УДК 005.934

COBISS.SR-ID 513526709

https://doi.org/10.18485/fb_godisnjak.2019.3

**КОНЦЕПТ БЕЗБЕДНОСТИ – СИСТЕМСКИ
ПРИСТУП
(ПРИМЕНА СИСТЕМСКИХ АРХЕТИПОВА
У УПРАВЉАЊУ РИЗИЦИМА)**

Проф. др Озрен Џигурски*
Универзитет у Београду, Факултет безбедности

* odzigurski@gmail.com

КОНЦЕПТ БЕЗБЕДНОСТИ – СИСТЕМСКИ ПРИСТУП (ПРИМЕНА СИСТЕМСКИХ АРХЕТИПОВА У УПРАВЉАЊУ РИЗИЦИМА)

Сажетак: Појам безбедности се у раду разматра са аспектима корпоративне, организационе, пословне или људске безбедности. У том смислу, у концептуалном погледу, безбедносни систем може се посматрати као комплексни систем, чије су варијабле променљиве у времену, где се у његовом проучавању може применити методологија која припада области Системске динамике. Овај приступ је погодан с обзиром да омогућава реалну операционализацију концепта безбедности. У раду се разматрају аспекти концепта безбедности који произилазе из системског приступа, као што су онтологије и системски архетипови у домену безбедности. Ово представља генерални приступ, који полази од изабране системске архетипа као генеричке форме, који се затим мапира на архетип за одговарајућу примену. Применом специјализованог софтвера за симулацију система генерише се инстанца модела, тј. одговарајући математички и симулациони модел. На основу резултата симулација могу се одредити оптималне одлуке за управљање ризицима у реалном времену. Примена системског приступа, заснованог на системским архетиповима, приказана је на примеру управљања ризицима.

Кључне речи: безбедност, ризици, архетип, системска динамика, компјутерска симулација.

Увод

Појам безбедности који се у раду разматра, највећу примену има у области корпоративне, организационе, пословне и људске безбедности, а у мањој мери се односи на националну или интернационалну безбедност, мада је могуће у даљим истраживањима овај приступ проширити и применити и на ове области. Приступ који је у раду примењен односи се на операционализацију концепта безбедности у домену управљања ризицима. У том смислу, у концептуалном погледу, безбедносни систем може се посматрати као комплексни систем чије су варијабле променљиве у времену, па се у том циљу може применити методологија која припада области Системске динамике (System Dynamics – SD). Овај приступ је подобан с обзиром да омогућава реалну имплементацију, тј. операционализацију концепта безбедности. У раду се разматрају аспекти концепта безбедности који произилазе из Системског приступа (Systems Thinking – ST), као што су онтологије и системски архетипови у домену безбедности.

Архетипови као концепт који се односи на Системски приступ анализи сложених система, развијен је средином осамдесетих година двадесетог века, у покушају да се опише понашање ових система, као и да се сазнања о њиховом функционисању и структури приказују на лакши и ефикаснији начин. Системски архетипови представљају скуп системских структура које производе уобичајене обрасце понашања у многим и различитим областима (Braun, 2002).

Један од најважнијих и потенцијално најснажнијих увида који потичу из системског приступа је да се одређени обрасци и структуре у системима понављају изнова и изнова. Ови обрасци, као *системски архетипови* или *јенеричке структуре*, омогућавају да се препознају структуре и функције у комплексним организационим системима, тј. они се могу универзално препознати у многим сложеним системима.

У постојећој литератури нема довољно референци за примену Системског приступа и системских архетипова у области безбедности и управљању ризицима. Већина актуелних приступа анализи ризика заснована је на акцидентним догађајима и не садржи на одговарајући начин динамичку комплексност и нелинеарне интеракције које карактеришу сложене системе. У неколико радова предлаже се скуп системских архетипова који анализирају уобичајене безбедносне недостатке у организацијама, тј. динамику понашања организација која често доводи до акцидентата (Marais, 2006).

Приликом конкретне примене сви системски архетипови се реализују помоћу елемената који припадају основним компонентама за анализу понашања сложених динамичких система применом методологије из области Системске динамике. Ово представља генерални приступ, који полази од изабраног системског архетипа као генеричке форме, а затим се мапира на архетип за одговарајућу примену. На основу тога, даље се реализује логички концепт система у виду узрочно-последичног дијаграма који приказује ентитете и релације у систему. На основу претходног, применом специјализованог софтвера за симулацију система генерише се инстанца модела, тј. одговарајући математички и симулациони модел. Вишеструким извршавањем симулационог модела, са различитим варијацијама параметара у моделу, може се вршити анализа понашања система за различите облике и узроке безбедносних угрожавања. На основу резултата симулација могу се, затим, одредити оптималне управне и оперативне одлуке за управљање ризицима у реалном времену.

Примена Системског приступа, заснованог на системским архетиповима и методологији из области Системске динамике, приказана је на примеру управљања ризицима.

Концепт безбедности – онтолошки приступ

Појам концепта се може у општем смислу дефинисати као скуп апстрактних идеја или општих појмова у мишљењу, који се односе на одређену категорију или домен људских активности. У општем случају, концепти се проучавају у више различитих дисциплина, као што су: лингвистика, психологија, филозофија, као и у многим другим научним и стручним областима. Ово доприноси формирању логичке и менталне структуре концепта, кроз изградњу одговарајућег категоријалног апарата. На тај начин омогућава се и интердисциплинарни приступ изучавању безбедности, што доприноси бољем разумевању ове области, нарочито када је у питању апстрактни део промишљања и објашњења појма безбедности, или када се бавимо језичким конструкцијама, тумачењима и правилностима у употреби термина *безбедности*.

За формирање концепта безбедности могуће је, поред осталог, користити и онтолошки приступ. Онтологија припада грани метафизике која се бави општим својствима постојања и представља скуп концепата, категорија и ентитета у одређеној области или домену и приказује

фундаменталне особине, као и релације међу њима. У општем смислу онтолошка безбедност се односи на осећај постојања сигурности и стабилности у животима људи (Giddens, 1991). Поред тога, у оквиру онтолошке безбедности претпоставља се да постоји позитиван аспект у односу на животе људи, њихово постојање у глобалним и локалним околностима и у будућности.

Са аспекта безбедности, у системском приступу, онтологија садржи пет основних класа/структура: организација, ресурси, ризици, угрожавање и контрола, или у проширеном облику: организација/власник, ресурси, рањивости/слабости/ризици, угрожавања/претње, контрола/противмере (Hercog, 2007). Ове класе су фундаменталне у области система безбедности и могу се даље разложити на ниже нивое и компоненте. Релације између онтолошких класа уобичајено се приказују у виду специјалног графа, тј. графикана знања - *Knowledge Graph* (Singhal, 2012). Слика 1 приказује основне онтолошке класе и релације у домену безбедности.

Слика 1. Основне онтолошке класе и релације у домену безбедности – *Knowledge Graph*

Системски архетипови у домену безбедности

У општем смислу архетип је савршен пример или модел нечега и представља наслеђени образац мишљења произашао из претходног искуства из свих могућих извора. Архетип може бити: исказ, образац понашања, прототип, изворни облик или главни модел који други искази, обрасци понашања и објекти могу да копирају, опонашају или интегришу. Генерално, архетип се може дефинисати као „оригинални модел”, чији сви остали изведени појмови, објекти или концепти могу бити само деривати, копирани, узорковани или опонашани (Stevens, 2006).

Архетипови као концепт који се односи на Системски приступ за анализу сложених система, развијени су средином осамдесетих година двадесетог века, у покушају да се опише понашање ових система, као и да се сазнања о њиховом функционисању и структури приказују на лакши и ефикаснији начин. Системски архетипови представљају скуп системских структура које производе уобичајене обрасце понашања у многим различитим областима. Ова категорија архетипова може да обједињује дисциплине које су често изучаване као одвојене области – психологија, економија, биологија, урбанизам, технологија, државни системи, безбедност итд., јер се њихова структура може универзално препознати у многим сложеним системима.

Један од најважнијих и потенцијално најснажнијих увида који потичу из системског приступа је да се одређени обрасци и структуре у системима понављају изнова и изнова. Ови обрасци, као *системски архетипови* или *генеричке структуре*, омогућавају да се препознају структуре и функције у комплексним организационим системима.

Постојећа литература описује десет различитих системских архетипова, што је приказано у изворној литератури из ове области (Senge, 1990). То су релативно једноставне, генеричке структуре са повратном спрегом (*feedback*), које се понављају у различитим облицима и размерама кроз многе друштвене, еколошке, техничке и друге системе. Системски архетипови садрже основне структуре повратних информација које приказују експоненцијални раст или опадање, достизање или осцилације задатог циља, генеричке структуре раста, прекорачења и функционални колапс, детерминистички хаос итд. Поред тога, постоје и сложеније структуре системских архетипова који се налазе у основи многих проблема и система управљања. Многи од ових система управљања садрже проблеме у вези са кашњењем при доношењу стратешких управљачких одлука.

Системске архетипове могуће је применити и у области безбедности, и то посебно у домену управљања ризицима. Као средства за анализу ризика, системски архетипови се могу користити за препознавање начина на који ризици могу настати у сложеним социо-техничким системима. Поред тога, као средства за анализу и истраживање акцидената, архетипови се могу користити за развој динамичких модела који описују системске и организационе факторе који доприносе појави акцидената. Ови модели могу помоћи да се донесу оптималне одлуке везане за безбедност и управљање ризицима, како би функционисање система било могуће довести на задовољавајући ниво безбедности.

Од укупно десет генеричких системских архетипова могуће је предложити иницијални скуп од шест архетипова, који могу да моделирају општа динамичка организациона понашања која уобичајено доводе до повећања ризика (Wolstenholme, 2003). На основу тога, могуће је затим одређени архетип користити као основу за проширени модел за доношење ефикасних одлука у домену управљања ризицима.

За анализу у оквиру овог рада усвојен је системски архетип који је изворно назван *Shifting the burden (to intervener)*, што се у слободном преводу може дефинисати као: *Преношење/пребацавање проблема (на извршиоца)*.

Генерички облик овог системског архетипа, као његов мапирани облик за примену у домену безбедности приказан је на слици 2.

Слика 2. Системски архетипови за примену у домену безбедности.

На горњем дијаграму (слика 2а), може се уочити да варијабла **Проблемски симптом** (*Problem symptom*) има више могућих начина деловања, односно решавања. Једним током акције, **Симптоматско решење** (*Symptomatic solution*) има очигледну временску предност извршавања над **Фундаменталним решењем** (*Fundamental solution*), због постојећих кашњења у доношењу стратегијских – фундаменталних одлука. Као резултат, симптоматски проблеми претежно утичу на примену симптоматског решења. Примена симптоматског решења умањује симптоматске проблеме, који затим смањују потребу за проналажењем новог фундаменталног решења.

Како то обично није задовољавајуће, вишеструка примена симптоматског решења често, временом, утиче на развој ненамерних, тј. **Споредних ефеката** (*Side effects*), који онемогућавају ефикасно коришћење постојећих фундаменталних решења. Интеракције између проблемских симптома, симптоматских решења, споредних ефеката и фундаменталних решења формирају дестабилизирајући процес, који прави извор проблема временом чини још тежим за решавање. Из тог разлога, неопходно је приступити доношењу нових облика фундаменталних и симптоматских решења. Међутим, често се акценат ставља на изналажење нових симптоматских решења, због привремених побољшања, иако је улагање у фундаментално решење много бољи избор од потраге за новим симптоматским решењима.

У сагласности са онтолошким приступом, приказаним на Слици 1, извршено је мапирање генеричког архетипа (слика 2а), на системски архетип за примену у домену безбедности (слика 2б). Даља примена и развој овог архетипа може се вршити помоћу методологије из области Системске динамике. Средства из ове области представљају основни алат за конкретну примену системских архетипова. У наставку је приказана примена системског архетипа из домена безбедности на проблем управљања ризицима, коришћењем методологије Системске динамике.

Примена Системске динамике на област управљања ризицима

Приликом конкретне примене сви системски архетипови могу се реализовати помоћу блокова система који чине: стабилизирајући процеси, дестабилизирајући процеси и процеси кашњења у систему. Овome треба додати и нelineарности у систему које неповољно утичу на директно и пропорционално извршавање управљачких функција. Истовремено, наведени блокови представљају основне компоненте за анализу понашања сложених динамичких система применом методологије из области Системске динамике.

Област Системске динамике генерално припада концепту Системског приступа, који представља оквир, структуру знања и средстава који је развијан и примењиван у последњих педесет година. Системски концепт или *Systems Thinking*, представља холистички приступ анализи система који се односи на начине на које компоненте система међусобно функционишу, у оквиру неког сложеног система, и како комплетан

систем функционише у току времена. Може се сматрати да је Системски концепт когнитивни процес за анализу и разумевање функционисања сложених система било које врсте.

Системска динамика (SD) је методологија која се користи да би се анализирано како се системи мењају у току времена. Шездесетих година прошлог века развијена је техника SD моделирања за решавање дугорочних, постојећих, динамичких проблема (Forrester, 1961). Данас, SD се примењује за решавање различитих пословних политика и стратешких проблема (Stermann, 2002). Типична SD студија фокусира се на разумевање начина на који делују компоненте система, како и зашто се генеришу проблеми у динамици функционисања и како политике, стратешке и оперативне одлуке утичу на перформансе система.

SD приступ омогућава анализу разних система, феномена и појава, интеграцијом квантитативних и квалитативних варијабли које имају утицај и одређују понашање ових система, и то из перспективе сложених система. Системска динамика, у општем, може се дефинисати као компјутерска и нумеричка симулација континуалних, нелинеарних система са повратном спрегом, са нагласком на ендогену тачку гледишта (Simonović, 2011).

Концепт повратне спреге (*feedback*) је централни за SD приступ. То значи, да постоји затворени узрочно-последични ланац – петља, тако да последично стање има утицај на узрочне варијабле. Повратна спрега може бити позитивна или негативна. Позитивна спрега тежи да интензивира или појача неку појаву у систему. Негативна спрега се супротставља променама, тако да има улогу стабилизирања и уравнотежења у систему.

Други фундаментални концепт SD се односи на појам **складишта** (*stock*) и **тока** (*flow*), као што је приказано на слици 3. *Stock* варијабле представљају неку врсту акумулације и приказују стање система у току времена. *Flow* варијабле представљају брзину промене, односно оне повећавају или смањују *stock* варијабле у току неког временског интервала. *Stock* варијабле могу бити мењане само помоћу *flow* варијабли, тако да у ствари, *flow* варијабле врше управљање понашањем или стањем система. *Flow* варијабле могу бити улазног или излазног смера.

Слика 3. Графички приказ основних елемената Системске динамике – *Stock* и *Flow*.

За потребе компјутерске симулације неопходно је формирати модел система који се жели истраживати. Критични део поступка представља формирање математичког модела на основу описа система, пошто грешке и непрецизности у овој фази имају доминантан утицај на резултате у даљем процесу симулације. Да би се то поједноставило, развијена су посебна софтверска средства (на пример *Vensim*), која на основу визуелне представе компонентни и релација у систему, интерно генеришу математички модел и затим и сам симулациони модел. Овај симулациони софтвер омогућава директно формирање симулационог модела на бази узрочно-последичног дијаграма (*Causal Loop Diagram* - CLD), који путем визуелизације приказује како се различите варијабле система налазе у међусобном односу у систему.

Концепт Системске динамике може се примењивати у многим областима безбедности. Једна таква специјална област је корпоративна безбедност, где примена SD долази нарочито до изражаја у домену управљања ризицима. У наставку, приказан је узрочно-последични дијаграм – CLD, SD модела за управљања ризицима (слика 4). Овај дијаграм креиран је на основу системског генеричког и одговарајућег мапираног архетипа за примену у домену безбедности.

Слика 4. Узрочно-последични дијаграм – CLD, SD модела за управљања ризицима.

На основу анализе, применом метода Системске динамике и одговарајућег софтверског алата [*Vensim*], може се уочити да су контролно-управљачке петље R4 (Безбедносна политика – менаџмент систем – Захтев за промену управљања – Безбедносна политика) и R5 (Безбедносна политика – Мониторинг ризика – Стање безбедности – Захтев за промену управљања – Безбедносна политика), узрочници нестабилности

функционисања система управљања. Главни разлог за то су кашњења у доношењу одговарајућих управних политика и одлука, као и неусклађеност у динамици примена и извршавања контролних и управљачких активности. Даљом анализом, може се закључити да се стабилизација функционисања система управљања може постићи додавањем једног новог функционалног блока – хибридног блока, креирањем међуинституционалног нивоа безбедности. Блок хибридне безбедности, као и одговарајуће управљачке релације, приказани су сивом бојом на слици 4.

Улога хибридног блока је да омогући изградњу функционалнијег система безбедности усаглашавањем формалних управних одлука и оперативних управљачких функција, чиме се омогућава ефикасно управљање ризицима. На тај начин, постиже се усклађивање рада формалног сектора који креира безбедносну политику и оперативног сектора који остварује управљање ризицима у реалном времену. Сектор хибридног блока би требало да садржи два дела: истраживачко-развојни и извршни део. Истраживачко-развојни део би требало да ради на изналажењу модела за доношење одлука и система комуникација који ће на бази анализе стања безбедности и уочених промена индикатора ризика омогућити ефикасно управљање. Извршни део се састоји из разних комуникационих модула неопходних за синхронизацију активности у реалном времену између формалних и оперативних актера у домену управљања ризицима.

Битне компоненте за управљање и мониторинг ризицима представља *Систем раној ујозорења*, који је неопходан за генерисање података у сврху управљања у ванредним ситуацијама. У оквиру реализованог CLD дијаграма приказан је и овај функционални блок, као и његове релације са осталим компонентама у оквиру система управљања ризицима (слика 4).

На основу приказаног CLD дијаграма, специјализовани софтвер за симулацију система формира одговарајући математички и симулациони модел. Вишеструким извршавањем симулационог модела, са различитим варијацијама параметара у моделу, може се вршити анализа понашања система за различите облике и узроке угрожавања. На основу резултата симулација могу се, затим, одредити оптималне управне и оперативне одлуке за управљање ризицима у реалном времену.

Применом симулационог софтвера могу се генерисати различите варијанте симулационих модела, са различитим варијацијама параметара система. Једна инстанца модела за управљање ризицима приказана је на слици 5.

Слика 5. Симулациони модел за управљање ризицима

Конкретан пример једне варијанте симулационог модела, као и детаљни резултати извршавања симулационог модела за управљање ризицима у систему корпоративне безбедности приказани су у литератури (Цигурски, 2018). У том примеру симулације, на корпоративни систем је деловао акцидент облика импулсног дејства на објекте и људе и то у дужем трајању. Затим се анализом, на основу добијених резултата симулација, у сврху ублажавања последица акцидента, доношењем одлука могу применити одговарајуће оперативне и формалне контроле у циљу стабилизације система и смањења ризика.

Закључак

У раду је приказан генерални приступ операционализацији у домену управљања ризицима. Овај приступ полази од онтолошког концепта безбедности, који затим води даље до одређивања системских архетипова који су релевантни за примену у области безбедности. Реализација, тј. операционализација селектованог архетипа за примену у области управљања ризицима, приликом конкретне примене, врши се применом методологије и помоћу средстава која се односе на анализу понашања сложених динамичких система из области Системске динамике.

Ово представља генерални приступ који полази од изабраног системског архетипа као генеричке форме, који се затим мапира на архетип за одговарајућу примену. На основу тога, даље се реализује логички концепт система у виду узрочно-последичног дијаграма који приказује ентитете и релације у систему. На основу претходног, применом специјали-

зованог софтвера за симулацију система генерише се инстанца модела, тј. одговарајући математички и симулациони модел. Вишеструким извршавањем симулационог модела, са различитим варијацијама параметара у моделу, може се вршити анализа понашања система за различите облике и узроке безбедносних угрожавања. На основу резултата симулација могу се затим одредити оптималне управне и оперативне одлуке за управљање ризицима у реалном времену.

Овакав приступ, на основу генерисаног модела који произилази из примењене методологије, омогућава детаљну структурну анализу проблема који постоје у неком систему за управљање ризицима. Поред тога, иста методологија омогућава и синтезу унапређеног модела и система управљања у којем би се елимисали или умањили постојећи ризици. На тај начин, може се демонстрирати значај Системског приступа који води преко системских архетипова до конкретне примене методологије Системске динамике система, као битних средстава за анализу и синтезу система управљања ризицима.

ЛИТЕРАТУРА

- Braun, W. (2002). *The System Archetypes*. Доступно на: https://www.albany.edu/faculty/gpr/PAD724/724WebArticles/sys_archetypes.pdf
- Forrester, J. W. (1961). *Industrial Dynamics*. Portland, OR: Productivity Press.
- Giddens, A. (1991). *Modernity and Self-identity: Self and Society in the Late Modern Age*. Stanford University Press.
- Herzog, A., Shahmehri, N. C. & Duma, C. (2007). An Ontology of Information Security, *International Journal of Information Security and Privacy*, 1(4), 1-23.
- Marais, K., Leveson N. G. (2006). Archetypes for Organizational Safety. *Safety Science*, 44(7), 565-582.
- Senge, P. M. (1990). *The Fifth Discipline: The Art & Practice of the Learning Organization*. New York: Doubleday Business.
- Simonović, S. (2011). *Systems Approach to Management of Disasters*. Hoboken, NJ: Wiley.
- Singhal, A. (2012). *Introducing the Knowledge Graph: Things, Not Strings*. Google Official Blog. Доступно на: <https://www.blog.google/products/search/introducing-knowledge-graph-things-not/> (приступљено 3. јула 2019).
- Sterman, J. D. (2002). System Dynamics: Systems Thinking and Modelling for a Complex World. *Proceedings of the ESD Internal Symposium*. Cambridge: MIT.
- Stevens, A. (2006). *The Archetypes*. In: Papadopoulos, R. K. (Ed.). (2006). *The Handbook of Jungian Psychology: Theory, Practice and Applications*. Psychology Press, 74-93.
- Vensim, Ventant Systems, Inc. (2015). Доступно на: www.vensim.com
- Wolstenholme, E. F. (2003). Toward the Definition and Use of a Core Set of Archetypal Structures in System Dynamics. *System Dynamics Review*, 19(1), 7-26.
- Џигурски, О. (2018). „Системско-структурни приступ у анализи и решавању безбедносних проблема корпорација: системски концепт.“ У: Кековић, З., Димитријевић, Р. И. и Шекарић, Н. (Прир.) (2018). *Корпоративна безбеднос – Хресїомаїија*. Београд: Факултет безбедности, 253-276.

SECURITY CONCEPT – SYSTEM APPROACH (SYSTEM ARCHETYPES IMPLEMENTATION IN RISK MANAGEMENT)

Ozren Džigurski, Associate Professor
University of Belgrade, Faculty of Security Studies

Summary

The security concept in this paper is considered from the aspect of corporate, organizational, business or human security. In this sense, in conceptual terms, a security system can be viewed as a complex system the variables of which are time-varying and to this end, methodology belonging to the field of System Dynamics can be implemented. This approach is adequate given that it enables the real operationalization of the security concept. The paper discusses the aspects of security concept derived from the systems approach, such as ontologies and system archetypes in the domain of security. This is the general approach that starts from the chosen system archetype as a generic form that is then mapped to the archetype for the specific, appropriate implementation. By applying the specialized system simulation software, an instance of the model, that is, a corresponding mathematical and simulation model is then generated. Based on the results of the simulations, optimal decisions for real-time risk management can be determined. The implementation of the systems approach, based on system archetypes, is presented on the example of risk management.

Keywords: *security, risks, archetype, system dynamics, computer simulation.*