прив'язати ці розрахунки до плану евакуації. Але, на наш погляд, така робота потрібна на стадії проєктування, а не як виправлення зауважень інспекції.

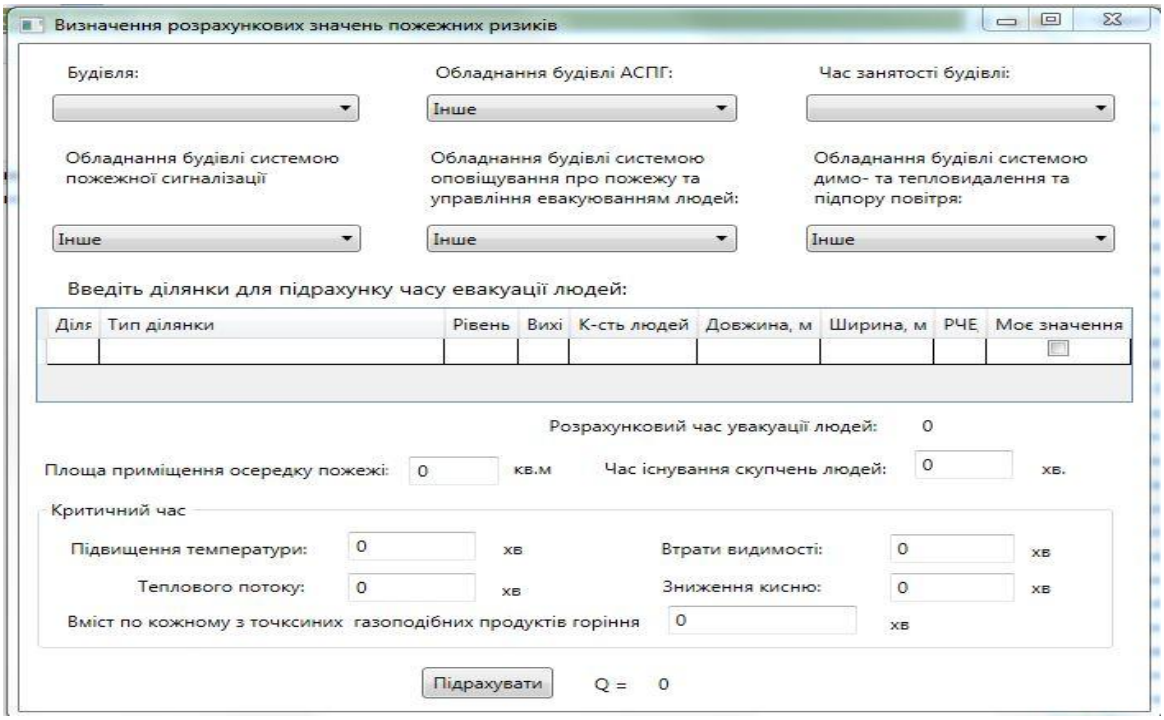

Рисунок 3 – Вікно програми розрахунку часу евакуації

Імовірність евакуації людей P_e розраховують за формулою

$$P_e = \begin{cases} 0{,}999 \cdot \dfrac{0{,}8 \cdot t_{бл} - t_р}{t_{пе}}, \text{ якщо } t_р < 0{,}8 \cdot t_{бл} < t_р + t_{пе} \text{ та } t_{ск} \le 6 \text{ хв}, \\ 0{,}999, \text{ якщо } t_р + t_{пе} \le 0{,}8 \cdot t_{бл} \text{ та } t_{ск} \le 6 \text{ хв}, \\ 0{,}000, \text{ якщо } t_р \ge 0{,}8 \cdot t_{бл} \text{ або } t_{ск} > 6 \text{ хв}, \end{cases}$$

де t_p – розрахунковий час евакуації людей, хв;

$t_{пе}$ – час початку евакуації (інтервал часу від виникнення пожежі до початку евакуації людей), хв;

$t_{бл}$ – час блокування шляхів евакуації (інтервал часу від початку пожежі до блокування евакуаційних шляхів у результаті поширення на них небезпечних факторів пожеж, що мають гранично допустимі для людей значення), хв;

$t_{ск}$ – час існування скупчень людей на ділянках шляху (щільність людського потоку на шляхах евакуації перевищує значення 0,5).

Розрахунковий час евакуації людей t_p слід визначати як суму часу руху людського потоку по окремих ділянках шляху t_i за формулою

$$t_p = t_1 + t_2 + t_3 + \dots t_i,$$

де t_1 – час руху людського потоку на першій (початковій) ділянці, хв;

t_1, t_2, t_3, $\dots t_i$ – час руху людського потоку на кожній із наступних після першої ділянки шляху, хв.

Як свідчить із наведеного, час евакуації залежить, у першу чергу, від маршруту та відстані до виходу. Відстані між відкритими входами-виходами в деяких ТРЦ складають сотні метрів, причому знайти їх у лабіринті магазинів ще й у натовпі людей не проста задача під час стресу. Так, існують і запасні виходи, але не факт, що до них буде доступ, та й чи будуть вони відчинені. Як показує світова статистика, це не завжди так, що й призводить до загибелі людей. Швидкість руху невелика навіть у широких ділянках, але в багатьох ТРЦ ще й треба спускатися по зовсім вузьких і крутих сходах вниз (зупинений ескалатор, не відповідає визначенню «сходи») Тобто, очікувано, що в багатьох випадках умови евакуації можуть не виконуватися, тому цей розрахунок, на наш погляд, має бути обов'язковим для будь-якого проєкту.

5. Визначення проблем безпеки ТРЦ

На основі проведеного аналізу можна сформулювати проблеми та задачі з безпеки ТРЦ, які мають бути вирішені для безпечного функціонування цих об'єктів.

Проблеми:

1. Проєкти ТРЦ не завжди відповідають ДБН та стандартам України.

2. Ставлення хазяїв до безпеки громадянина під час його знаходження в ТРЦ не завжди відповідає Конституції та законодавству України.

3. Перевірки державних інспекцій, які діють на основі чинного законодавства, частіше призводять до припису закриття ТРЦ, з чого виникають протиріччя з бізнесом, перешкоди інвестиціям, загальна напруга в суспільстві.

4. Степінь інформованості відвідувача не достатня для адекватних дій під час можливих аварій, недостатня кількість показників основних та запасних виходів.

5. Існує об’єктивна необхідність розвитку сфери безпеки ТРЦ у напрямах узгодження з нормативним полем України та впровадження ІТ у сферу безпеки.

Задачі:

1. Узгодження НД з ЄС у повній міри з питань безпеки тощо.

2. Мають бути оцінки ризику у проєктній документації, розрахунки часу евакуації тощо.

3. Потрібно розробити та впроваджувати світло-голосові показники, що не залякують відвідувачів, а допомагають визначити найкращий за часом маршрут евакуації.

4. Потрібно приймати міри з забезпечення вимог ДБН із безумовного виконання вимог часу евакуації з усіх ділянок.

5. Провести класифікацію ТРЦ за типовими проєктами та створити програмне забезпечення щодо оцінок ризику персоналу та відвідувачів у вільному доступі.

6. У рамках інформаційного забезпечення та розвитку ЕУ забезпечити прозорість та відкритість інформації з безпеки в ТРЦ як осередка сучасної масової культури.

У висновку слід зазначити, що існуючі проблеми функціонування ТРЦ України як у законодавчому, так і в інформаційному полі, потрібно вирішувати на державному рівні в рамках ЕУ.

6. Розробка концепції ризику ТРЦ на основі ІТ

Відомо, що ризик – величина розрахункова, потрібно визначати ймовірність небажаної події (пожежі) й можливі наслідки. З цього видно, що має бути відповідне моделювання. Як було зазначено, для розрахунку наслідків ризику потрібна модель евакуації. Моделювання ймовірності пожежі за класичним підходом робимо деревом відмов (ДВ).

Один із варіантів моделі представлено ДВ (рис. 4), яке розроблено на основі моделі китайських дослідників [13]. Відомо, що для того, щоб виникла пожежа, мають існувати джерело вогню та горюча речовина. Джерелом вогню в ТРЦ може бути відкритий вогонь (від покупців або від специфічних предметів); електрична іскра (при несправності електрики чи витоку газу); накопичення тепла (погана вентиляція та погане охолодження); вогонь від електростатичних сил та ін. (ліва гілка ДВ). Буде досить необачно враховувати тільки прямі причини займання і не враховувати фактори, які роблять пожежу катастрофічною. Таким чином, ми маємо врахувати також, наскільки якісна рятувальна діяльність буде проведена при виникненні загорання, для того щоб з самого початку зрозуміти, на яку поміч і за який час ти можеш розраховувати і як зробити так, щоб пожежні бригади швидше розібралися у причинах пожежі (права гілка ДВ).

Таким чином, маємо кістяк нашого дерева відмов (типову модель), який можемо заповнювати в залежності від типу проєкту ТРЦ. Відомо [5], що представлену модель можна доповнювати новими базисними подіями та змінювати числові ймовірнісні характеристики подій. Тобто є можливість враховувати особливості небезпечних речовин, справність систем безпеки, їх надійність, рівень навченості персоналу тощо. Модель реалізована у програмному середовищі Python. Програмою згенеровано 481 варіант імовірного протікання аварії – мінімальні перерізи (Min Cat – MC) та розраховані їх числові значення, що, звісно, не може бачити жоден кваліфікований експерт. Додаткове удосконалення моделі шляхом збільшення кількості врахованих факторів та обставин призводить до збільшення MC до 1200 та більше. Такий підхід на практиці показує себе досить добре [5] і може бути інтегрований у державні системи електронного уряду.

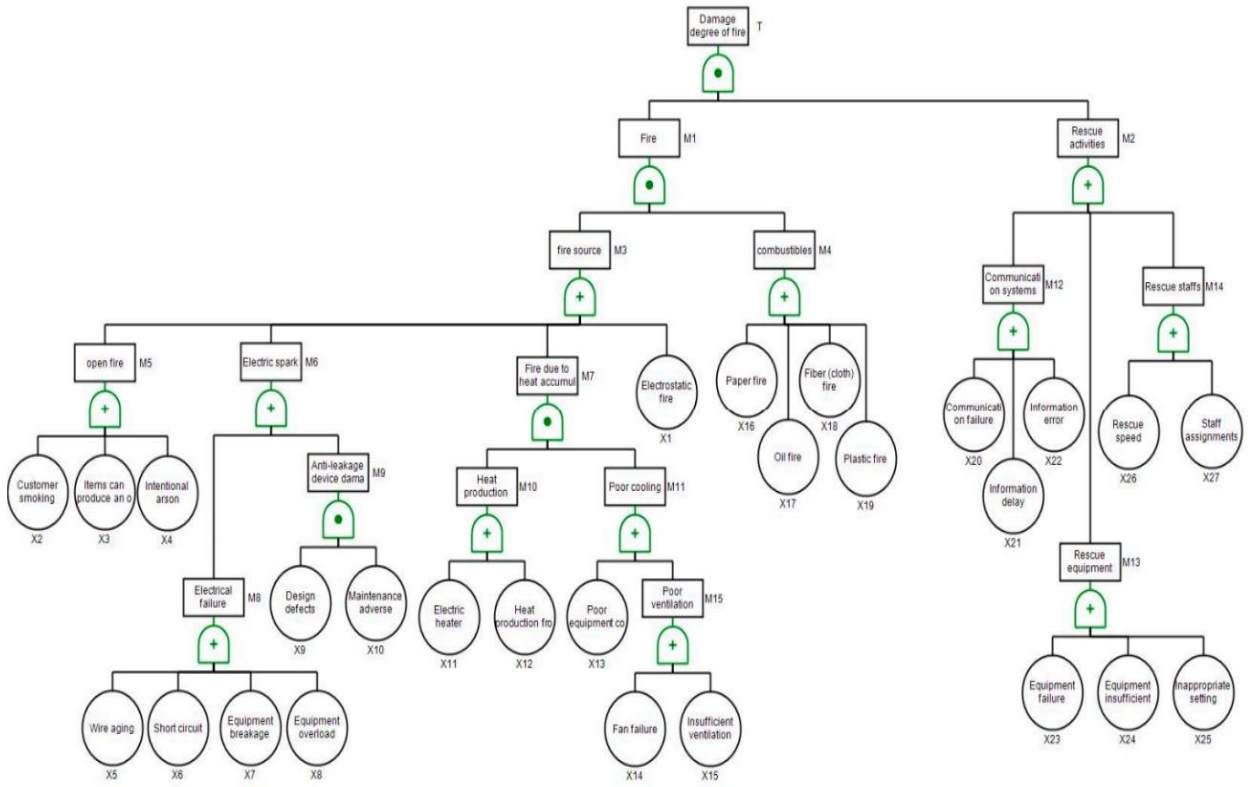

Рисунок 4 – Базове дерево відмов – ймовірнісна модель виникнення та розвитку пожежі
Позначення подій: X1 – електростатична пожежа, X2 – клієнт курить, X3 – предмети можуть виробляти відкритий вогонь, X4 – умисний підпал, X5 – старіння проводу, X6 – коротке замикання, X7 – поломка обладнання, X8 – перевантаження обладнання, X9 – дефекти конструкції, X10 – негативне обслуговування, X11 – електричний обігрівач, X12 – виробництво тепла від робочого обладнання, X13 – погане охолодження обладнання, X14 – несправність вентилятора, X15 – недостатня вентиляція, X16 – загорання паперу, X17 – пожежа ЛЗР, X18 – загорання волокна, X19 – загорання пластмаси, X20 – збій зв'язку, X21 – затримка інформації, X22 – інформаційна помилка, X23 – несправність обладнання, X24 – недостатність обладнання, X25 – невідповідне налаштування, X26 – швидкість порятунку, X27 – долучення персоналу команди рятувальників

Для практичної реалізації щодо підходу визначення безпеки (ризику) ТРЦ на основі інформаційних технологій, очевидно, потрібно провести класифікацію об'єктів за їх основними параметрами: тип проєкту, системи безпеки, наявність легко займистих матеріалів та ін.

Отже, принципове рішення проблем із боку інформаційного забезпечення оцінок ризику ТРЦ доведено практично. Попередньо проведені оціночні розрахунки на основі ймовірнісного моделювання показують низькі ймовірності виникнення пожеж, з чого видно, що ключову роль відіграє можливість евакуації відвідувачів та персоналу. Але за результатами ймовірнісного моделювання можна також розробити заходи з підвищення безпеки, що потрібно всім об'єктам. Отже, для рішення питання у масштабі держави потрібні тільки політична воля уряду та відповідні зміни чинного законодавства.

7. Можливий варіант включення питань безпеки ТРЦ в ІТ [14]

Зростаюча кількість мобільних пристроїв та розширення їх функціональності створюють попит на програмне забезпечення, сумісне з мобільними пристроями.

Наявна у світі тенденція до здешевлення послуг у сфері хмарних технологій паралельно з розвитком технологій захисту інформації, зростанням потужності та кількості

хмарних хостингів створює сприятливі умови для розвитку хмарних сервісів. Зокрема, все більшого поширення набирає концепція Software-as-a-Service (SaaS) – програмне забезпечення як сервіс [15]. Такий підхід також дозволяє знизити навантаження на пристрій (персональний комп'ютер чи мобільний пристрій) користувача за рахунок перенесення найбільш ресурсоємних розрахунків на потужний хмарний сервер чи групу хмарних серверів у рамках хмарного хостингу. Пристрій користувача у такому разі тільки передає вхідні дані та отримує результати розрахунку.

Тому доцільно побудувати систему програмних модулів для оптимізації та оцінки рівня безпеки (ризику) на основі концепції SaaS [15]. Взаємодію між різними програмними модулями пропонуємо організувати, скориставшись одним із варіантів:

1. REpresentational State Transfer (REST) [16].
2. Simple Object Access Protocol (SOAP) [17, 18].

Такий підхід є зручним як для створення додатків для мобільних пристроїв, так і веб-сервісів на основі веб-сайтів.

8. Висновки

Розвиток цифрової індустрії у світі вимагає рухатися синхронно зі світовим суспільством, наша держава має добрі успіхи на шляху реформ щодо впровадження ЕУ, але й до цього часу спостерігаємо факт відсутності інформаційних технологій у процедурах оцінки безпеки, що призводить до протиріч у суспільстві. Сфера безпеки в усіх галузях виробництва в нашій державі потребує сучасної інформаційної та методичної підтримки.

Оскільки ТРЦ стають об'єктами сучасної масової культури з дуже великим числом щоденних відвідувань, потрібно в рамках інформаційного забезпечення та розвитку ЕУ забезпечити прозорість та відкритість інформації з безпеки в ТРЦ як об'єкта з одночасним перебуванням великої кількості людей.

Нові сучасні інвестиційні проєкти ТРЦ при їх впровадженні мають бути адаптовані до умов України. Існуючі проблеми функціонування ТРЦ України як в законодавчому, так і в інформаційному полі потрібно вирішувати на державному рівні в рамках ЕУ. Можлива й необхідна розробка інформаційних технологій контролю рівня ризику та оптимізації періоду його контролю в залежності від надійності систем безпеки об'єктів, ТРЦ тощо.

СПИСОК ДЖЕРЕЛ

1. Исследование ООН: Электронное правительство 2020: звіт. URL: https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20-%20Russian.pdf.
2. Индекс развития электронного правительства (EGDI). URL: https://publicadministration-un-org.translate.goog/egovkb/en-us/About/Overview/-E-Government-Development-Index?_x_tr_sl=en&_x_tr_tl=ru&_x_tr_hl=ru&_x_tr_pto=sc.
3. Розвиток електронних послуг. URL: https://www.kmu.gov.ua/diyalnist/reformi/efektivne-vryaduvannya/rozvitok-elektronnih-poslug.
4. G20 BALI LEADERS' DECLARATION Bali, Indonesia, 15–16 November, 2022. URL: https://d1fdloi71mui9q.cloudfront.net/AoiUxBV4QbyF0cMIHxxM_G20%20Bali%20Leaders-%20Declaration%2C%2015.
5. Бєгун В.В. Методологічні основи інформаційної технології управління безпекою на основі ризик-орієнтованого підходу: дис. … д-ра техн. наук: 05.13.06. Київ, 2020. 553 с.
6. Бєгун В.В., Бєгун С.В. Одиниці виміру ризику за теорією ризик-орієнтованого підходу. *Математичні машини і системи*. 2019. № 1. С. 191–202.
7. Risk management – Risk assessment techniques. International Standard IEC 31010:2019. IEC, Geneva, 2019.
8. ТРЦ «LAVINA» – Найбільший торгово-розважальний центр. URL: https://lavinamall.ua/.
9. ТРЦ «Голлівуд». URL: https://gullivercenter.com/mfk.

10. ГОСТ 12.1.004-91. Пожарная безопасность. общие требования. Рекомендации по расчету параметров эвакуации людей на основании положений. Минск, 1999.
11. Строительство торговых центров группой компаний «Новые зодчие». URL: http://www.n-zodchie.com/stroitelstvo-torgovyh-centrov.html.
12. Руфтоп (ROOFTOP) или крышный кондиционер. URL: http://condicionery.od.ua/ru/blog/main/11159.htm.
13. Ishola F., Oladokun V., Petinrin O., Olatunji O., Akinlabi S. A mathematical model and application for fire risk management in commercial complexes in South Africa. *Results in Engineering*. 2020. Vol. 7. DOI: https://doi.org/10.1016/.rineng.2020.100145.
14. Бєгун В., Волошин О., Бєгун С. Оптимізація контролю безпеки торговельно-розважальних комплексів на основі аналізу моделей визначення ризику. *Інформаційні технології та комп'ютерне моделювання*: матеріали статей міжнар. наук.-практ. конф. (м. Івано-Франківськ, 15–16 грудня 2022 р.). Івано-Франківськ: п. Голіней О.М., 2022. С. 4–6.
15. Melland P., Grance T. The NIST Definition of Cloud Computing, NIST Special Publication 800-145. National Institute of Standards and Technology, U.S. Department of Commerce, 2011.
16. Fielding R.T. Architectural Styles and the Design of Network-based Software Architectures, PhD thesis. Irvine, USA: University of California, 2000.
17. SOAP Version 1.2 Part 1: Messaging Framework (Second Edition), W3C recommendation, 2007, URL: https://www.w3.org/TR/soap12/.
18. WSDL 1.1 Binding Extension for SOAP 1.2, W3C member submission, 2006. URL: https://www.w3.org/Submission/wsdl11soap12/.

Стаття надійшла до редакції 12.01.2023