საქართველოს ტექნიკური უნივერსიტეტი

გ. სურგულაძე, ბ. ურუშაძე

საინფორმაციო სისტემების მენეჯმენტის საერთაშორისო გამოცდილება (BSI, ITIL, COBIT)

რეკომენდებულია საქართველოს
ტექნიკური უნივერსიტეტის
სარედაქციო-საგამომცემლო საბჭოს
მიერ. 06.06.2014, ოქმი №2

თბილისი
2014

უაკ 004.5

კორპორაციული ობიექტების საინფორმაციო სისტემების ასაგებად განიხილება პროგრამული უზრუნველყოფის მენეჯმენტის ამოცანების გადაწყვეტის საერთაშორისო სტანდარტები და მეთოდოლოგიები, პროცესორიენტირებული დაპროექტების და სერვისორიენტირებული რეალიზაციის მიდგომებით. ინფორმაციული უსაფრთხოების საერთაშორისო სტანდარტების (BSI) გათვალისწინების და ინფორმაციული ტექნოლოგიების ინფრასტრუქტურის ბიბლიოთეკის (ITIL) საფუძველზე წარმოდგენილია პროგრამული სისტემების მენეჯმენტის სასიცოცხლო ციკლის ეტაპების ამოცანების დახასიათება, მოდელირება და ანალიზი, ორივე მეთოდოლოგიის ძირითადი ცნებები და მათი თანამოქმედების საფუძველზე შემუშავებული კონცეფცია კორპორაციული მართვის მხარდამჭერი სისტემის ასაგებად.

დამხმარე სახელმძღვანელო განკუთვნილია მართვის საინფორმაციო სისტემების (Management Information Systems) შექმნის საკითხებით დაინტერესებული სპეციალისტების, დოქტორანტების, მაგისტრანტების და სხვა სფეროს მკითხველთათვის, რომელთაც სურთ თავიანთი ბიზნეს-პროცესების სამართავად გამოიყენონ ახალი უსაფრთხო ინფორმაციული ტექნოლოგიები.

რეცენზენტები: სრული პროფესორი თ. სუხიაშვილი,
ასოცირებული პროფესორი კ. ოდიშარია

© საგამომცემლო სახლი „ტექნიკური უნივერსიტეტი", 2014
ISBN 978-9941-20-458-6
http://www.gtu.ge/publishinghouse/



ყველა უფლება დაცულია. ამ წიგნის ნებისმიერი ნაწილის (ტექსტი, ფოტო, ილუსტრაცია თუ სხვა) გამოყენება არც ერთი ფორმითა და საშუალებით (ელექტრონული თუ მექანიკური) არ შეიძლება გამომცემლის წერილობითი ნებართვის გარეშე.

საავტორო უფლებების დარღვევა ისჯება კანონით.

შინაარსი

	შესავალი ----------	9
I	ნაწილი: BSI	
1	თავი. შესავალი BSI სტანდარტში ----------	13
1.1.	მიზანი ----------	13
1.2.	ვისთვისაა ეს წიგნი	15
1.3.	გამოყენებული მეთოდები ----------	15
2	თავი. BSI და ინფორმაციული უსაფრთხოება ----------	17
2.1.	რა არის ინფორმაციული უსაფრთხოება ----------	17
2.2.	ტერმინების შესახებ ----------	18
2.3.	ინფორმაციული უსაფრთხოების სტანდარტები, მოკლე მიმოხილვა ----------	19
2.3.1.	ISO - სტანდარტები ინფორმაციული უსაფრთხოებისთვის ----------	19
2.3.2.	შერჩეული BSI პუბლიკაციები და ინფორმაციული უსაფრთხოების სტანდარტები ----------	22
2.3.2.1.	IT - საბაზო დაცვა - კატალოგები ----------	22
2.3.2.2.	BSI-სტანდარტები ინფორმაციული უსაფრთხოებისთვის: თემა IS-მენეჯმენტი ----------	24
2.3.3	სხვა სტანდარტები: COBIT, ITIL ----------	27
3	თავი. ინფორმაციული უსაფრთხოების მენეჯმენტის სისტემა (ISMS) და მისი პროცესების აღწერა ----	28
3.1.	ISMS -ის კომპონენტები ----------	28
3.2.	პროცესის აღწერა და სასიცოცხლო ციკლის მოდელი --	30
3.2.1.	სასიცოცხლო ციკლი ინფორმაციულ უსაფრთხოებაში -	30
3.2.2.	ინფორმაციული უსაფრთხოების პროცესების აღწერა --	32
4	თავი. მენეჯმენტის პრინციპები ----------	35
4.1.	მენეჯმენტის ამოცანები და მოვალეობები ----------	36
4.1.1.	ინფორმაციული უსაფრთხოებისთვის საერთო პასუხისმგებლობის აღება ----------	36
4.1.2.	ინფორმაციული უსაფრთხოების ინტეგრაცია	36

4.1.3.	ინფორმაციული უსაფრთხოების მართვა და მხარდაჭერა	37
4.1.4.	მიღწევადი მიზნების შერჩევა	38
4.1.5.	შეფასება: უსაფრთხოების ხარჯები vs სარგებელი	38
4.1.6.	როლური მოდელები (Role Models)	39
4.2.	ინფორმაციული უსაფრთხოების მხარდაჭერა და უწყვეტი სრულყოფა	39
4.3.	კომუნიკაცია და ცოდნა	41
5	თავი. რესურსები ინფორმაციული უსაფრთხოებისთვის	47
6	თავი. თანამშრომელთა ჩართვა უსაფრთხოების პროცესში	49
7	თავი. ინფორმაციული უსაფრთხოების პროცესი	50
7.1.	უსაფრთხოების პროცესის დაგეგმვა	50
7.1.1.	მოქმედების დიაპაზონის დადგენა, რომელშიც ISMS უნდა იქნას გამოყენებული	50
7.1.2.	გარემოს პირობების განსაზღვრა	51
7.1.3.	უსაფრთხოების მიზნების ფორმულირება და გზამკვლევი ინფორმაციული უასაფრთხოებისთვის	52
7.1.4.	ინფორმაციული უსაფრთხოების ორგანიზაციის აგება	52
7.2.	სახელმძღვანელო პოლიტიკის (კონცეფციის) დანერგვა ინფორმაციული უსაფრთხოებისთვის	53
7.3.	სახელმძღვანელო პოლიტიკის დანერგვა ინფორმაციული უსაფრთხოებისთვის	53
8	თავი. უსაფრთხოების კონცეფცია (პოლიტიკა)	56
8.1.	უსაფრთხოების კონცეფციის შექმნა	56
8.1.1.	რისკების შეფასების მეთოდის არჩევა	56
8.1.2.	რისკების ან დაზიანებების კლასიფიკაცია	58
8.1.3.	რისკების შეფასება	59
8.1.4.	სტრატეგიის დამუშავება რისკების დასამუშავებლად	60

8.1.5.	უსაფრთხოების ღონისძიებათა არჩევა	60
8.2.	უსაფრთხოების კონცეფციის რეალიზება	62
8.2.1.	რეალიზაციის გეგმის შექმნა უსაფრთხოების კონცეფციისთვის	62
8.2.2.	უსაფრთხოების ღონისძიებათა დანერგვა	62
8.2.3.	დანერგვის კონტროლი და მონიტორინგი	63
8.3.	შედეგების მონიტორინგი და უსაფრთხოების კონცეფციის სრულყოფა	63
9	თავი. BSI–ის ISMS: IT–საბაზო დაცვა	68
9.1.	შესავალი „IT-საბაზო–დაცვის“ მეთოდიკაში	68
9.2.	უსაფრთხოების პროცესი IT–საბაზო დაცვის მიხედვით	69
9.2.1.	რისკების შეფასება ინფორმაციულ უსაფრთხოებაში	70
9.2.2.	რისკების კლასიფიკაცია	73
9.2.3.	რისკის შეფასება	75
9.2.3.1.	სტრუქტურული ანალიზი: დაცვის ობიექტების იდენტიფიკაცია	75
9.2.3.2.	დაცვის მოთხოვნების დადგენა: უსაფრთხოების ინციდენტების გავლენის ანალიზი განსახილველ ბიზნესპროცესებზე	76
9.2.3.3.	უსაფრთხოების დამატებითი ანალიზი	77
9.3.	უსაფრთხოების კონცეფციის დანერგვა	79
II	ნაწილი: ITIL	81
10	თავი. ITIL - ინფორმაციული ტექნოლოგიების ინფრასტრუქტურის ბიბლიოთეკა	81
10.1.	შესავალი ITIL–ში: ძირითადი ტერმინები	81
10.2.	სერვისის სასიცოცხლო ციკლი	91
10.3.	სერვისების ცოდნის ბაზის მართვის სისტემა	97
11	თავი. სერვისების სტრატეგიის აგება	99
11.1.	სტრატეგიის აგება – სერვისების სასიცოცხლო ციკლის ეტაპი	99
11.2.	ფუნქციები და პროცესები სერვისის სასიცოცხლო ციკლში	102

11.3.	სერვისის ფასეულობაზე გავლენის მომხდენი ფაქტორები	105
11.4.	სერვისების მიმწოდებელთა ტიპები	107
11.5.	დაგეგმვის ფუნდამენტური საფუძვლები	115
11.6.	ოთხი „P“ სტრატეგიის ასაგებად	120
12	თავი. სერვისის მახასიათებლები	126
12.1.	სერვისის შესაძლებლობების და ფასეულობის განსაზღვრა	126
12.2.	სერვისების პორტფელის ფორმირება	133
12.3.	ფინანსების მართვა	143
12.4.	ინვესტიციების დაბრუნება	154
12.4.1.	ბიზნეს-კეისი	156
12.4.2.	წინაპროგრამული ROI	157
12.4.3.	პოსტპროექტული ROI	160
13	თავი. სერვისების დაპროექტება, როგორც სერვისების სასიცოცხლო ციკლის ეტაპი	163
13.1.	სერვისების დაპროექტება, როგორც სასიცოცხლო ციკლის ეტაპი	163
13.2.	დაპროექტების ძირითადი ასპექტები	176
13.2.1.	გადაწყვეტათა დაპროექტება	177
13.2.2.	მხარდამჭერი სისტემის სერვისების პორტფელის დაპროექტება	181
13.2.3.	ტექნოლოგიების არქიტექტურის დაპროექტება	184
13.2.4.	პროცესების დაპროექტება	189
13.2.5.	მეთოდების და მეტრიკების დაპროექტება გაზომვისთვის	192
13.3.	შემდგომი ქმედებები სერვისების დაპროექტების ჩარჩოებში	193
13.4.	სერვისების დაპროექტების და უზრუნველყოფის მოდელები	194
14	თავი. პროცესები დაპროექტების ეტაპის ფარგლებში: სერვისების კატალოგის, სიმძლავრეების და წვდომის მართვა	202

14.1.	სერვისების კატალოგის მართვა	202
14.2.	სერვისების დონის მართვა	208
14.3.	სიმძლავრების მართვა	218
14.4.	წვდომის მართვა	230
14.4.1.	რექტიური და პროაქტიური ქმედებები	234
14.4.2.	კრიტიკული ბიზნესფუნქცია	236
14.4.3.	წვდომის მართვის პროცესის ეფექტურობის შეფასება	241
15	თავი. სერვისების უწყვეტობის და ინფორმაციული უსაფრთხოების მართვა დაპროექტების ეტაპის ჩარჩოებში. მიმწოდებლების მართვა	243
15.1.	სერვისების უწყვეტობის მართვა	243
15.2.	ინფორმაციული უსაფრთხოების მართვა	262
15.3.	მიმწოდებლების მართვა	275
15.3.1.	ახალი მიმწოდებლების და კონტრაქტების შეფასება	279
15.3.2.	მიმწოდებლების კატეგორიები და SCD-ს მართვა	281
15.3.3.	ახალ მიმწოდებლებთან ურთიერთკავშირების დამყარება	284
15.3.4.	კონტრაქტების, მიმწოდებლების და მათი მწარმოებლურობის მართვა	284
15.3.5.	კონტრაქტების დასრულება და განახლება	285
16	თავი. დანერგვა - სერვისების სასიცოცხლო ციკლის ეტაპი	289
16.1.	სერვისების დანერგვის ეტაპის არსი და ტერმინები, მიზნები და ამოცანები	289
16.2.	დანერგვის ეტაპის ძირითადი პრინციპები	297
16.2.1.	დანერგვის ფორმალური პოლიტიკის განმარტება და განხორციელება	297
16.2.2.	ცვლილებების განხორციელება სერვისებში დანერგვის გზით	298

16.2.3. დანერგვის ზოგადი სტრუქტურის და სტანდარტების შემუშავება ---------- 300
16.2.4. დანერგვის გეგმების ფორმირება ბიზნესის მოთხოვნათა შესაბამისად ---------- 301

III ნაწილი: COBIT ---------- 303
17 თავი. COBIT სტანდარტული მეთოდოლოგია ---------- 303
17.1. COBIT- ტექნოლოგია და ძირითადი ტერმინები -------- 303
17.2. COBIT-ის მიზნები, პრინციპები და პროცესები --------- 305
17.3. COBIT-ის პროცესები ---------- 307
ლიტერატურა ---------- 312

შესავალი

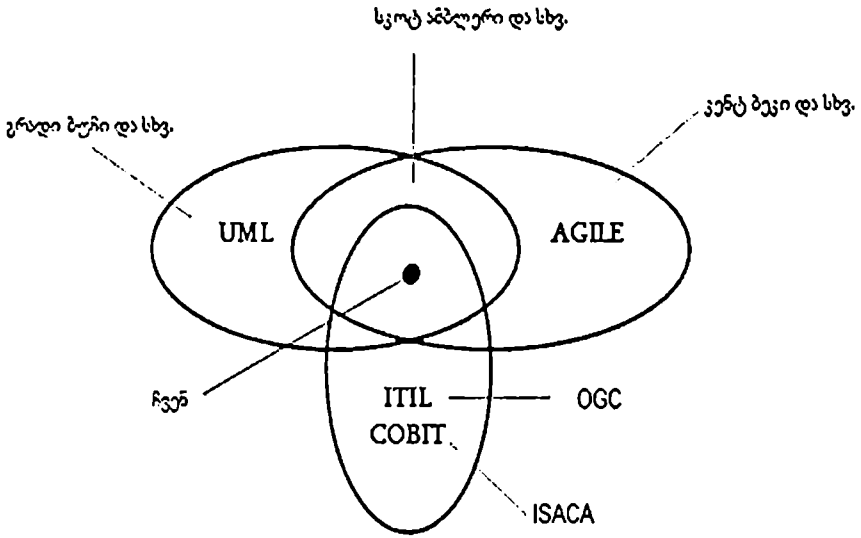
კორპორაციული ბიზნესპროცესების მენეჯმენტის მექანიზმების მუდმივი სრულყოფით შესაძლებელი ხდება მთლიანი სისტემის სასიცოცხლო ციკლის გახანგრძლივება, რაც უდავოდ აქტუალური საკითხია ინტეგრაციის და რეინჟინერინგის ამოცანების გადასაწყვეტად [1,2].

კორპორაციული ობიექტების მართვის საინფორმაციო სისტემის შექმნა მოიცავს ბიზნესპროცესების მოთხოვნილებათა განსაზღვრის, დიაგნოსტიკური ანალიზის, ბიზნეს-პროგრამების დაგეგმვის და პროექტირების, IT-სერვისების დადგენის, მათი განხორციელების ორგანიზების, ფაქტ-შედეგების აღრიცხვის, რისკების ანალიზის და შეფასების, ინფორმაციული უსაფრთხოების უზრუნველყოფის, ობიექტზე ეფექტური ზემოქმედების მმართველი გადაწყვეტილების მიღების პროცესების ხელშემწყობი მექანიზმების შემუშავებას და მათ კომპიუტერულ რეალიზაციას მენეჯმენტის საინფორმაციო სისტემების აგების თანამედროვე კონცეფციების საფუძველზე, როგორებიცაა ITIL და COBIT [3,4].

სრულყოფილი და საიმედო, მოქნილი პროგრამული უზრუნველყოფის (Software Engineering) სრულყოფილად და სწრაფად დაპროექტება, რეალიზაცია, დანერგვა და შემდგომი თანხლება სისტემის დამკვეთ ორგანიზაციაში მეტად მნიშვნელოვანი ამოცანაა და მისი ეფექტურად გადაწყვეტა ბევრადაა დამოკიდებული როგორც საპროექტო-დეველოპმენტის გუნდის შემადგენლობასა და გამოცდილებაზე, ასევე IT-ინფრასტრუქტურასა და CASE-ინსტრუმენტებზე, კერძოდ, UML და Agile მეთოდოლოგიების გამოყენებაზე [5-9, 16, 28].

1-ელ ნახაზზე მოცემულია პროგრამული სისტემების აგების პროცესში თანამედროვე ინფორმაციული ტექნოლოგიების

უნივერსალური, მოქნილი და უსაფრთხო სტანდარტების კომპლექსური გამოყენების კონცეფცია, რომლის საფუძველზე შესაძლებელია ეფექტური და საიმედო მენეჯმენტის განხორციელება.



ნახ. 1. პროგრამული სისტემების და IT-სერვისების მენეჯმენტის მეთოდოლოგიათა კვეთა:
- OGC (Office of Government Commerce) - სახელმწიფო სავაჭრო პალატა (დიდი ბრიტანეთი),
- ISACA (Information Systems Audit and Control Association) - საინფორმაციო სისტემების აუდიტის და კონტროლის ასოციაცია (აშშ)

სახელმწიფო ორგანიზაციების და კერძო ბიზნესის სფეროს მართვის საინფორმაციო სისტემების აგების ასეთი მიდგომა, ინფორმაციული უსაფრთხოების სისტემების თვალსაზრისით, ინტენსიურად განიხილება ამერიკის, ევროპის, რუსეთისა და სხვა ქვეყნების საუნივერსიტეტო-სამეცნიერო და სამრეწველო-

პრაქტიკული დანიშნულების ლიტერატურაში. წინამდებარე წიგნში შეტანილია ინგლისურ, გერმანულ და რუსულენოვანი ოფიციალური გამოცემების თარგმნის, გაანალიზების და ქართული, ორგანიზაციული მენეჯმენტის თვალსაზრისით ადაპტირებული მასალა, რომელიც ახალია ჩვენი მკითხველისთვის და უდავოდ სასარგებლო იქნება.

წიგნის პირველ ნაწილში, რომელიც ცხრა თავისგან შედგება, გადმოცემულია ინფორმაციული ტექნოლოგიების უსაფრთხო გამოყენების სტანდარტების არსი, მნიშვნელობა, დანიშნულება და საერთაშორისო მდგომარეობა. დეტალურად განიხილება BSI სტანდარტების სტრუქტურა და კომპონენტები, სტრატეგია და პრინციპები, რესურსები და პროცესები, რისკების ანალიზის, შეფასების და მონიტორინგის, რეალიზაციის და დანერგვის კონცეფციები. ნაჩვენებია BSI სტანდარტში ITIL და COBIT სისტემების ადგილი, როგორც პროგრამული უზრუნველყოფის მენეჯერის აუცილებელი მეთოდოლოგიური ინსტრუმენტი.

სახელმძღვანელოს მეორე ნაწილი, ექვსი თავით, ეხება ინფორმაციული ტექნოლოგიების ინფასტრუქტურის ბიბლიოთეკის (ITIL), როგორც უახლესი მეთოდოლოგიის, დეტალურ განხილვას; წარმოდგენილია ახალი ტერმინები, ცნებები და ამ სფეროში, სერვისებზე ორიენტირებული პროგრამული უზრუნველყოფის სასიცოცხლო ციკლის სტრუქტურა, მისი ცალკეული ფაზების და ამოცანების დახასიათებით. განიხილება სერვისების სტრატეგიის აგების, სერვისების დაპროექტების, სერვისების სიმძლავრეების და წვდომის მართვის საკითხები, რეაქტიური და პროაქტიური ქმედებების არსი, სერვისების უწყვეტობის და ინფორმაციული უსაფრთხოების მართვა დაპროექტების ეტაპის ფარგლებში, IT-სფეროს მიმწოდებლების და ბიზნესის სფეროს მომხმარებლების,

დამკვეთების და ინვესტორების ურთიერთდამოკიდებულებების და კონტრაქტების მართვის საკითხები. ბოლოს, განიხილება სერვისების დანერგვის ძირითადი პრინციპები, ბიზნესის მხარდაჭრის საკითხები ინფორმაციული სერვისების უწყვეტი განვითარებისა და ცვლილებების დანერგვის გზით.

წიგნის მესამე ნაწილში მოკლედაა განხილული COBIT სტანდარტის არსი, მისი მიზნები, პრინციპები და პროცესები.

დასასრულ, შეიძლება აღინიშნოს, რომ წარმოდგენილი ნაშრომი ქართულენოვან ტექნიკურ ლიტერატურაში არის პირველი მცდელობა მართვის საინფორმაციო სისტემების დაპროექტების და პროგრამული რეალიზაციის პროცესების განხილვისა, ინფორმაციული უსაფრთხოების დაცვის საერთაშორისო BSI სტანდარტების, ITIL და COBIT მეთოდოლოგიების კომპლექსური გამოყენების თვალსაზრისით.

საერთაშორისო მდგომარეობა და გამოცდილება ამ მიმართულებით გვიჩვენებს, რომ ჩვენ ქვეყანაშიც მომავალში აუცილებლად გაფართოვდება ინტერესი და სახელმწიფო და კერძო ბიზნესის ობიექტების დაინტერესება უსაფრთხო ინფორმაციული ტექნოლოგიების შექმნის და და მათი არსებულ სისტემებთან ინტეგრაციის საკითხებზე. მნიშვნელოვნად გვეჩვენება ასევე წინამდებარე ნაშრომის მასალის კავშირი სოციალური სისტემების, კერძოდ, ინფორმაციული სამართლის, როგორც მეცნიერული მიმართულების ჩამოყალიბების და განვითარების სფეროში.

ავტორები იტოვებენ იმედს და მადლიერების გრძნობით ელოდებიან აღნიშნული სფეროს სპეციალისტების და დაინტერესებული მკითხველის შენიშვნებს.

I ნაწილი
1. შესავალი BSI-ში
1.1. მიზანი

ინფორმაცია არის ხელისუფლების და კომპანიების მნიშვნელოვანი ფასეულობა და უნდა იყოს ადეკვატურად დაცული. ინფორმაციის უმეტესობა დღეისათვის, ნაწილობრივ მაინც, საინფორმაციო ტექნოლოგიებითაა (IT) შექმნილი, შენახული, ტრანსპორტირებული ან გადამუშავებული. ბიზნესისა და მართვის სფეროში არავინ არ კამათობს იმის შესახებ, რომ საჭიროა საკუთარი IT ლანდშაფტის შესაბამისი დაცვა. ამასთანავე ინფორმაცია ადეკვატურად უნდა იყოს დაცული ბიზნეს-პროცესების ყველა სხვა ფაზაზე [29-33]. უსაფრთხოების ინციდენტებს, მათ შორის ინფორმაციის გამჟღავნებას ან მანიპულირებას შეიძლება ჰქონდეს ბიზნესის დამაზიანებელი შორსმიმავალი ზემოქმედების უნარი ან აფერხებდეს ამოცანების შესრულებას, რაც იწვევს მაღალ ხარჯებს.

პრაქტიკამ გვიჩვენა, რომ უსაფრთხოების მენეჯმენტის ოპტიმიზაცია ხშირად ინფორმაციული უსაფრთხოებით უფრო ეფექტურად და სტაბილურად უმჯობესდება, ვიდრე უსაფრთხოების ტექნიკის ინვესტიციებით. ღონისძიებებს, რომლებიც ადრე იქნა დანერგილი ინფორმაციული უსაფრთხოების სრულყოფისათვის, შეუძლია ასევე უსაფრთხოების კონტექსტის გარეთ ჰქონდეს დადებითი გავლენა და წარმოაჩინოს იგი როგორც მომგებიანი. ინვესტიციებს ინფორმაციულ უსაფრთხოებაში შეუძლია ხელი შეუწყოს ხარჯების ეკონომიას, ხშირ შემთხვევაში - საშუალოვადიან პერსპექტივაშიც კი. დადებითი გვერდითი ეფექტების სახით განიხილება მაღალი სამუშაო ხარისხი, კლიენტთა ნდობის ამაღლება, IT ლანდშაფტის ოპტიმიზაცია და ორგანიზაციული პროცესები, ასევე სინერგიული ეფექტების

გამოყენება ინფორმაციული უსაფრთხოების მენეჯმენტის უკეთესი ინტეგრაციის საშუალებით არსებულ სტრუქტურებში.

ადეკვატური უსაფრთხოების დონე არის დამოკიდებული, პირველ რიგში, სისტემურ მიდგომაზე და შემდეგ - ინდივიდუალურ ტექნიკურ ღონისძიებებზე. შემდეგი მოსაზრებები განმარტავს ამ თეზისებს:

- ხელმძღვანელობის დონე პასუხისმგებელია, რათა იურიდიული კანონები და კონტრაქტები მესამე მხარესთან გათვალისინებულ იყოს და რომ მნიშვნელოვანი ბიზნეს–პროცესები მტყუნების გარეშე სრულდებოდეს;
- ინფორმაციულ უსაფრთხოებას აქვს ინტერფეისები დაწესებულების მრავალ სფეროსთან, იგი დაკავშირებულია მნიშვნელოვან ბიზნესპროცესებთან და ამოცანებთან. მხოლოდ ხელმძღვანელობის დონეს შეუძლია ინფორმაციული უსაფრთხოების მენეჯმენტის შეუფერხებელი ინტეგრაციის უზრუნველყოფა, არსებულ ორგანიზაციულ სტრუქტურებსა და პროცესებში.
- ხელმძღვანელობის დონე ამასთანავე პასუხისმგებელია რესურსების ეკონომიურ გამოყენებაზე.

ამგვარად, ხელმძღვანელობის დონეს აქვს დიდი პასუხისმგებლობა ინფორმაციული უზრუნველყოფისთვის. მართვის არარსებობას, არაადეკვატური უსაფრთხოების სტრატეგიას ან არასწორ გადაწყვეტილებებს შეიძლება ჰქონდეს შორს მიმავალი უარყოფითი ეფექტები როგორც უსაფრთხოების ინციდენტებზე, ასევე ხელიდან გაშვებულ შესაძლებლობებსა და ცუდ ინვესტიციებზე.

წინამდებარე სტანდარტი აღწერს ეტაპობრივად, ნაბიჯ–ნაბიჯ, თუ რას აკეთებს წარმატებული ინფორმაციული უსაფრთხოების მენეჯმენტი და რომელ ამოცანებს განიხილავენ ამ დროს კომპანიების და ხელისუფლების მართვის დონეები [29].

1.2. ვისთვისაა ეს წიგნი

ნაშრომი ორიენტირებულია პირებზე, რომლებიც პასუხისმგებელნი არიან IT–ოპერაციებსა და ინფორმაციულ უზრუნველყოფაზე, ექსპერტებზე, კონსულტანტებსა და სხვა დაინტერესებულ პირებზე, რომლებსაც ეხებათ ინფორმაციული უსაფრთხოების მართვის ფუნქციების შესრულება.

ინფორმაციული უსაფრთხოების ეფექტური და ეფექტიანი მართვა მნიშვნელოვანი საკითხია არა მხოლოდ მსხვილი დაწესებულებებისთვის, არამედ მცირე და საშუალო კორპორაციულ და კერძო ორგანიზაციებისთვის.

თუ როგორ გამოიყურება ინფორმაციული უსაფრთხოების მართვის მისაღები სისტემა, დამოკიდებულია თვით ორგანიზაციის ზომაზე. წინამდებარე სტანდარტი და განსაკუთრებით IT-დაცვის საფუძვლების კონკრეტული რეკომენდაციები დახმარებაა ნებისმიერი მენეჯერისთვის, რომელსაც სურს ინფორმაციული უსაფრთხოების სრულყოფა თავის სამოქმედო ზონაში. შემდგომში მოცემული იქნება ის მითითებებიც, თუ როგორ გამოვიყენოთ აუცილებლობის შემთხვევაში ამ სტანდარტის რჩევები ჩვენი ორგანიზაციის ზომებთან ადაპტირების პირობებში.

1.3. გამოყენებული მეთოდები

BSI - British Standards Institution (ბრიტანეთის სტანდარტების ინსტიტუტი) შეიქმნა 1901 წელს როგორც ინჟინრების კომიტეტი სტანდარტების განსაზღვრის საკითხებზე [34]. ამჟამად იგი სტანდარტების საერთაშორისო კომიტეტის (ISO) წევრია. მისი ჯგუფის ფუნქციებია:

- მენეჯმენტის სისტემებზე სერვისები და გადაწყვეტები;
- სერვისები შეფასებებზე და სერტიფიკაციაზე;

- პროდუქციის სერტიფიკაცია;
- მენეჯმენტის სისტემების სწავლება;
- სტანდარტები და გამოცემები;
- და სხვა.

წინამდებარე წიგნში ჩვენ ვიხილავთ გერმანიის საინფორმაციო ტექნოლოგიების უსაფრთხოების ფედერალურ ბიუროს (BSI - Bundesamt für Sicherheit in der Informationstechnik) მიერ შემუშავებულ სტანდარტებს [29-33]. მათ შორის BSI-Standard 100-1: Managementsysteme für Informations-sicherheit (ISMS) სტანდარტი აღწერს, თუ როგორ შეიძლება აიგოს ინფორმაციული უსაფრთხოების მენეჯმენტის სისტემა (ISMS).

მენეჯმენტის სისტემა მოიცავს ყველა წესს, რომლებიც ითვალისწინებს კონტროლს და მართვას ორგანიზაციის მიზნების მისაღწევად. ამგვარად, ინფორმაციული უსაფრთხოების მენეჯმენტის სისტემა, განსაზღვრავს თუ რომელ მეთოდებს და ინსტრუმენტებს მიმართავს გასაგებად ორგანიზაციის ხელმძღვანელობის დონე ინფორმაციულ უსაფრთხოებაზე ორიენტირებული ამოცანების და ქმედებებისათვის.

ეს BSI-სტანდარტი პასუხობს შემდეგ კითხვებს:

- რა არის მართვის საინფორმაციო უსაფრთხოების წარმატების ფაქტორები ?
- როგორ შეიძლება უსაფრთხოების პროცესის მართვა და მონიტორინგი საპასუხისმგებლო მენეჯმენტით ?
- როგორ ხდება უსაფრთხოების მიზნებისა და შესაბამისი უსაფრთხოების სტრატეგიის განვითარება ?
- როგორ შეირჩევა უსაფრთხოების ზომები და როგორ იქმნება უსაფრთხოების კონცეფცია (პოლიტიკა) ?
- როგორ შეიძლება უსაფრთხოების ერთხელ მიღწეული დონის შენარჩუნება და სრულყოფა ?

მენეჯმენტის ეს სტანდარტი მოკლედ და თვალნათლივ ასახავს ინფორმაციული უსაფრთხოების მენეჯმენტის უმნიშვნელოვანეს ამოცანებს. ამ რეკომენდაციების რეალიზაციის დროს BSI გვეხმარება IT-საბაზო დაცვის მეთოდიკით. IT-საბაზო დაცვა იძლევა ეტაპობრივ ინსტრუქციებს ინფორმაციული უსაფრთხოების მენეჯმენტის პრაქტიკაში დასამუშავებლად და კონკრეტულ ზომებს ინფორმაციული უსაფრთხოების ყველა ასპექტით.

IT-საბაზო დაცვის მეთოდიკა აღწერილია BSI-Standard 100-2-ში და ხელს უწყობს სათანადო დონის ინფორმაციული უსაფრთხოების მიღწევას შესაბამისი ეკონომიკური ეფექტით [30]. ამასთანავე რეკომენდებულია IT-საბაზო დაცვის სტანდარტული უსაფრთხოების ზომების კატალოგები უსაფრთხოების შესაბამისი დონის პრაქტიკული რეალიზაციისთვის.

2. BSI და ინფორმაციული უსაფრთხოება

2.1. რა არის ინფორმაციული უსაფრთხოება

ინფორმაციული უსაფრთხოების მიზანია ყველა სახის და წარმომავლობის ინფორმაციის დაცვა. ეს ინფორმაცია შეიძლება ინახებოდეს როგორც ქაღალდზე, ასევე კომპიუტერულ სისტემებში ან თუნდაც მომხმარებელთა გონებაში. IT-უსაფრთხოება იცავს პირველ რიგში ელექტრონულად შენახული ინფორმაციის უსაფრთხოებას და ზრუნავს მის დამუშავებაზე.

ინფორმაციული უსაფრთხოების კლასიკური საბაზო ფასეულობებია კონფიდენციალობა, მთლიანობა და წვდომა. მრავალი მომხმარებელი თავიანთ წამოდგენებში განიხილავს ასევე სხვა ფასეულობებსაც. ეს შეიძლება სასარგებლოც იყოს ინდივიდუალური აპლიკაციების თვალსაზრისით.

ინფორმაციული უსაფრთხოების სხვა გენერირებული ზოგადი ტერმინებია, მაგალითად, აუთენთიციტეტი, პასუხისმგებლობა, საიმედოობა და შეუფერხებლობა.

ინფორმაციის უსაფრთხოებას ემუქრება არა მხოლოდ განზრახ ქმედებები (მაგალითად, კომპიუტერული ვირუსები, ინფორმაციის წართმევა/მოსმენა, კომპიუტერის ქურდობა). შემდეგი მაგალითები იძლევა ამის ილუსტრაციას:

- დაუძლეველი ძალის მიერ (როგორიცაა ცეცხლი, წყალი, ქარიშხალი, მიწისძვრა) მედია-მატარებლები და IT-სისტემები დაზარალებულია ან ჩაშლილია ხელმისაწვდომობა მონაცემთა ცენტრში. დოკუმენტები, IT-სისტემები ან სამსახურები აღარაა სურვილისამებრ ხელმისაწვდომი;
- მას შემდეგ, რაც მოხდა წარუმატებელი პროგრამული განახლება, აპლიკაციები აღარ ფუნქციონირებს ან მონაცემები შეუმჩნევლად შეიცვალა;
- მნიშვნელოვანი ბიზნესპროცესი ჭიანურდება, რადგან ერთადერთი ადამიანი, რომელიც პროგრამებს იცნობს, ავადაა;
- კონფიდენციალური ინფორმაცია შემთხვევით გადაეცა არასანქცირებულ პირს, რადგან დოკუმენტები ან ფაილი არ იყო მონიშნული, როგორც „საიდუმლო".

2.2. ტერმინების შესახებ

გერმანულენოვან ლიტერატურაში ტერმინები „საინფორმაციო ტექნოლოგიები", „საინფორმაციო და საკომუნიკაციო ტექნოლოგიები" ან „საინფორმაციო და სატელეკომუნიკაციო ტექნოლოგიები" ხშირად გამოიყენება როგორც სინონიმები.

ამ ტერმინების სხვადასხვა სიგრძეების გამო, მიღებულია შესაბამისი შემოკლებების გამოყენება. ვინაიდან ინფორმაციის

ელექტრონული დამუშავება გავრცელებულია ცხოვრების თითქმის ყველა სფეროში, აღარ აქვს მნიშვნელობა განსხვავებას, ინფორმაცია მუშავდება ინფორმაციული ტექნოლოგით, საკომუნიკაციო ტექნოლოგიით თუ ქაღალდზე.

ტერმინი საინფორმაციო უსაფრთხოება, ნაცვლად IT უსაფრთხოებისა, ყოვლისმომცველია და ამიტომ უფრო შესაფერისი. თუმცა, ლიტერატურაში გამოიყენება ძირითადად ტერმინი „IT უსაფრთხოება" (რადგან ეს მოკლეა).

წინამდებარე ნაშრომშიც იქნება გამოყენებული ეს ტერმინი, ან შესაბამისი ტერმინი „IT საბაზო დაცვა".

2.3. ინფორმაციული უსაფრთხოების სტანდარტები – მოკლე მიმოხილვა

ინფორმაციული უსაფრთხოების სფეროში სხვადასხვა სტანდარტები შემუშავდა, რომლებშიც ნაწილობრივ სხვადასხვა მიზნობრივი ჯგუფები ან თემატური სფეროები არის წინა პლანზე წამოწეული. უსაფრთხოების სტანდარტების გამოყენება ბიზნესში ან ხელისუფლებაში არა მხოლოდ აუმჯობესებს უსაფრთხოების დონეს, ის ასევე ხელს უწყობს სხვადასხვა დაწესებულებებს შორის კოორდინაციას, რომლებშიც უსაფრთხოების ზომები უნდა განხორციელდეს ნებისმიერი ფორმით. ქვემოთ შემდეგი მიმოხილვა გვიჩვენებს ყველაზე მნიშვნელოვანი სტანდარტების მიმართულებებს.

2.3.1. I SO - სტანდარტები ინფორმაციული უსაფრთხოებისთვის

ISO და IEC საერთაშორისო ნორმების ორგანიზაციებში გადაწყდა, რომ ინფორმაციული უსაფრთხოების სტანდარტები გაერთიანებულიყო 2700x სერიაში, რომელიც მუდმივად იზრდება. მნიშვნელოვანი სტანდარტებია:

- ISO 2700x

ეს სტანდარტი იძლევა ზოგად მიმოხილვას ინფორმაციული უსაფრთხოების მენეჯმენტის სისტემების (ISMS) და მათი ურთიერთდამოკიდებულების შესახებ ISO 2700 x – ოჯახის სხვადასხვა სტანდარტებს შორის. აქვე გადმოცემულია ISMS-ის ძირითადი პრინციპები, კონცეფციები, ტერმინები და განსაზღვრებანი.

- ISO 27001

საინფორმაციო ტექნოლოგიების სირთულისა და სერთიფიკატებზე მოთხოვნების გამო ბოლო წლებში წარმოიშვა მრავალი ინსტრუქცია და ინფორმაციული უსაფრთხოების ეროვნული სტანდარტი. სტანდარტი ISO 27001 – "ინფორმაციული ტექნოლოგია – უსაფრთხოების ტექნიკა – ინფორმაციული უსაფრთხოების მართვის სისტემის მოთხოვნების სპეციფიკაცია" არის პირველი საერთაშორისო სტანდარტი ინფორმაციული უსაფრთხოების მართვაში, რომელიც ასევე სერტიფიცირების საშუალებას იძლევა. ISO 27001 იძლევა 10-გვერდიან ზოგად რეკომენდაციებს, მათ შორის შესავლის (დანერგვის), ექსპლუატაციის და დოკუმენტირებული ინფორმაციის უსაფრთხოების მართვის სისტემის სრულყოფისთვის,. ასევე რისკების გათვალისწინებით. ნორმატიულ დანართში მოხსენიებულია კონტროლი ISO / IEC 27002-დან. თუმცა, მკითხველი არ იღებს დახმარებას პრაქტიკული განხორციელებისთვის.

- ISO 27002

ISO 27002–ის (ყოფილი ISO 17799:2005) "ინფორმაციული ტექნოლოგიები – ინფორმაციული უსაფრთხოების მენეჯმენტის საპროცესო კოდექსი" მიზანია ინფორმაციული უსაფრთხოების მენეჯმენტის ჩარჩოს განსაზღვრა. ამიტომაც ISO 27002, პირველ

რიგში, ეხება აუცილებელ ბიჯებს (ეტაპებს), ფუნქციონირებადი უსაფრთხოების მენეჯმენტის ასაგებად და ორგანიზაციაში მიმაგრებას. აუცილებელი უსაფრთხოების ზომები მოკლედაა აღწერილი ISO-სტანდარტის ISO/IEC 27002–ში, დაახლოებით 100 გვერდზე. რეკომენდაციები განკუთვნილია მართვის დონისთვის და, შესაბამისად, შეიცავს მცირე კონკრეტულ ტექნიკურ შენიშვნებს. უსაფრთხოების ISO 27002-ის რეკომენდაციების რეალიზაცია არის ერთ–ერთი გზა მრავალი შესაძლებლობიდან, რომლებიც აკმაყოფილებს ISO სტანდარტის 27001-ის მოთხოვნებს.

შენიშვნა: ISO 17799 სტანდარტი 2007 წლის დასაწყისში გადაეცა არსებითი ცვლილებების გარეშე ISO 27002–ს, იმისათვის, რომ ხაზი გაესვათ მის მიკუთვნებაზე ISO 2700x სერიისთვის.

- ISO 27005

ISO–სტანდარტი „ინფორმაციული უსაფრთხოების რისკების მენეჯმენტი“ შეიცავს ძირითად რეკომენდაციებს რისკების მართვის შესახებ ინფორმაციული უსაფრთხოებისთვის. მათ შორის იგი მხარს უჭერს ISO/IEC 27001 სტანდარტის მოთხოვნების რეალიზაციას. ოღონდ აქ არავითარი მეთოდი რისკების მართვისთვის არაა მოცემული. ISO/IEC 27005 ცვლის ISO 13335-2 სტანდარტს. ეს სტანდარტი ISO 13335-2, „უსაფრთხოების ინფორმაციულ–კომუნიკაციური ტექნოლოგიები, ნაწ.2: რისკების მენეჯმენტის მეთოდები ინფორმაციულ უსაფრთხოებაში“, იძლეოდა ინსტრუქციებს ინფორმაციული უსაფრთხოების მენეჯმენტისთვის.

- ISO 27006

ISO-სტანდარტი 27006 „ინფორმაციული ტექნოლოგია – უსაფრთხოების უზრუნველყოფის მეთოდები – მოთხოვნები სერტიფიცირების აკრედიტაციული ორგანოების მიმართ ინფორმაციული უსაფრთხოების მენეჯმენტის სისტემებში“,

განსაზღვრავს აკრედიტაციის მოთხოვნებს სერტიფიცირების ორგანოებისთვის ISMS-ში და განიხილება ამ სერტიფიცირების პროცესების თავისებურებანი.

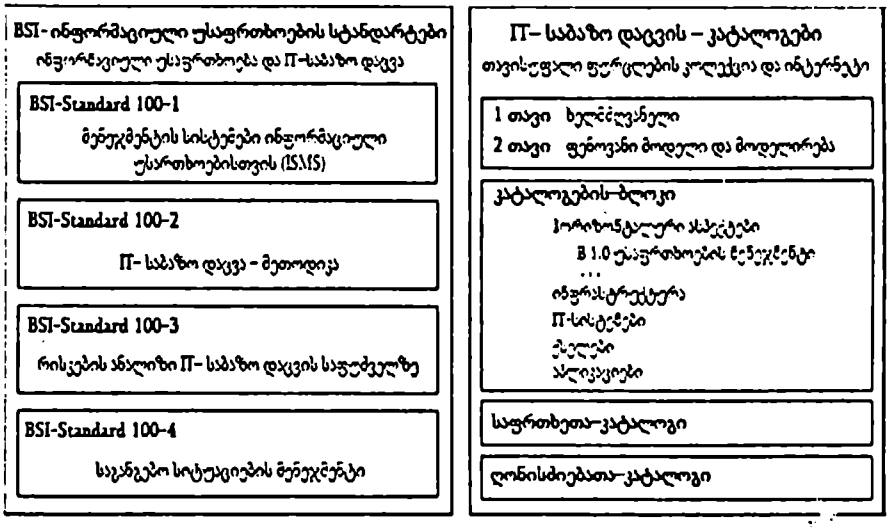
- ISO-2700x- რიგის სხვა სტანდარტები

ISO 2700x სტანდარტული სერია, სავარაუდოდ, გრძელვადიან პერსპექტივაში ISO სტანდარტების 27000-27019 27030-27044 სახით დაკომპლექტდება. ამ სერიის ყველა სტანდარტი მოიცავს უსაფრთხოების მართვის სხვადასხვა ასპექტებს და ეფუძნება ISO 27001–მოთხოვნებს. სხვა სტანდარტების მიზანია გაუმჯობესოს გაგება და პრაქტიკული გამოყენების ISO 27001–ის. ეს შეთანხმებაა, მაგალითად, ISO 27001-ის პრაქტიკული განხორციელებისთვის, ანუ რისკების შეფასება ან რისკების მართვის მეთოდებია.

2.3.2. შერჩეული BSI პუბლიკაციები და ინფორმაციული უსაფრთხოების სტანდარტები

2.3.2.1. IT – საბაზო დაცვა – კატალოგები

BSI-ის ყველაზე ცნობილი გამოცემა ინფორმაციულ უსაფრთხოებაში იყო 2005 წლამდე IT–საბაზო დაცვის სახელმძღვანელო, რომელშიც 1994 წლიდან აღწერილი იყო დეტალურად არა მხოლოდ ინფორმაციული უსაფრთხოების მენეჯმენტის, არამედ დეტალური უსაფრთხოების ზომები ტექნოლოგიის, ორგანიზაციის, პერსონალის და ინფრასტრუქტურის სფეროებში [29-32]. IT საბაზო დაცვის სახელმძღვანელო 2005–ში არა მარტო განახლდა, არამედ რესტრუქტურიზებაც განიცადა. ამასთანავე IT–საბაზო დაცვის და IT–საბაზო დაცვის კატალოგების პროცესების აღწერა გამოეყო ერთმანეთს (ნახ.1.1).



ნახ.1.1. უსაფრთხოების მენეჯმენტის BSI პუბლიკაციების მიმოხილვა

IT–საბაზო დაცვის კატალოგები აგებულია მოდულარულად და შეიცავს ტიპური პროცესების, პროგრამების და IT–კომპონენტების სამშენებლო ბლოკებს (მოდულებს). თითოეული თემისთვის რეკომენდებულია არა მხოლოდ უსაფრთხოების ზომების დასახელებები, არამედ აღიწერება აგრეთვე მნიშვნელოვანი (ძირითადი საფრთხეები) რისკებიც, რომელთაგანაც უნდა დაიცვას თავი დაწესებულებამ. მომხმარებლებს შეუძლიათ ამით ფოკუსირება კონკრეტულად მათი სფეროების შესაბამის სამშენებლო ბლოკებზე.

IT–საბაზო დაცვის კატალოგების სამშენებლო ბლოკები რეგულარულად აქტუალიზდება და ფართოვდება ახალი ტექნიკური განვითარების გათვალისწინებით. ამიტომაც ისინი პუბლიცირდება როგორც თავისუფალი ფურცლების კოლექცია, CD/DVD-ის სახით და, ამას გარდა, ინტერნეტშიც.

IT–საბაზო–დაცვის–მეთოდები აღწერს, თუ როგორ შეირჩევა სტანდარტული–უსაფრთხოების ზომებით უსაფრთხოების გადაწყვეტები, როგორ აიგება და გამოიცდება. ეს მეთოდები გამოქვეყნებულია როგორც BSI-Standard 100-2 სტანდარტი ინფორმაციული უსაფრთხოებისთვის.

2.3.2.2. BSI-სტანდარტები ინფორმაციული უსაფრთხოებისთვის: თემა IS-მენეჯმენტი

- **100-1 ინფორმაციული უსაფრთხოების მენეჯმენტის სისტემები (ISMS)**

ეს სტანდარტი განსაზღვრავს ISMS-ის ზოგად მოთხოვნებს. ეს არის სრულად თავსებადი ISO სტანდარტის 27001 და კვლავაც გაითვალისწინებს რეკომენდაციებს ISO სტანდარტების 27000 და 27002. იგი სთავაზობს მკითხველს ადვილად გასაგებ და სისტემატურ ინსტრუქციებს, მიუხედავად იმისა, თუ რომელი მეთოდის საშუალებით სურთ მათ მოთხოვნების განახორციელება.

BSI წარმოადგენს ISO სტანდარტის შინაარსს საკუთარ BSI სტანდარტში, გარკვეული საკითხების უფრო დეტალურად აღსაწერად, და ამით შინაარსის დიდაქტიკური წარმოდგენის საშუალება მიეცეს.

გარდა ამისა, სტრუქტურა იყო ისე დამუშავებული, რომ იგი თავსებადია IT-საბაზო დაცვის მეთოდებთან. უნიფიცირებული სათაურების საშუალებით აღნიშნულ დოკუმენტებში მკითხველისთვის ძალიან მარტივია ორიენტირება.

- **100-2 IT-საბაზო დაცვა–მეთოდკა**

IT–საბაზო–დაცვა–მეთოდიკა აღწერს ეტაპობრივად, ნაბიჯ–ნაბიჯ, თუ როგორ უნდა აიგოს ინფორმაციული უსაფრთხოების მენეჯმენტის სისტემა პრაქტიკულად და როგორ მოხდეს მისი

ექსპლუატაცია. ინფორმაციული უსაფრთხოების მენეჯმენტის ამოცანები და ორგანიზაციული სტრუქტურის აგება ინფორმაციული უსაფრთხოებისთვის ძალზე მნიშვნელოვანი თემებია. IT–საბაზო დაცვის მეთოდიკა დეტალურად განიხილავს იმას, თუ როგორ შეიძლება უსაფრთხოების კონცეფციის (პოლიტიკის) დამუშავება პრაქტიკაში, როგორ აირჩევა შესაბამისი უსაფრთხოების ზომები და რა შეიძლება ჩაითვალოს უსაფრთხოების კონცეფციის რეალიზაციად. ასევე საკითხი, თუ როგორ ხდება ინფორმაციული უსაფრთხოების მხარდაჭერა და სრულყოფა ექსპლუატაციის პირობებში, არის ამომწურავად პასუხგაცემული.

IT–საბაზო დაცვა BSI-Standard 100-2 სტანდარტთან კავშირში, ახდენს აქამდე დასახელებული 27000, 27001 და 27002 ISO-სტანდარტების ძალზე ზოგადად მიღებული მოთხოვნების ინტერპრეტირებას და ეხმარება მომხმარებლებს პრაქტიკაში რეალიზაციის დროს, მრავალი შენიშვნით, საცნობარო ინფორმაციით და მაგალითით.

IT–საბაზო დაცვის კატალოგები ხსნის არა მხოლოდ იმას, თუ *რა* უნდა გაკეთდეს, არამედ იძლევა ძალიან კონკრეტულ შენიშვნას, თუ *როგორ* უნდა გამოიყურებოდეს რეალიზაცია (ასევე ტექნიკურ დონეზე). პროცესი IT–საბაზო–დაცვის მიხედვით არის აპრობირებული და ეფექტური შესაძლებლობა, ზემოჩამოთვლილ ISO-სტანდარტის ყველა მოთხოვნის შესასრულებლად.

- 100-3 რისკების ანალიზი IT–საბაზო–დაცვის საფუძველზე

BSI-მ დაამუშავა რისკების ანალიზის მეთოდიკა IT–საბაზო–დაცვის საფუძველზე. მის გამოყენებას აზრი აქვს მაშინ, როცა კომპანიები ან სახელმწიფო დაწესებულებები მუშაობენ წარმატებით IT–საბაზო–დაცვასთან და უჩნდებათ სურვილი დამატებითი უსაფრთხოების ანალიზის ჩასატარებლად.

- **100-4 საგანგებო სიტუაციათა მენეჯმენტი**

BSI Standard 100-4 სტანდარტში ახსნილია სახელმწიფო დაწესებულებათა ან კომპანიების მასშტაბებში საგანგებო სიტუაციათა მენეჯმენტის აგების და ექსპლუატაციის მეთოდიკა. იგი ეფუძნება BSI-Standard 100-2 სტანდარტის IT–საბაზო–დაცვის–მეთოდიკას და აფართოებს მას თავის სასარგებლოდ.

- **ISO 27001 სერტიფიცირება IT–საბაზო–დაცვის საფუძველზე**

BSI ახდენს საინფორმაციო ქსელების სერტიფიცირებას, ანუ ინფრასტრუქტურული, ორგანიზაციული, პერსონალური და ტექნიკური კომპონენტების ურთიერთმოქმედებას, რომლებიც გამოიყენება ბიზნესპროცესების და ტექნიკური დავალებების სარეალიზაციოდ. BSI სერტიფიცირება მოიცავს გამოცდას როგორც ინფორმაციული უსაფრთხოების მენეჯმენტის სისტემებში, ასევე კონკრეტულ უსაფრთხოების ზომებში IT–საბაზო–დაცვის საფუძველზე. BSI სერტიფიცირება ამასთანავე ყოველთვის მოიცავს ოფიციალურ ISO–სერტიფიცირებას ISO 27001–ის მიხედვით, თუმცა ბევრად მნიშვნელოვანია, ვიდრე უბრალოდ ISO-სერტიფიცირება, დამატებითი კვლევით–ტექნიკური ასპექტების გამო. უსაფრთხოების მენეჯმენტის გამოცდის ძირითადი მოთხოვნები აუდიტის ჩარჩოებში აღმოცენდება უსაფრთხოების მენეჯმენტის საბაზო დაცვის ბლოკის (B 1.0) ღონისძიებებიდან. იგი ისეა დაწერილი, რომ ISMS-ის BSI–სტანდარტის მნიშვნელოვანი მოთხოვნები სწრაფად იყოს იდენტიფიცირებული. 1.1 ნახაზი იძლევა BSI–დოკუმენტების ზოგადი სტრუქტურის ილუსტრაციას.

ISO 27001 სტანდარტთან ადაპტირებისათვის ჩატარდა კორექტირებები სერტიფიცირების სქემაში ინფორმაციული ქსელებისთვის და სერტიფიცირების სქემაში აუდიტორებისთვის [35, 36].

2.3.3. სხვა სტანდარტები (COBIT, ITIL)

- COBIT

COBIT (Control Objectives for Information and related Technology – კონტროლის მიზნები ინფორმაციული და დაკავშირებული ტექნოლოგიებისთვის) აღწერს რისკების კონტროლის მეთოდს, რომელიც ხორციელდება IT–დანერგვის საშუალებით კრიტიკული ბიზნესპროცესების შესრულების მხარდასაჭერად [4]. COBIT–დოკუმენტები გაიცემა საინფორმაციო სისტემების აუდიტის და კონტროლის ასოციაციის (ISACA–Information Systems Audit and Control Association) IT მართვის ინსტიტუტის (ITGI – IT Governance Institute) მიერ. COBIT–ის დამუშავების დროს ავტორები ორიენტირებულნი იყვნენ უსაფრთხოების მენეჯმენტის არსებულ სტანდარტებზე, როგორიცაა ISO 27002.

- ITIL

IT Infrastructure Library (ITIL – IT ინფრასტრუქტურის ბიბლიოთეკა) არის IT სერვის მენეჯმენტის რამდენიმე წიგნის კოლექცია [3]. იგი შემუშავებულ იქნა გაერთიანებული სამეფოს სახელმწიფო კომერციის მთავრობის მიერ (OGC). ITIL განიხილავს IT–სერვისების მენეჯმენტს IT–მომსახურების თალსაზრისით. IT–მომსახურება შეიძლება იყოს როგორც შიგა IT–დეპარტამენტის ან გარე სერვისის პროვაიდერის. საერთო მიზანი არის IT მომსახურების და ხარჯების ეფექტურობის ოპტიმიზაცია და ხარისხის გაუმჯობესება.

ITIL ბიბლიოთეკა და COBIT სტანდარტი განხილული იქნება წიგნის მომდევნო თავებში.

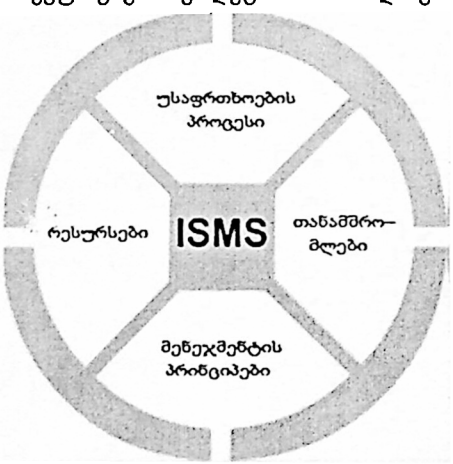
3. ინფორმაციული უსაფრთხოების მენეჯმენტის სისტემა (ISMS) და მისი პროცესების აღწერა

3.1. ISMS -ის კომპონენტები

სახელმწიფო დაწესებულებას და ყოველ კომპანიას აქვს მენეჯმენტი, რომელიც შემდგომში მოხსენიებულ იქნება როგორც „ხელმძღვანელობის დონე“, თუ პასუხისმგებელად ხელმძღვანელი ბალაა მოაზრებული და არსებობს უწესრიგობის რისკი „მენეჯმენტზე“, როგორც მართვის პროცესზე (Leiten-ხელმძღვანელობა, Lenken-გაძღოლა და Planen - დაგეგმვა) [29].

მენეჯმენტის სისტემა მოიცავს ყველა წესს, რომლებიც ორგანიზაციის მიზნის მიღწევისთვის კონტროლზე და მართვაზე ზრუნავს. მენეჯმენტის სისტემის ნაწილს, რომელიც დაკავებიულია ინფორმაციული უსაფრთხოებით, ISMS უწოდებენ.

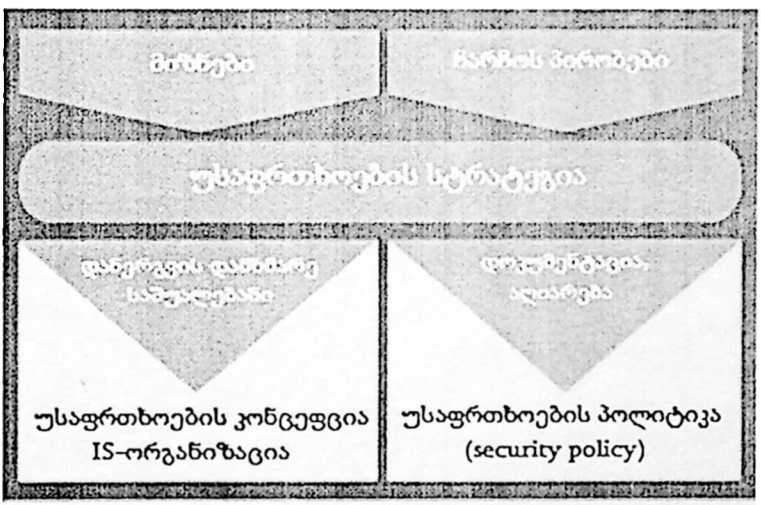
ISMS ამტკიცებს, თუ რომელი ინსტრუმენტებით და მეთოდებით მართავს (გეგმავს, ნერგავს, ასრულებს, აკონტროლებს და სრულყოფს) მენეჯმენტი ინფორმაციულ უსაფრთხოებაზე მიმართულ ამოცანებს და ქმედებებს მიზანმიმართულად. ISMS-ს მიეკუთვნება შემდეგი ძირითადი კომპონენტები (ნახ.1.2):



ნახ.1.2. ISMS–ის შედგენილობა

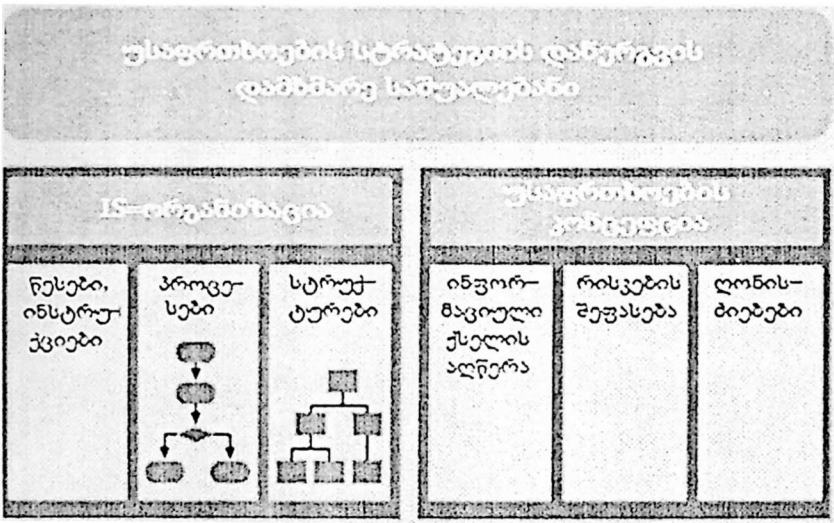
- მენეჯმენტის პრინციპები;
- რესურსები;
- თანამშრომლები;
- უსაფრთხოების პროცესი;
- ხელმძღვანელობა ინფორმაციული უსაფრთხოებისათვის, რომელშიც უსაფრთხოების მიზნები და სტრატეგია მისი რეალიზაციისთვის დოკუმენტირებულია;
- უსაფრთხოების კონცეფცია (პოლიტიკა);
- ინფორმაციული უსაფრთხოების ორგანიზაცია.

ინფორმაციული უსაფრთხოების ორგანიზაცია და უსაფრთხოების კონცეფცია არის მენეჯმენტის ინსტრუმენტი მისი უსაფრთხოების სტრატეგიის დასანერგად. მე-3 და მე-4 ნახაზები ამ დამოკიდებულებას ნათელს ჰფენს.



ნახ.3. ინფორმაციული უსაფრთხოების სტრატეგია, ISMS–ის მთავარი კომპონენტი

ინფორმაციის უსაფრთხოების უზრუნველყოფის მიზნით უსაფრთხოების სტრატეგიის ძირითადი პუნქტები აისახება სახელმძღვანელო პრინციპებში. უსაფრთხოების პოლიტიკას არსებითი მნიშვნელობა აქვს, რადგან იგი შეიცავს ხელმძღვანელობის ხილულ აღიარებას მათი სტრატეგიის შესახებ.



ნახ.4. უსაფრთხოების სტრატეგიის დანერგვა უსაფრთხოების კონცეფციის და ინფორმაციული უსაფრთხოების ორგანიზაციის დახმარებით

3.2. პროცესის აღწერა და სასიცოცხლო ციკლის მოდელი

3.2.1. სასიცოცხლო ციკლი ინფორმაციულ უსაფრთხოებაში

უსაფრთხოება არ არის უცვლელი მდგომარეობა, რომელიც მიიღწევა ერთხელ და შემდეგ არასდროს იცვლება. ყოველი დაწესებულება ექვემდებარება მუდმივ დინამიკურ ცვლილებებს.

მრავალი ცვლილება დაკავშირებულია ბიზნესპროცესების სპეციალიზებული ამოცანების, ინფრასტრუქტურის, ორგანიზაციული სტრუქტურების IT-ის და საინფორმაციო უსაფრთხოების ცვლილებებთან.

შესამჩნევ ცვლილებებთან ერთად დაწესებულების ფარგლებში იცვლება გარე პირობები, როგორიცაა სამართლებრივი ან ხელშეკრულებით გათვალისწინებული მოთხოვნები, აგრეთვე რადიკალურად შეიძლება შეიცვალოს არსებული ინფორმაციის ან საკომუნიკაციო ტექნოლოგიებიც. აქედან გამომდინარე, აუცილებელია უსაფრთხოების აქტიური მართვა, რათა შენარჩუნდეს უსაფრთხოების მიღწეული დონე.

არ არის საკმარისი, მაგალითად, რომ ბიზნესპროცესების დაგეგმვა ან ახალი IT-სისტემის დანერგვა და მიღებული უსაფრთხოების ზომები განხორციელდეს მხოლოდ ერთხელ. უსაფრთხოების ზომების განხორციელების შემდეგ ისინი რეგულარულად უნდა მოწმდებოდეს ეფექტურობასა და მიზანშეწონილობაზე, ასევე მათ გამოყენებადობასა და ფაქტობრივ გამოყენებაზე. უნდა მოიძებნოს სუსტი წერტილები ან გაუმჯობესების შესაძლებლობები, უნდა მოხდეს ღონისძიებათა ადაპტირება და გაუმჯობესება.

ეს ადაპტაციის საჭიროებით მოთხოვნილი ცვლილებები თავიდანვე უნდა დაიგეგმოს და განხორციელდეს. თუ ბიზნეს-პროცესები მთავრდება ან კომპონენტები და IT–სისტემები იცვლება ან ამოიღება მომსახურებიდან, მაშინ არსებული უსაფრთხოების ასპექტები უნდა გადაიხედოს (მაგალითად, პრივილეგიების ამოღება ან მყარი დისკების უსაფრთხო წაშალა).

უკეთესი სიცხადისთვის IT-საბაზო დაცვის კატალოგებში უსაფრთხოების ზომები გადანაწილდება შემდეგ ფაზებში:

- დაგეგმვა და კონცეფცია;

- შესყიდვა (საჭიროების შემთხვევაში);
- დანერგვა;
- ექსპლუატაცია (ზომები ექსპლუატაციაში ინფორმაციის უსაფრთხოების მხარდასაჭერად მოიცავს მონიტორინგს და შედეგების კონტროლს);
- გამოყოფა (საჭიროების შემთხვევაში);
- საგანგებო სიტუაციებისადმი მზადყოფნა.

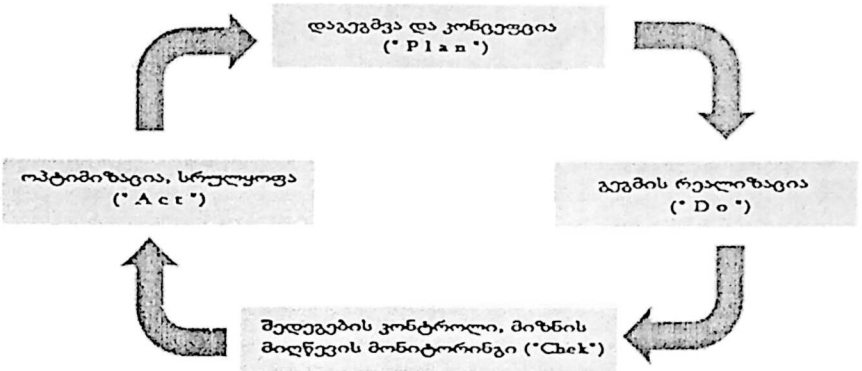
3.2.2. ინფორმაციული უსაფრთხოების პროცესების აღწერა

არა მხოლოდ ბიზნესპროცესებს და IT-სისტემებს აქვს „სასიცოცხლო ციკლები“. იგი გააჩნია ასევე უსაფრთხოების კონცეფციას, ინფორმაციული უსაფრთხოების ორგანიზაციას და, ბოლოს, თვით მთლიან უსაფრთხოების პროცესს. უსაფრთხოების პროცესის დინამიკის მარტივად აღწერის მიზნით, იგი ლიტერატურაში ხშირად წარმოდგენილია შემდეგი ფაზებით:

1. დაგეგმვა;
2. დაგეგმილის დანერგვა ან პროექტის რეალიზაცია;
3. შედეგების კონტროლი ან მიზნის მიღწევის მონიტორინგი;
4. გამოვლენილი დეფექტების და ნაკლოვანებების აღმოფხვრა ან ოპტიმიზაცია და სრულყოფა.

მე-4 ფაზა აღწერს მცირე დეფექტების დაუყოვნებლივ აღმოფხვრას. საფუძვლიანი ან მრავალი ცვლილებების მიზნით პროცესი უეჭველად უნდა დაიწყოს ისევ დაგეგმვის ფაზიდან.

მე-5 ნახაზზე მოცემულია მოდელი, ცალკეული ფაზების ინგლისური ქვეაღნიშვნებით („Plan", „Do", „Check", „Act") ან აღსაძნულია როგორც PDCA–მოდელი.



ნახ.5. სასიცოცხლო ციკლი Deming-ის მიხედვით
(PDCA-მოდელი)

PDCA–მოდელი არის ასევე ISO-Standard 27001 სტანდარტშიც. მისი გამოყენება პრინციპულად შესაძლებელია უსაფრთხოების პროცესის ყველა ამოცანისთვის. ასევე უსაფრთხოების კონცეფციის და ინფორმაციული უსაფრთხოების ორგანიზაციის სასიცოცხლო ციკლები შეიძლება ძალზე გასაგებად აღიწეროს. ამ დოკუმენტის ეს თავი ეხება სწორედ სასიცოცხლო ციკლის მოდელის ოთხ ფაზას.

ინფორმაციული უსაფრთხოების პროცესის დაგეგმვის ფაზაზე ხდება ჩარჩოს იმ (საბაზო) პირობების ანალიზი, რომელიც უსაფრთხოების მიზნებს განსაზღვრავს და უსაფრთხოების სტრატეგიას ამუშავებს. ამავე დროს შეიცავს საფუძვლიან მტკიცებებს, თუ როგორ უნდა იქნას მიღწეული დასახული მიზნები.

უსაფრთხოების სტარატეგია ხორციელდება უსაფრთხოების კონცეფციის და შესაფერისი სტრუქტურის დახმარებით ინფორმაციიული უსაფრთხოების ორგანიზაციისთვის.

უსაფრთხოების კონცეფცია და ინფორმაციული უსაფრთხოების ორგანიზაცია თავიდან უნდა დაიგეგმოს და შედეგების კონტროლის შესაბამისად მოხდეს მისი რეალიზება.

ზედა დონის ინფორმაციული უსაფრთხოების შედეგების კონტროლის დროს რეგულარულად მოწმდება, არის თუ არა ჩარჩოს პირობები (მაგალითად, კანონები ან ბიზნესმიზნები) შეცვლილი და აღმოჩნდა თუ არა უსაფრთხოების კონცეფცია და ინფორმაციული უსაფრთხოების ორგანიზაცია ეფექტური და მოქმედი.

ვინაიდან სხვადასხვა დაწესებულებას აქვს სხვადასხვა საწყისი პირობები, უსაფრთხოების მოთხოვნები და ფინანსური საშუალებები, ეს მეთოდი ნამდვილად გვთავაზობს ეფექტურ ორიენტაციას, თუმცა იგი ადაპტირებული უნდა იყოს ყოველ კომპანიასა და დაწესებულებაზე თავის საკუთარ მოთხოვნილებებზე. ყოველი დაწესებულება ინდივიდუალურად განსაზღვრავს ან აკონკრეტებს, თუ რომელი ფორმის სასიცოცხლო ციკლის მოდელია მისთვის მისაღები.

მცირე დაწესებულებები და კომპანიები არ უნდა შეშინდნენ, რადგან უსაფრთხოების პროცესის ხარჯები, როგორც წესი, ორგანიზაციის ზომებზეა დამოკიდებული. ამგვარად, ძალიან დიდ კომპანიაში, რომელსაც მრავალი განყოფილება და თანამშრომელი ჰყავს, ალბათ მოითხოვს უფრო ფორმალურ პროცესს და ზუსტად ამტკიცებს, თუ რომელი შიგა და გარე აუდიტებია საჭირო, ვინ ვისთანაა პასუხისმგებელი, ვინ ქმნის გადაწყვეტილებათა დოკუმენტებს, როდის იძლევა ხელმძღვანელობა უსაფრთხოების პროცესზე კონსულტაციას.

მცირე ბიზნესში ესაა ყოველწლიური შეხვედრა კომპანიის ხელმძღვანელსა და მის IT–მიმწოდებელს შორის, რომლის დროსაც განიხილება წინა წლის პრობლემები, ხარჯები, ახალი ტექნიკური გადაწყვეტები და სხვა ადაპტირებული ფაქტორები, რათა უსაფრთხოების პროცესის წარმატება კრიტიკულად განიხილოს.

4. მენეჯმენტის პრინციპები

ინფორმაციული უსაფრთხოების მენეჯმენტით ან მოკლედ IS-მენეჯმენტით აღნიშნავენ დაგეგმვის და მართვის ამოცანებს, რომლებიც საჭიროა შინაარსიანი სტრუქტურის, პრაქტიკული რეალიზებადობის და გააზრებული და გეგმაზომიერი უსაფრთხოების პროცესების ეფექტურობის უზრუნველსაყოფად, ასევე ყველა მასთან დაკავშირებული უსაფრთხოების ღონისძიებებისთვის.

იგი მოიცავს ასევე საკანონმდებლო მოთხოვნების შესრულებას და ყველა აუცილებელი სამართლებრივი აქტის დაცვას. არსებობს განსხვავებული კონცეფციები, თუ როგორ უნდა გამოიყურებოდეს ეფექტური IS–მენეჯმენტი და რომელი ორგანიზაციული სტრუქტურებია ამისთვის გამოსადეგი. იმისგან დამოუკიდებლად, თუ როგორ გამოიყურება IS–მენეჯმენტის სისტემა, მისთვის საჭიროა ფუნდამენტური პრინციპების გათვალისწინება.

აქ წარმოდგენილი მენეჯმენტის ზოგიერთი პრინციპი შეიძლება ბანალურად ჟღერდეს, მათ დანერგვას ხშირად ხელმძღვანელები თვლიან როგორც აშკარად ბუნებრივს.

პარადოქსულია, მაგრამ ასეთი მარტივი მეთოდები ხშირად პრაქტიკაში არასწორად გამოიყენება ან საერთოდ უგულებელიყოფა. დისციპლინა, მოთმინება, აღებული პასუხისმგებლობები, ასევე რეალური და ყურადღებით მომზადებული პროექტები მრავალ ორგანიზაციაში თეორიულად აღიარებულია, მაგრამ პრაქტიკაში ყოველთვის ვერ გამოიყენება.

ცოტაა თვალსაჩინო ღონისძიებები, როგორიცაა პროცესების ოპტიმიზაცია, განათლება და თანამშრომელთა მოტივაცია ან გასაგები დოკუმენტაციის მომზადება, რომლებიც თვალნათლივ აუმჯობესებენ უსაფრთხოების დონეს პრაქტიკაში. კომპლექსური

და ამასთანავე ძვირად ღირებული ღონისძიებები, დიდი პროექტები და ინვესტიციები ტექნოლოგიაში ხშირად სრულიად არასწორადაა წარმოდგენილი როგორც ეფექტური. ხშირად პასუხისმგებლები არიან ხარჯების განმკარგავები, უსაფრთხოების ღონისძიებების ცუდ რეპუტაციაზე.

შემდეგში წარმოდგენილ იქნება მენეჯმენტის პრინციპები, რომელთა გათვალისწინება კარგი საფუძველია ინფორმაციული უსაფრთხოების წარმატებული მენეჯმენტისთვის.

4.1. მენეჯმენტის ამოცანები და მოვალეობები

ხელმძღვანელობის დონის ამოცანები და ვალდებულებები ინფორმაციული უსაფრთხოების მიმართებით შეიძლება შემდეგი პუნქტებით ჩამოვაყალიბოთ:

4.1.1. ინფორმაციული უსაფრთხოებისთვის საერთო პასუხისმგებლობის აღება

ყოველი დაწესებულების ან კომპანიის უმაღლესი მენეჯმენტის დონე პასუხისმგებელია ორგანიზაციის მიზანმიმართული და გამართული ფუნქციონირებისათვის და გამომდინარე აქედან - ინფორმაციული უსაფრთხოების უზრუნველყოფისათვის შიგნით და გარეთ. ეს შეიძლება აგრეთვე რეგულირდეს, ქვეყნის და ორგანიზაციული ფორმის მიხედვით, სხვადასხვა კანონებით. მართვის დონე, ასევე ნებისმიერი ცალკეული მენეჯერი, ვალდებულია გაითავისოს საკუთარი პასუხისმგებლობა და ნათლად აუხსნას თანამშრომლებსაც ინფორმაციული უსაფრთხოების მნიშვნელობა.

4.1.2. ინფორმაციული უსაფრთხოების ინტეგრაცია

ინფორმაციული უსაფრთხოება უნდა იყოს ინტეგრირებული ორგანიზაციის ყველა პროცესსა და პროექტში, რომლებშიც ინფორმაცია მუშავდება და გამოიყენება IT–ს მიერ. ეს ნიშნავს,

მაგალითად, რომ უსაფრთხოების მოთხოვნები უნდა იყოს განხილული არა მხოლოდ IT–ს შესყიდვის დროს, არამედ ბიზნეს–პროცესების დიზაინის (დაპროექტების) დროსაც, ასევე თანამშრომელთა მომზადების დროსაც.

4.1.3. ინფორმაციული უსაფრთხოების მართვა და მხარდაჭერა

ხელმძღვანელობის დონე აქტიურად უნდა აინიციირებდეს, მართავდეს და აკონტროლებდეს უსაფრთხოების პროცესს. ამისთვის განიხილება შემდეგი ამოცანები:

- მიღებულ უნდა იქნას ინფორმაციული უსაფრთხოების სტრატეგია და უსაფრთხოების მიზნები;
- უსაფრთხოების რისკების გავლენა ბიზნესზე ან ამოცანების შესრულებაზე უნდა იქნას გამოკვლეული;
- უნდა შეიქმნას ორგანიზაციული ჩარჩოს პირობები ინფორმაციული უსაფრთხოებითვის;
- ინფორმაციული უსაფრთხოებითვის უნდა გამოიყოს საკმარისი რესურსები;
- უსაფრთხოების სტრატეგია სისტემატურად უნდა მოწმდებოდეს და ტარდებოდეს მიზნის მიღწევის მონიტორინგი. გამოვლენილი ნაკლოვანებანი და შეცდომები უნდა გასწორდეს. ამისათვის უნდა შეიქმნას „ნოვატორული“ სამუშაო კლიმატი და ორგანიზაციის შიგნით მუდმივი სრულყოფის ნების დემონსტრირება;
- თანამშრომლები მოტივირებული უნდა იყვნენ უსაფრთხოების საკითხებზე და ინფორმაციული უსაფრთხოება განიხილონ როგორც თავიანთი ამოცანების მნიშვნელოვანი ასპექტი. ამისათვის საჭიროა, სხვებთან ერთად, საკმარისი საინფორმაციო-საგანმანათლებლო ღონისძიებების შეთავაზება.

4.1.4. მიღწევადი მიზნების შერჩევა

პროექტები ხშირად ვერ სრულდება (ჩავარდნა) არარეალური ან ამბიციური მიზნების დასმის გამო. ეს ასევეა ინფორმაციული უსაფრთხოების სფეროშიც. ამიტომ უსაფრთხოების სტრატეგია უნდა იყოს შეთანხმებული არსებულ რესურსებთან. იმისათვის, რომ მიღწეულ იქნას უსაფრთხოების აუცილებელი მიზნები, შეიძლება მრავალი მცირებიჯიანი და გრძელვადიანი, უწყვეტი სრულყოფის პროცესის დაწყება მაღალი საინვესტიციო ხარჯების გარეშე უფრო ეფექტურად, ვიდრე ერთი დიდმასშტაბიანი პროექტის დროს იქნებოდა. ამიტომ შეიძლება მიზანშეწონილი იყოს, უსაფრთხოების მოთხოვნილი დონის რეალიზება მხოლოდ შერჩეულ უბნებზე. ამის შემდეგ კი უსაფრთხოების მოთხოვნილი დონე განხორციელდება მთლიანი ორგანიზაციისთვის.

4.1.5. შეფასება: უსაფრთხოების ხარჯები vs სარგებელი

ერთ-ერთი ურთულესი ამოცანა ისაა, რომ ინფორმაციული უსაფრთხოების ხარჯები შეფასდეს სარგებელის და რისკების მიმართებით. ძალზე მნიშვნელოვანია, თავდაპირველად იმ ღონისძიებების ინვესტირება, რომლებიც განსაკუთრებით ეფექტურია ან განსაკუთრებით მაღალი რისკების წინააღმდეგაა მიმართული. მაღალეფექტური ღონისძიებები, პრაქტიკული გამოცდილებით, არაა ყოველთვის უძვირესი. ამიტომაც ძალზე მნიშვნელოვანია, ბიზნესპროცესების დამოკიდებულების ცოდნა ინფორმაციის დამუშავების ამოცანებთან, რათა შესაბამისი უსაფრთხოების ზომების შერჩევა შეიძლებოდეს.

ამასთან შეიძლება ითქვას, რომ ინფორმაციის უსაფრთხოება ყოველთვის მიიღწევა ტექნიკური და ორგანიზაციული ზომების ურთიერთქმედებით. ინვესტიციები ტექნოლოგიებზე უშუალოდ ბიუჯეტშია ასახული. ამგვარად, ეს ხარჯები გამართლებულია. უსაფრთხოების პროდუქტები ისე უნდა დაინერგოს, რომ

ოპტიმალური სარგებელი მოიტანოს. ამიტომ ისინი უნდა შეიქმნას ისე, რომ ისინი მიზანმიმართულად და შესაფერისად მოქმედებდეს, მაგალითად, უნდა იყოს ინტეგრირებული უსაფრთხოების ერთიან კონცეფციაში და თანამშრომლებმა უნდა შეისწავლონ მათი გამოყენება.

ხშირად ტექნიკური გადაწყვეტები შეიძლება ასევე უსაფრთხოების ორგანიზაციული ღონისძიებებით ჩანაცვლდეს. პრაქტიკული გამოცდილება გვიჩვენებს, რომ მისი უზრუნველყოფა რთულია, რომ ორგანიზაციული ზომები მიმდევრობით ხორციელდება. ამას გარდა, იგი ზრდის პერსონალის ხარჯს და ტვირთავს რესურსებს.

4.1.6. როლური მოდელები (Role Models)

ინფორმაციული უსაფრთხოების სფეროში ხელმძღვანელობამ თავის თავზე უნდა აიღოს „როლური მოდელი“, რაც ნიშნავს „იდეალურ ნიმუშს“ სხვებისთვის. აქ იგულისხმება, რომ ხელმძღვანელობამ უნდა დაიცვას ყველა გათვალისწინებული უსაფრთხოების წესი, თვითონაც მონაწილეობდეს ინფორმაციული უსაფრთხოების ღონისძიებათა გატარებასა და დაცვაში, აგრეთვე სწავლების ღონისძიებებშიც.

4.2. ინფორმაციული უსაფრთხოების მხარდაჭერა და უწყვეტი სრულყოფა

ინფორმაციული უსაფრთხოების შექმნა არაა დროში შეზღუდული პროექტი, მაგრამ უწყვეტი პროცესია. მენეჯმენტის სისტემის ყველა ელემენტის ადაპტირება და ეფექტურობა ინფორმაციული უზრუნველყოფისთვის სისტემატურად უნდა მოწმდებოდეს. ეს ნიშნავს, რომ არა მხოლოდ ცალკეული უსაფრთხოების ზომები უნდა იყოს შემოწმებული, არამედ სისტემატურად უნდა გადაისინჯოს უსაფრთხოების სტრატეგიაც.

უსაფრთხოების უზრუნველყოფის ზომების რეალიზაცია უნდა შეფასდეს რეგულარულ საფუძველზე შიგა აუდიტების მიერ. მათ ფუნქციებში შედის ასევე ყოველდღიური პრაქტიკის გამოცდილების შეკრება და შეფასება. აუდიტთან ერთად საჭიროა ტრეინინგების და ცნობიერების ამაღლების ღონისძიებათა ჩატარება, რადგან მხოლოდ ასე შეიძლება დამტკიცდეს, ფაქტობრივად ფუნქციონირებს თუ არა ყველა გათვალისწინებული პროცესი და ქმედება საგანგებო სიტუაციებზე.

დასკვნებმა სუსტი ადგილებისა და სრულყოფის შესაძლებლობათა შესახებ გამონაკლისების გარეშე უნდა მიგვიყვანოს შედეგებამდე ინფორმაციული უსაფრთხოების ორგანიზაციაში. ამას გარდა, მნიშვნელოვანია სამომავლო განვითარების წინასწარ განჭვრეტა როგორც დანერგილი ტექნიკის, ასევე ბიზნესპროცესებსა და ორგანიზაციულ სტრუქტურებში, რათა დროულად იქნას შესაძლო რისკები იდენტიფიცირებული, მიღებულ იქნას გამაფრთხილებელი ზომები და უსაფრთხოების ღონისძიებები დანერგილი.

თუ წარმოიშობა მნიშვნელოვანი ცვლილებები ბიზნეს–პროცესებში ან ორგანიზაციულ სტრუქტურებში, აქ უნდა ჩაერთოს ინფორმაციული უსაფრთხოების მენეჯმენტი. აგრეთვე, არ უნდა ველოდოთ ორგანიზაციის განკარგულებებით წინასწარ გათვალისწინებულ ეტაპებს, არამედ დროულად უნდა მოხდეს ერთმანეთზე დამოკიდებული პროცესების ინტეგრირება.

ყველა აუდიტის დროს უნდა მიექცეს ყურადღება იმას, რომ ისინი არ ჩაატარონ იმათ, ვინც მონაწილეობდა უსაფრთხოების მოთხოვნათა დაგეგმვისა და კონცეფციის ეტაპებზე, რადგან ძნელია საკუთარი შეცდომების პოვნა. დიდ ორგანიზაციებში სასურველია კონსულტირება გარე აუდიტებთან, რათა აღმოიფხვრას ექსპლუატაციის სიბრმავე (organizational blindness).

მცირე და საშუალო ბიზნესისთვის, აგრეთვე მნიშვნელოვანი მომენტია ინფორმაციული უსაფრთხოების მხარდაჭერა. აუდიტები იქნება ნაკლებად მოცულობითი, ვიდრე დიდ დაწესებულებებში მაგრამ არავითარ შემთხვევაში არ უნდა იყოს გამოტოვებული. ყოველწლიური მენეჯმენტური შეფასების ფარგლებში უმაღლესი ხელმძღვანელობის დონეც უნდა გადამოწმდეს, ხომ არ იყო ახალი კანონმდებლური მოთხოვნები, რომლებიც შესრულებას მოითხოვდა ან ხომ არ შეიცვალა ჩარჩოს სხვა პირობები.

უსაფრთხოების პროცესის შემოწმება საბოლოო ჯამში ემსახურება მის სრულყოფას. შედეგები ისე უნდა იქნას გამოყენებული, რომ ეფექტურობა და მწარმოებლურობა უსაფრთხოების არჩეული სტრატეგიისათვის შეფასდეს და შესაძლოდ ადაპტირდეს. აგრეთვე შესაბამისად უნდა გადამუშავდეს უსაფრთხოების სტრატეგია უსაფრთხოების მიზნების ან ჩარჩოს პირობების ცვლილებისას.

ეს საკითხი მე-7 თავში დეტალურად იქნება განხილული.

4.3. კომუნიკაცია და ცოდნა

უსაფრთხოების პროცესის ყველა ფაზაზე კომუნიკაცია არის მნიშვნელოვანი ქვაკუთხედი, რათა დასახული მიზნები იქნას მიღწეული. გაუგებრობები და ცოდნის უქონლობა არის უსაფრთხოების პრობლემების გაჩენის ყველაზე გავრცელებული მიზეზი. ამიტომ აუცილებელია დაწესებულების ყველა დონეზე და ყველა სფეროში მოხდეს ზრუნვა შეუფერხებელი ინფორმაციული ნაკადების უსაფრთხოების ინციდენტების და ღონისძიებების შესახებ. ამას მიეკუთვნება შემდეგი პუნქტები:

- ანგარიშები (რეპორტები) ხელმძღვანელობის დონეზე

ზედა დონის მენეჯმენტი სისტემატურად უნდა იძლეოდეს ინფორმაციას პრობლემების, გადამოწმების შედეგებზე და

აუდიტებზე, ასევე ახალ განვითარებებზე, ჩარჩოს შეცვლილ პირობებზე ან სრულყოფის შესაძლებლობებზე, რათა შეასრულოს თავისი მართვის ფუნქცია.

- საინფორმაციო ნაკადები

ცუდი კომუნიკაციისა და ინფორმაციის არარსებობის გამო შესაძლებელია უსაფრთხოების პრობლემების აღმოცენება, ასევე მცდარი გადაწყვეტილებების მიღება ან ზედმეტი სამუშაო ბიჯების შესრულება. ეს უნდა აღმოიფხვრას შესაბამისი ზომებით და ორგანიზაციული წესებით. თანამშრომლები ინფორმირებული უნდა იყვნენ უსაფრთხოების ზომების არსსა და მიზანზე, განსაკუთრებით, როცა ეს იწვევს დამატებით სამუშაოებს ან მოჰყვება მას კომფორტის დაკარგვა. ამას გარდა თანამშრომლები ინფორმირებულნი უნდა იყვნენ თავიანთ საქმიანობასთან დაკავშირებულ ინფორმაციული უზრუნველყოფის სამართლებრივ საკითხებზე, ასევე მონაცემთა დაცვაზე. მომხმარებლები ასევე ჩართული უნდა იყვნენ ღონისძიებათა რეალიზაციის გეგმაში, რათა ითანამშრომლონ საკუთარი იდეების ფორმირებასა და მათი პრაქტიკულობის შემოწმებაში.

- დოკუმენტაცია

მთლიანი უსაფრთხოების პროცესის უწყვეტობისა და მიმდევრობითობის უზრუნველსაყოფად აუცილებელია მისი დოკუმენტირება. მხოლოდ ასე იქნება გასაგები სხვადასხვა პროცესის ბიჯები და გადაწყვეტილებები. ამის გარდა, გარანტირებულია ადეკვატური დოკუმენტაცია, რომ მსგავსი სამუშაოები სრულდება ერთნაირად, ანუ პროცესები გაზომვადი და განმეორებადია. დამატებითი დოკუმენტაცია არსებობს იმისთვის, რომ პროცესების ძირითადი ნაკლოვანებები გამოვლინდეს და შეცდომების გამეორება შემცირდეს.

აუცილებელი დოკუმენტაცია ასრულებს უსაფრთხოების სხვადასხვა ქმედებებიდან განსხვავებულ ფუნქციებს და მიმართულია განსხვავებულ მიზნობრივ ჯგუფებზე. უნდა განვასხვავოთ შემდეგი დოკუმენტაციის სახეები:

დ1. ტექნიკური დოკუმენტაცია და სამუშაო პროცესები
(მიზნობრივი ჯგუფი: ექსპერტები)

შესაძლებელი უნდა იყოს დარღვევების და უსაფრთხოების ინციდენტების დროს სასურველი მიზნობრივი მდგომარეობის აღდგენა ბიზნესპროცესებში და მასთან დაკავშირებულ IT-თან. ტექნიკური დეტალები და სამუშაო პროცესები (workflow) უნდა იყოს ისე დოკუმენტირებული, როგორც ეს გონივრულ დროშია შესაძლებელი.

მაგალითები მოიცავს ინსტრუქციებს IT–აპლიკაციების ინსტალაციისთვის, მონაცემთა უსაფრთხოებისთვის, მონაცემთა სარეზერვო ასლის აღდგენისთვის (backup), ატს–დანადგარის კონფიგურაციისთვის, რათა გადაიტვირთოს აპლიკაციის სერვერი დენის შეწყვეტის გამო, ასევე დოკუმენტაცია ტესტირების და გამოშვების (რელიზის) პროცედურისთვის, და ინსტრუქციები მოქმედებისათვის დარღვევების და უსაფრთხოების ინციდენტების შემთხვევაში.

დ2. ინსტრუქციები IT-მომხმარებლისთვის
(მიზნობრივი ჯგუფი: IT-მომხმარებლები)

სამუშაო პროცესები, ორგანიზაციული მოთხოვნები და უსაფრთხოების ტექნიკური ზომები ისე უნდა იყოს დოკუმენტირებული, რომ უსაფრთხოების ინციდენტები უცოდინარობის ან ადამიანების შეცდომების გამო შეძლებისდაგვარად გამოირიცხოს. მაგალითად, უსაფრთხოების

პოლიტიკა email-ების და ინტერნეტის გამოსაყენებლად, ინსტრუქციები ვირუსული ინციდენტების პროფილაქტიკის შესახებ ან სოციალური ინჟინერიის აღმოსაჩენად (საინფორმაციო რესურსებზე არასანქცირებული წვდომის მეთოდი, დაფუძნებული ადამიანის ფსიქოლოგიის თვისებებზე [37]), ასევე ქცევის წესები მომხმარებლისთვის, როცა უსაფრთხოების ინციდენტი მოიაზრება.

დ3. რეპორტები მენეჯმენტის ამოცანებზე
(მიზნობრივი ჯგუფი: ხელმძღვანელობის დონე,
უსაფრთხოების მენეჯმენტი)

ყველა ინფორმაცია, რომელსაც მენეჯმენტი იყენებს, რათა თავისი ორგანიზაციული და მართვის ამოცანები დააკმაყოფილოს, აუცილებელია მოთხოვნილი დეტალიზაციის ხარისხით დაფიქსირდეს (მაგალითად, აუდიტის შედეგები, ეფექტურობის შეფასებები, რეპორტები უსაფრთხოების ინციდენტებზე).

დ4. მენეჯმენტის გადაწყვეტილებათა ჩაწერა
(მიზნობრივი ჯგუფი: ხელმძღვანელობის დონე)

ხელმძღვანელობის დონემ უსაფრთხოების არჩეული სტრატეგია უნდა დააფიქსიროს და გაამართლოს. ამას გარდა, ასევე უნდა დაფიქსირდეს ყველა სხვა დონეების გადაწყვეტილებები, რომლებიც უსაფრთხოების საკითხებს ეხება. ასე, რომ ისინი ყო.ველთვის ხილვადი და განმეორებადია.

მომდევნო თავებში ყველა ქმედება, რომელიც მოითხოვს დოკუმენტურად დაფიქსირებას, აღნიშნულია "[DOK]" –ით.

- ფორმალური მოთხოვნები დოკუმენტაციისადმი:

დოკუმენტაცია არაა სავალდებულო ინახებოდეს ქაღალდის ფორმით. დოკუმენტაციის მატარებელი უნდა შეირჩეს მოთხოვნილების მიხედვით. მაგალითად, საგანგებო სიტუაციების

მენეჯმენტისთვის სასარგებლო იქნება კრიზისულ შემთხვევებში მობილურად გამოსაყენებელი პროგრამული პაკეტის დანერგვა, რომელიც გულისხმობს საგანგებო სიტუაციის ყველა ღონისძიებას და პასუხისმგებელ პირს.

საჭიროა, რომ ეს ინსტრუმენტი ფლობდეს ყველა აუცილებელ ინფორმაციას და IT-სისტემებს, მაგალითად ლეპტოპზე. კრიზისული შემთხვევისგან დაცვის მიზნით შეიძლება აზრი ჰქონდეს ყველა ინფორმაციის ერთ პრაქტიკულ სახელმძღვანელოში მოთავსებას ქაღალდის ფორმით.

საკანონმდებლო და სახელშეკრულებო მოთხოვნები შეიძლება წარმოდგენილი იყოს დოკუმენტაციით, რომლის დაცვა აუცილებელია, მაგალითად, შენახვის ვადებით და დეტალიზაციის სიღრმით. დოკუმენტაცია მხოლოდ მაშინ ასრულებს თავის მიზანს, როცა ის სისტემატურად იქმნება და მუდმივად განახლებადია. ამავდროულად, ისინი ისე უნდა იყოს აღნიშნული და შენახული, რომ აუცილებლობის შემთხვევაში სწრაფად ხელმისაწვდომი იყოს.

გარკვეული უნდა იყოს დოკუმენტაცია ან მისი ნაწილი, ვინ შექმნა და როდის. მითითებული და აღწერილი უნდა იყოს გამოყენებული წყაროები. დამატებითი დოკუმენტები, საჭიროების შემთხვევაში, უნდა იყოს ასევე ადვილად ხელმისაწვდომი.

უსაფრთხოების დოკუმენტაცია შეიძლება შეიცავდეს კონფიდენციალურ ინფორმაციას და უნდა იყოს სათანადოდ დაცული. დაცვის მოთხოვნასთან ერთად უნდა დადგინდეს შენახვის ხერხი, ხანგრძლივობა და ოფციები ინფორმაციის განადგურებისთვის. პროცესების აღწერაში უნდა ჩაიწეროს, დოკუმენტაცია უნდა იყოს თუ არა შეფასებული და როგორ.

- ხელმისაწვდომი წყაროების და გამოცდილების გამოყენება

ინფორმაციული უსაფრთხოება კომპლექსური თემაა, ამიტომ მასზე პასუხისმგებელმა პირებმა იგი დიდი სიფრთხილით უნდა დაამუშაონ. არსებობს მრავალი ხელმისაწვდომი საინფორმაციო წყარო, რომელთა გამოყენება ამისთვის შესაძლებელია. ამისთვისაა დანიშნული არსებული ნორმები და სტანდარტები, ინტერნეტ გამოცემები და სხვა პუბლოიკაციები.

ამას გარდა, გამოყენებულ უნდა იქნას თანამშრომლობა ასოციაციებთან, პარტნიორებთან, ორგანოებთან, სხვა დაწესებულებებსა და კომპანიებთან, ასევე შეიძლება CERT ჯგუფების გამოყენება ინფორმაციული უსაფრთხოების აქციების გამოცდილების გაზიარების თვალსაზრისით. ეს თემა ძალზე ფართოა და ამიტომ ნებისმიერი დაწესებულებისთვის ჩარჩოს მოთხოვნების შესაბამისი ინფორმაციული წყაროების, პარტნიორების იდენტიფიცირება და დოკუმენტირება ძალზე მნიშვნელოვანია.

5. რესურსები ინფორმაციული უსაფრთხოებისთვის

უსაფრთხოების განსაზღვრული დონის მხარდაჭერა ყოველთვის მოითხოვს ფინანსურ, ადამიანურ და დროით რესურსებს, რომლებიც ხელმძღვანელობის მიერ უნდა იყოს საკმარისად უზრუნველყოფილი. თუ მიზნები ვერ მიიღწევა არასაკმარისი რესურსების გამო, აქ პასუხს აგებენ არა პროექტში დაკავებული თანამშრომლები, არამედ ხელმძღვანელები, რომლებმაც არარეალური მიზნები დასახეს, ან აუცილებელი რესურსით ვერ უზრუნველყვეს პროცესი.

იმისთვის, რომ დასმული მიზნების მიღწევის შანსი არ დაიკარგოს, მნიშვნელოვანია მიზნების ფორმირებისას განხორციელდეს ხარჯების და სარგებლის საწყისი შეფასება. უსაფრთხოების პროცესის მსვლელობისას ეს ასპექტი კვლავ უნდა ასრულებდეს გადამწყვეტ როლს, ერთი მხრივ, რომ არ მოხდეს რესურსების ხარჯვა და, მეორე მხრივ, საჭირო ინვესტიციებით უზრუნველყოფილ იქნას უსაფრთხოების შესაბამისი დონის მიღწევა.

ხშირად IT-უსაფრთხოებასთან ასოცირდება განსაკუთრებული ტექნიკური გადაწყვეტები. ესაა კიდევ ერთი მიზეზი, რომ IT–უსაფრთხოების ნაცვლად ტერმინი ინფორმაციული უსაფრთხოება უკეთ იქნეს გამოყენებული.

უპირველეს ყოვლისა, მნიშვნელოვანია აღინიშნოს, რომ ინვესტიციები ადამიანურ რესურსებში ხშირად უფრო ეფექტურია, ვიდრე ინვესტიციები უსაფრთხოების ტექნიკაში. ტექნიკა დამოუკიდებლად ვერ წყვეტს პრობლემებს, ის ყოველთვის უნდა იყოს მიბმული ორგანიზაციულ გარემოზე. აგრეთვე უსაფრთხოების ზომების ეფექტურობის და ვარგისიანობის

გადამოწმება უზრუნველყოფილი უნდა იქნას აუცილებელი რესურსებით.

პრაქტიკაში ხშირად უსაფრთხოების შინაგან ექსპერტებს არ ჰყოფნით დრო, რათა გააანალიზონ უსაფრთხოებასთან დაკავშირებული ყველა ფაქტორი და მდგომარეობა (მაგალითად, იურიდიული მოთხოვნები ან ტექნიკური საკითხები). ზოგიერთ შემთხვევაში მათ არ გააჩნიათ შესაბამისი ბაზაც. ამიტომ უფრო მისაღებია გარე ექსპერტების გამოყენება მაშინ, როცა საკითხების და პრობლემების გადაწყვეტა ვერ ხერხდება საკუთარი საშუალებებით. ეს უნდა იყოს დოკუმენტურად დამოწმებული შიგა ექსპერტების მიერ, რათა ხელმძღვანელობის დონემ უ[illegible]უნველყოს აუცილებელი რესურსები.

წინაპირობა IT-ის უსაფრთხო მუშაობისათვის კარგად ფუნქციონირებადი IT-ექსპლუატაციაა. ამისათვის კი საკმარისი რესურსია აუცილებელი. IT-ექსპლუატაციის ტიპური პრობლემები (მცირე რესურსები, გადატვირთული ადმინისტრატორები ან არასტრუქტურირებული და ცუდ მდგომარეობაში მყოფი IT-გარემო), როგორც წესი, უნდა გადაიჭრას, რითაც უსაფრთხოების ზომების განხორციელება ეფექტურად და შედეგიანად იქნება შესაძლებელი.

6. თანამშრომელთა ჩართვა უსაფრთხოების პროცესში

ინფორმაციული უსაფრთხოება ორგანიზაციაში თითოეული თანამშრომლის საპასუხისმგებლო საქმეა. ამიტომ აუცილებელი პირობაა თანამშრომელთა და ხელმძღვანელთა ინფორმირება ინფორმაციული უსაფრთხოების საკითხებზე, აგრეთვე შესაბამისი სასწავლო პროცესის ორგანიზება და ხელშეწყობა ამ სფეროში.

უსაფრთხოების ღონისძიებათა რეალიზაციის მიზნით, როგორც ეს გათვალისწინებულია წინასწარ, საჭიროა თანამშრომლებში აუცილებელი ცოდნის საფუძვლების არსებობა, ასევე გარკვეული უსაფრთხოების მექანიზმების მიწოდება, მათი მიზნების, გამოყენების და მომსახურების ცოდნისთვის. აგრეთვე სამუშაო გარემო, საერთო ღირებულებები და თანამშრომელთა ერთგულება კრიტიკულად ახდენს ზეგავლენას საინფორმაციო უსაფრთხოებაზე.

თანამშრომელთა დათხოვნა სამსახურიდან ან გადაყვანა სხვა თანამდებობაზე, მოითხოვს ადეკვატური უსაფრთხოების ზომების გატარებას. მაგალითად, სამსახურეობრივი მოწმობის, გასაღებების, შეღავათების ჩამორთმევა და ა.შ.

თანამშრომელი ვალდებულია დაიცვას ყველა შესაბამისი კანონი, წესი და დებულება. ამისათვის კი იგი ინფორმირებული უნდა იყოს ინფორმაციული უზრუნველყოფის არსებული წესების შესახებ და უნდა იყოს მოტივირებული მათ დასაცავად.

ამავდროულად თითოეული თანამშრომელი ვალდებულია უსაფრთხოების სავარაუდო ინციდენტების შესახებ, რომლებიც მისთვის გახდება ცნობილი ან სავარაუდო, აცნობოს უსფრთხოების სამსახურს.

7. ინფორმაციული უსაფრთხოების პროცესი

ხელმძღვანელობამ უნდა დააფიქსიროს უსაფრთხოების მიზნები, შესაბამისი გარემოს პირობების და კომპანიის ბიზნეს–მიზნებზე ან დაწესებულების ამოცანებზე ბაზირებულ ცოდნაში, და შექმნას პირობები მათ დასანერგად.

უსაფრთხოების სტრატეგიით იგეგმება პროცესი, რათა შეიქმნას უსაფრთხოების უწყვეტი პროცესი. სტრატეგია ინერგება უსაფრთხოების კონცეფციის (პოლიტიკის) და ინფორმაციული უსაფრთხოების ორგანიზაციის დახმარებით.

შემდგომში სასიცოცხლო ციკლის ყოველი ფაზისთვის აღიწერება მენეჯმენტის შესაბამისი აქტიურობები (ქმედებები). საკითხის მასშტაბურობის გამო და უკეთესი ხედვის ჩამოყალიბების მიზნით უსაფრთხოების კონცეფციის აქტიურობები განხილული იქნება ცალკე თავში.

7.1. უსაფრთხოების პროცესის დაგეგმვა

7.1.1. მოქმედების დიაპაზონის დადგენა, რომელშიც ISMS უნდა იქნას გამოყენებული [DOK]

მენეჯმეტის სისტემის ინფორმაციული უსაფრთხოებისთვის აუცილებელი არ არის მისი გამოყენება მთლიანი ორგანიზაციისთვის. თავდაპირველად უნდა განისაზღვროს მოქმედების დიაპაზონი, რომლისთვისაც ISMS იქნება პასუხისმგებელი. მოქმედების დიაპაზონი ხშირად მოიცავს მთლიან დაწესებულებას, მაგრამ შეიძლება აგრეთვე. კავშირი ჰქონდეს ერთ ან რამდენიმე სპეცდავალებასთან, ბიზნეს–პროცესთან ან ორგანიზაციულ ერთეულთან. ამიტომ მნიშვნელოვანია, რომ ეს სპეცდავალებები ან ბიზნესპროცესები ამ არჩეულ დიაპაზონში მთლიანად იყოს მოთავსებული.

IT–საბაზო დაცვის ფარგლებში მოქმედების დიაპაზონისთვის გამოიყენება ტერმინი „საინფორმაციო ქსელი“ (Informationsverbund). იგი მოიცავს ასევე ყველა ინფრასტრუქტურულ, ორგანიზაციულ, ადამიანურ და ტექნიკურ კომპონენტს, რომლებიც დავალებათა შესასრულებლად ინფორმაციის დამუშავების გამოყენებით ამ სფეროს ემსახურება.

7.1.2. გარემოს პირობების განსაზღვრა

ინფორმაციული უსაფრთხოების შექმნა არაა თვითმიზანი. აქტუალური და საიმედო ინფორმაცია საფუძველია მრავალი ბიზნესპროცესისთვის. საინფორმაციო–კომუნიკაციურმა ტექნოლოგიებმა სრულად უნდა დაუჭიროს მხარი ორგანიზაციის მიზნებს და ემსახუროს ბიზნესპროცესების მხარდაჭერას.

ინფორმაციული უსაფრთხოების სტრატეგიის დამუშავების დროს მინიმუმ გასათვალისწინებელია შემდეგი თემები:

- კომპანიის მიზნები ან დაწესებულების ამოცანები;
- იურიდიული მოთხოვნები და დებულებები, მაგალითად, მონაცემთა დაცვის შესახებ;
- დამკვეთის მოთხოვნები და მოქმედი შეთანხმებები;
- გარემოს შიგა პირობები (მაგალითად, რისკების მენეჯმენტი ორგანიზაციის მასშტაბით ან IT–ინფრასტრუქტურა);
- ბიზნესპროცესები (IT–ით მხარდაჭერილი) და სპეც-დავალებები (ტექნიკური დავალებები);
- გლობალური საფრთხეები ორგანიზაციის მოღვაწეობისთვის უსაფრთხოების რისკების გამო (მაგალითად, რეპუტაციის შელახვა, კანონების და სახელშეკრულებო ვალდებულებათა დარღვევა, კვლევების შედეგების მოპარვა).

7.1.3. უსაფრთხოების მიზნების ფორმულირება და გზამკვლევი ინფორმაციული უსაფრთხოებისთვის [DOK]

საჭიროა უსაფრთხოების მიზნების დადგენა და სტრატეგიული სპეციფიკაციების (ტექნიკური პირობების) ჩამოყალიბება, თუ როგორ უნდა იქნას მიზნები მიღწეული.

ძირითადი იდეები დოკუმენტირებულია ერთ გზამკვლევში (სახელმძღვანელოში) ინფორმაციული უსაფრთხოების შესახებ (ინგლისურად: information security policy ან IT security policy). უსაფრთხოების სახელმძღვანელო უნდა მოიცავდეს მინიმუმ შემდეგ თემებს:

- დაწესებულების ან კომპანიის უსაფრთხოების მიზნები;
- უსაფრთხოების მიზნების დამოკიდებულება ბიზნესის მიზნებთან ან დაწესებულების ამოცანებთან;
- უსაფრთხოების სასურველი დონე;
- ძირითადი მოსაზრებანი, თუ როგორ უნდა იქნას სასურველი მიზნები მიღწეული;
- საკვანძო მოსაზრება, თუ რა საშუალებით ხდება და უნდა მოხდეს უსაფრთხოების დონის განსაზღვრა.

სახელმძღვანელო მიიღება მენეჯმენტის მიერ და შედეგები ეცნობება ორგანიზაციას.

7.1.4. ინფორმაციული უსაფრთხოების ორგანიზაციის აგება [DOK]

ინფორმაციული უსაფრთხოების ორგანიზაციის დაგეგმვას მიეკუთვნება ორგანიზაციული სტრუქტურების დადგენა (მაგალითად, განყოფილებები, ჯგუფები, კომპეტენციური ცენტრები) და როლებისა და ამოცანების განსაზღვრა. ინფორმაციულ უსაფრთხოებაზე პასუხისმგებელი ერთი მენეჯერი

უნდა დასახელდეს ხელმძღვანელობის უმაღლესი დონიდან, მაგალითად, ორგანიზაციის მართვის საბჭოს წევრი. გარდა ამისა, უნდა დასახელდეს მინიმუმ ერთი IT–უსაფრთხოების თანამშრომელი, რომელსაც შეეძლება სისტემატურად და დამოუკიდებლად მიაწოდოს ხელმძღვანელობის ზედა დონეს საჭირო ინფორმაცია.

7.2. სახელმძღვანელო პოლიტიკის დანერგვა ინფორმაციული უსაფრთხოებისთვის

იმისათვის, რომ მიღწეულ იყოს დასმული მიზნები, საჭიროა უსაფრთხოების კონცეფციის (პოლიტიკის) შექმნა. ამ საკითხის უკეთესად გასაგებად ცალკე თავში განიხილება, თუ როგორ იგეგმება და ინერგება უსაფრთხოების პოლიტიკა, როგორ ხდება ინფორმაციული უსაფრთხოების დონის მხარდაჭერა და სრულყოფა.

უსაფრთხოების ღონისძიებათა გადამოწმების შედეგები შემდგომ გადაეცემა უსაფრთხოების კონტროლის წარმატებების მონიტორინგს და ხდება მათი მართვის ცალკეულ დონეებზე შეფასება.

7.3. შედეგების მონიტორინგი უსაფრთხოების პროცესში

ხელმძღვანელობის დონის მიერ სისტემატურად უნდა ტარდებოდეს მენეჯმენტის შეფასება, უსაფრთხოების პროცესის მსვლელობის კონტროლი და შეფასება.

აუცილებლობის შემთხვევაში (მაგალითად, უსაფრთხოების ინციდენტების დაგროვების ან გარემოს პირობების მნიშვნელოვანი ცვლილებებისას) შესაძლებელია მათი დაგეგმილ ვადებს შორისაც ჩატარება.

ყველა შედეგი და გადაწყვეტილება ზუსტად უნდა დოკუმენტირდებოდეს [DOK].

დისკუსიისთვის სხვებთან ერთად უნდა განიხილებოდეს შემდეგი საკითხები:

- შეიცვალა გარემოს პირობები, რომელთა გამო პროცესები ინფორმაციული უზრუნველყოფის თვალსაზრისით უნდა შეიცვალოს ?
- უსაფრთხოების მიზნები არის კვლავ შესაბამისი ?
- არის ინფორმაციული უსაფრთხოების სახელმძღვანელო პრინციპები კვლავ აქტუალური ?

უსაფრთხოების პროცესის შედეგების კონტროლის პრობლემა მდგომარეობს არა ცალკეული უსაფრთხოების ზომების მონიტორინგში ან ორგანიზაციულ მმართველობაში, არამედ მათ მთლიან განხილვაში. მაგალითად, ინტერნეტპორტალის უსაფრთხო ექსპლუატაცია მცირე ბიზნესისთვის შეიძლება ძალზე ძვირი აღმოჩნდეს. ხელმძღვანელობის დონემ ასეთ დროს შეიძლება ალტერნატივის სახით დაიქირავოს სერვისის სამსახური პორტალის მოსავლელად.

აქ იქნებოდა სასარგებლო იმის განხილვა, თუ უსაფრთხოების კონცეფციამ (პოლიტიკამ) და ინფორმაციული უსაფრთხოების ორგანიზაციამ აქამდე როგორ დაიმკვიდრეს თავი. უსაფრთხოების კონცეფციის თავში აღწერილი იქნება განსხვავებული ქმედებები უსაფრთხოების ცალკეული ზომების შედეგების კონტროლისათვის. აქ მოგროვილი შედეგები გათვალისწინებულ უნდა იქნას უსაფრთხოების სტრატეგიის შედეგების კონტროლის დროს. თუ, მაგალითად, დადგინდა, რომ უსაფრთხოების ზომები არაეფექტური ან ძალზე ძვირია, ეს შეიძლება იყოს ანალიზი, რომ მთლიანი უსაფრთხოების სტრატეგია იყოს თავიდან გააზრებული და ადაპტირებული.

განხილული უნდა იქნას შემდეგი საკითხები:

- არის უსაფრთხოების სტრატეგია კვლავ შესაბამისი ?
- უსაფრთხოების კონცეფცია ადაპტირებულია, რომ მიაღწიოს დასახულ მიზნებს ? არის, მაგალითად, საკანონმდებლო მოთხოვნები შესრულებული ?
- ინფორმაციული უსაფრთხოების ორგანიზაცია მისაღებია დასახული მიზნების მისაღწევად ? საჭიროა მათი პოზიციების გამაგრება დაწესებულებაში ან ისინი უფრი ძლიერ იქნებიან შიგა პროცესებში ჩართული ?
- დანახარჯები – ღირებულება, პერსონალი, მასალები, რომლებიც საჭიროა უსაფრთხოების მიზნების მისაღწევად, არის გონივრულ შესაბამისობაში სარგებლის თვალსაზრისით დაწესებულებისთვის ?

საქმიანობის კონტროლის შედეგები თანამიმდევრულად უნდა იქნას გამოყენებული შესაბამისი კორექტურისათვის. ეს შეიძლება ნიშნავდეს, რომ უსაფრთხოების მიზნები, სტრატეგია ან კონცეფცია (პოლიტიკა) უნდა იყოს შეცვლილი და ინფორმაციული უსაფრთხოების ორგანიზაცია იყოს ადაპტირებული მოთხოვნებისადმი.

ზოგიერთ განსაკუთრებულ შემთხვევაში სასარგებლოა ძირეული ცვლილებების ჩატარება ბიზნესპროცესებში ან IT-გარემოში, ან ბიზნესპროცესებზე უარი ითქვას ან აუთსორსინგზე გადაეცეს, როცა, მაგალითად, საიმედო ექსპლუატაცია არსებული რესურსებით ვერ უზრუნველიყოფა.

თუ დიდი ცვლილებები ჩატარდა და მრავალი სრულყოფა დაინერგა, მენეჯმენტის მართვის ციკლი იხურება დაგეგმვის ფაზის ახალი დასაწყისით.

8. უსაფრთხოების კონცეფცია (პოლიტიკა)

8.1. უსაფრთხოების კონცეფციის შექმნა

ინფორმაციული უსაფრთხოების მიზნების დასაკმაყოფილებლად და უსაფრთხოების სასურველი დონის მისაღწევად თავდაპირველად საჭიროა იმის გაგება, თუ როგორაა ამოცანების და ბიზნესპროცესების შესრულება დამოკიდებული ინფორმაციის კონფიდენციალურობაზე, მთლიანობასა და ხელმისაწვდომობაზე.

ამასთანავე განხილულ უნდა იქნას, თუ დაზიანების რომელი მიზეზით რა სიდიდის ძალადობა, ორგანიზაციული ნაკლოვანება, ადამიანური უმოქმედობა ან ასევე IT-რისკები ემუქრება ბიზნეს–პროცესებს. შემდეგ შეიძლება გადაწყდეს რისკების თავიდან აცილების გზები. კერძოდ, საჭიროა შემდეგი ქვეეტაპების განხილვა (ნახ.6).

8.1.1. რისკების შეფასების მეთოდის არჩევა [DOK]

კომპანიის საქმიანობის ან დაწესებულების ამოცანების დაზიანებები უსაფრთხოების ინციდენტების გამო უნდა იქნას გაანალიზებული და შეფასებული. რისკების შეფასების მეთოდები არის ინფორმაციული უსაფრთხოების მენეჯმენტის სისტემის შემადგენელი ნაწილი. რისკის გამოსავლენად საჭიროა საფრთხეების განსაზღვრა და მათი პოტენციური ზარალის და აღმოცენების ალბათობების შეფასება.

გამოყენებით შემთხვევებზე, ორგანიზაციულ შეზღუდვებზე, მიკუთვნების სფეროზე, ასევე უსაფრთხოების მოთხოვნილ დონეზე დამოკიდებულებით რისკების შეფასების მიზნით გამოიყენება განსხვავებული მეთოდები. ინფორმაციული უსაფრთხოების მენეჯმენტმა უნდა აირჩიოს ერთი მეთოდი, რომელიც დაწესებულების სახეობის და ზომების მიხედვით შესაფერისი იქნება.



ნახ.6. უსაფრთხოების კონცეფციის სასიცოცხლო ციკლის მიმოხილვა

მეთოდების შერჩევა გადამწყვეტად მოქმედებს შრომის დანახარჯებზე უსაფრთხოების კონცეფციის (პოლიტიკის) შესაქმნელად.

რისკების შეფასების განსხვავებული სახეები აღწერილია ISO/IEC 27005 ნორმაში. BSI-მ აქედან ნაწარმოები რამდენიმე მეთოდი დაამუშავა და პრაქტიკაში გამოსცადა. IT-საბაზო–დაცვის–პროცესებში აღწერილია ასევე რისკების შეფასების ძალზე პრაქტიკული მეთოდები, რომლებიც IT-საბაზო–დაცვის–კატალოგის დახმარებით შეიძლება იქნას დანერგილი. ეს მიდგომა ფართოვდება BSI-100–3 სტანდარტით „რისკების ანალიზი, ბაზირებული IT-საბაზო–დაცვზე “.

IT-საბაზო–დაცვის ან სხვა საუკეთესო–პრაქტიკული–საშუალებების გამოყენებას აქვს ის უპირატესობა, რომ შრომის დანახარჯები საგრძნობლად მცირდება, რადგან ავტორებმა უკვე აღწერეს კონკრეტული მეთოდები და შესაფერისი უსაფრთხოების ზომები შემოგვთავაზეს.

8.1.2. რისკების ან დაზიანებების კლასიფიკაცია [DOK]

ინფორმაციული უსაფრთხოების მენეჯმენტმა რისკების შეფასების არჩეული მეთოდისგან დამოკიდებულებით უნდა განსაზღვროს როგორ · კლასიფიცირდება და შეფასდება საფრთხეები, დაზიანებათა პოტენციალი, აღმოცენების ალბათობები და აქედან გამომდინარე – რისკები.

მაგრამ საკმაოდ ძნელი, ხარჯიანი და ამიტომ, შეცდომებითაა მოსალოდნელი საფრთხეების და აღმოცენების ალბათობების ინდივიდუალური მნიშვნელობების დადგენა. რეკომენდებულია, არ დაიხარჯოს დიდი დრო შრომატევად (და შეცდომების შემცველ) რისკების აღმოცენების ალბათობებისა და შესაძლო საფრთხეების ზუსტ განსაზღვრებაზე. ხშირ შემთხვევებში პრაქტიკულია, როგორც რისკების აღმოცენების ალბათობებთან, ასევე პოტენციურ დაზიანებათა სიდიდეებთან მუშაობა კატეგორიებით. აქ გამოყენებულია 3–5 კატეგორია, მაგალითად:

- აღმოცენების ალბათობები: *იშვიათად, ხშირად, ძალიან ხშირად;*
- პოტენციური დაზიანების დონე: *საშუალო, მაღალი, ძალიან მაღალი.*

შემდეგ დაწესებულებისთვის შესაფერისი გზით განისაზღვრება, შეიძლება თუ არა ასეთი კატეგორიების გამოყენებით რისკების ხარისხობრივი დამუშავება.

8.1.3. რისკების შეფასება [DOK]

რისკების ყოველი შეფასება მოიცავს შემდეგ ბიჯებს:

- დასაცავი ინფორმაცია და ბიზნესპროცესები უნდა იყოს იდენტიფიცირებული;
- დასაცავი ინფორმაციის და ბიზნესპროცესების შესაბამისი ყველა საფრთხე უნდა იყოს იდენტიფიცირებული;
- სუსტი ადგილები, რომლებშიც შეუძლია ზემოქმედება საფრთხეებს, უნდა იყოს იდენტიფიცირებული;
- შესაძლო დაზიანებები, გამოწვეული კონფიდენციალობის, მთლიანობისა და წვდომის დაკარგვის გამო, უნდა იყოს იდენტიფიცირებული;
- სავარაუდო ზეგავლენები ბიზნესზე ან შესასრულებელ ამოცანებზე, გამოწვეული უსაფრთხოების ინციდენტებით, უნდა იქნას გაანალიზებული;
- რისკი, რომელიც უსაფრთხოების ინციდენტებით იწვევს დაზიანებას, უნდა შეფასდეს.

აქ გამოყენებული ტერმინები „საფრთხე", „სუსტი ადგილი" და „რისკი" განსაზღვრულ იქნება IT–საბაზრო–დაცვის კატალოგის ლექსიკონში.

8.1.4. სტრატეგიის დამუშავება რისკების დასამუშავებლად [DOK]

ხელმძღვანელობის ზედა დონემ უნდა განსაზღვროს, თუ როგორ მოუარონ აღმოჩენილ რისკებს. ინფორმაციული უსაფრთხოების მენეჯმენტის მიერ უნდა იყოს ეს საკითხი მომზადებული. ამისთვის არსებობს შემდეგი ოფციები:

- რისკები შეიძლება შემცირდეს, უსაფრთხოების ადეკვატური ზომების გამოყენებით;
- რისკები შეიძლება შემცირდეს, მაგალითად, ბიზნეს-პროცესების ან სპეცამოცანების რესტრუქტურირებით ან ამოგდებით;
- რისკები შეიძლება გადაცემულ იქნას, მაგალითად, ოუთსორსინგით ან დაზღვევით;
- რისკები შეიძლება იყოს დასაშვები.

რისკების თავიდან აცილების სახეები უნდა იყოს დოკუმენტირებული და ხელმძღვანელობის ზედა დონის მიერ დამტკიცებული. აუცილებელი რესურსები სტრატეგიის დანერგვისთვის უნდა დაიგეგმოს და უზრუნველყოფილ იქნას.

სტრატეგიის დამუშავებისას ხარჯებისგან დამატებით, გადაწყვეტილების მნიშვნელოვან კრიტერიუმად განიხილავენ ნარჩენ რისკს, რომელიც გათვალისწინებულ უნდა იქნას ხელმძღვანელობის ზედა დონეზე. ნარჩენი რისკი უნდა შეფასდეს და დოკუმენტირებულ იქნას.

8.1.5. უსაფრთხოების ღონისძიებათა არჩევა [DOK]

უსაფრთხოების ზოგადი მიზნებიდან და მოთხოვნილებებიდან, რომლებიც მოცემულია ხელმძღვანელობის დონის მიერ, გამომდინარეობს უსაფრთხოების კონკრეტული ღონისძიებები. უსაფრთხოების ზომების არჩევის დროს განიხილება აგრეთვე უსაფრთხოების დონეზე გავლენასთან

ერთად მოგება–ზარალის ასპექტები და პრაქტიკული რეალიზებადობა.

უსაფრთხოების ტექნიკურ ზომებთან ერთად უნდა შეიქმნას ასევე ორგანიზატორული პროცედურები და პროცესები (როგორიცაა მომხმარებელთა პოლიტიკა, წვდომის უფლებები, უსაფრთხოების სწავლება, ტესტირების და გამოშვების მეთოდები). სხვა საკითხებთან ერთად განიხილება შემდეგი თემები:

- ორგანიზაციული (მათ შორის: ვალდებულებები, დავალებათა და ფუნქციების განაწილება, კონტროლი ინფორმაციის დამუშავების, აპლიკაციების და IT–კომპონენტების, აპარატურული და პროგრამული უზრუნველყოფის მენეჯმენტი, ცვლილებების მენეჯმენტი და ა.შ.);
- ადამიანური (მაგალითად, ახალი თანამშრომლების ტრეინინგი, წარმომადგენლობის სქემები, ა.შ.)
- სწავლება და ინფორმირება ინფორმაციული უსაფრთხოებისთვის;
- მონაცემთა საიმედოობა (მთელი ინფორმაციის, აპლიკაციების და IT-კომპონენტების სარეზერვო კოპირება);
- მონაცემთა დაცვა;
- კომპიუტერის ვირუსული დაცვა;
- ინფორმაციის დაცვა მისი გადამუშავების, გადაცემის და შენახვისას (მაგალითად, კრიპტოგრაფიის დანერგვით);
- აპარატურული და პროგრამული უზრუნველყოფის განვითარება;
- უსაფრთხოების ინციდენტების მოვლა (incident handling);
- საგანგებო სიტუაციებისთვის მზადყოფნა და ბიზნეს–პროცესების უწყვეტობის მხარდაჭერა ავარიულ შემთხვევებში (business continuity);
- ოუთსორსინგი.

პროცესები ზუსტად უნდა იყოს დოკუმენტირებული, თუ რატომაა არჩეული ღონისძიებები შესაფერისი უსაფრთხოების მიზნების და მოთხოვნილებების მისაღწევად.

8.2. უსაფრთხოების კონცეფციის რეალიზება

უსფრთხოების ღონისძიებათა შერჩევის შემდეგ საჭიროა ის ჩაიდეს რეალიზაციის გეგმაში. ამ დროს უნდა განხორციელდეს შემდეგი ბიჯები:

8.2.1. რეალიზაციის გეგმის შექმნა უსაფრთხოების კონცეფციისთვის [DOK]

აქ განიხილება შემდეგი თემები:

- პრიორიტეტების დადგენა (დანერგვის მიმდევრობა);
- პასუხისმგებლობის განსაზღვრა ინიციალიზაციისათვის;
- რესურსების მომზადება მენეჯმენტის მიერ;
- დანერგვის გეგმა ცალკეული ზომებისთვის [ვადების განსაზღვრა, ხარჯების, შესრულებაზე პასუხისმგებლობასა და კონტროლზე (დანერგვის ეფექტურობაზე) პასუხისმგებლების დადგენა];

8.2.2. უსაფრთხოების ღონისძიებათა დანერგვა

დაგეგმილი უსაფრთხოების ზომები უნდა განხორციელდეს რეალიზაციის გეგმის შესაბამისად. ინფორმაციული უსაფრთხოება ინტეგრირებულ უნდა იქნას პროცედურებსა და ბიზნეს-პროცესებში ორგანიზაციის მთელი მასშტაბით.

თუ დანერგვისას თავს იჩენს სირთულეები, ისინი სასწრაფოდ უნდა განიხილოს და მოინახოს აღმოფხვრის გზები. ტიპური გადაწყვეტის გზის მაგალითად შეიძლება განვიხილოთ როგორც საკომუნიკაციო გზების ან დანიშნული უფლებების ცვლილება, ასევე ტექნოლოგიური მეთოდების (პროცედურების) ადაპტირება.

8.2.3. დანერგვის კონტროლი და მონიტორინგი [DOK]

მიზნის მაჩვენებლების მიღწევა სისტემატურად უნდა მოწმდებოდეს. თუ ამ მაჩვენებლების დაცვა ვერ ხერხდება, აუცილებელია ინფორმაციული უსაფრთხოების პასუხისმგებელი ხელმძღვანელი პირის ინფორმირება, რათა პრობლემაზე მოხდეს დროული რეაგირება.

8.3. შედეგების მონიტორინგი და უსაფრთხოების კონცეფციის სრულყოფა

უსფრთხოების დონის მხარდასაჭერად საჭიროა, ერთი მხრივ, უსაფრთხოების შესაბამისად იდენტიფიცირებული ღონისძიებების კორექტულად გამოყენება და, მეორე მხრივ, უსფრთხოების კონცეფციის მუდმივად აქტუალიზება. ამასთანავე, უსაფრთხოების ინციდენტები დროულად უნდა იყოს აღმოჩენილი და ასევე სასწრაფოდ და შესაბამისად უნდა მოხდეს მასზე რეაგირება. საჭიროა სისტემატურად მიმდინარეობდეს უსაფრთხოების კონცეფციის შედეგების კონტროლი. დანერგილი ზომების ეფექტურობა და ქმედითობა უნდა შეფასდეს შიგა აუდიტის ჩარჩოებში. თუ არაა საკმარისი რესურსები ასეთი აუდიტის ჩასატარებლად შიგა ექსპერტების მიერ, მაშინ ხდება გარე ექსპერტების მოწვევა და კონტროლის ქმედებების ჩატარების უფლებამოსილების გადაცემა.

ვინაიდან აუდიტის ხარჯები დამოკიდებულია ინფორმაციული ქსელის სირთულესა და ზომებზე, ამიტომაც შემოწმების მოთხოვნები მცირე დაწესებულებების ან კომპანიებისთვის შესაბამისად იქნება დაბალი, ვიდრე დიდი და რთული ორგანიზაციებისთვის. IT-სისტემების წლიური ტექნიკური შემოწმება, არსებული დოკუმენტაციის მიმოხილვა, რათა შემოწმდეს აქტუალობა, და ვორკშოპი, სადაც უსაფრთხოების კონცეფციაზე პრობლემები და გამოცდილება იქნება გაზიარებული, უკვე საკმარისია გარკვეულ შემთხვევებში მცირე ორგანიზაციებისთვის.

კერძოდ, უნდა გატარდეს შემდეგი ქმედებები:

- რეაქცია ცვლილებებზე მოქმედი წარმოებისთვის

ცვლილებების დროს მოქმედ წარომებაში (მაგალითად, ახალი ბიზნესპროცესის დანერგვა, ორგანიზაციული ცვლილებები ან ახალი IT-სისტემების დანერგვა) განახლებულ უნდა იქნას როგორც უსაფრთხოების კონცეფცია, ასევე მასთან დაკავშირებული დოკუმენტაცია (როგორც აგრეთვე ვალდბულებათა ან IT-სისტემების სია).

- უსაფრთხოების ინციდენტების აღმოჩენა ექსპლუატაცის პროცესში [DOK]

ღონისძიებები უნდა იყოს რეალიზებული, რომლებიც საშუალებას იძლევა, რომ ინფორმაციის დამუშავების შეცდომები (რომელთაც შეუძლია გავლენა იქონიოს კონფიდენვიალობაზე, წვდომაზე ან მთლიანობაზე), უსაფრთხოებისთვის კრიტიკულად მნიშვნელოვანი ადამიანური შეცდომები და ინციდენტები შეძლებისდაგვარად იყოს თავიდან აცილებული, რომ მათი გავლენა შეიზღუდოს ან მინიმუმ, მოხდეს მათი ადრეულ სტადიაზე დაფიქსირება.

უსაფრთხოების პრობლემების ადრეული ამოცნობის მიზნით შეიძლება, მაგალითად, ინსტრუმენტების გამოყენება სისტემის მონიტორინგისთვის, მთლიანობის შესაფასებლად, წვდომათა პროტოკოლირებისათვის (რეგისტრირებისთვის), ქმედებების ან შეცდომებისთვის, შენობების და ოთახების შესასვლელთა კონტროლისთვის, ხანძრის, წყლის და ჰაერის სენსორებისთვის. გამოვლენის ღონისძიებათა ჩანაწერები და ოქმები სისტემატურად უნდა ფასდებოდეს.

- კონტროლი მოთხოვნილებების დაცვისთვის [DOK]

აუცილებელია სისტემატურად შემოწმდეს, იყო თუ არა უსაფრთხოების ყველა ზომა გამოყენებული და ჩატარებული ისე, როგორც ეს უსაფრთხოების კონცეფციაშია მითითებული. აქ

საჭიროა როგორც ტექნიკური უსაფრთხოების ზომების (მაგალითად, კონფიგურაციის შესახებ), ისე ორგანიზაციული ზომების (მაგალითად, პროცესები, მეთოდები და ოპერაციები) დაცვის კონტროლირება.

საჭიროა აგრეთვე შემოწმდეს, არის თუ არა განკარგულებაში ღონისძიებების კორექტულად დასანერგად აუცილებელი რესურსები, და ყველა პერსონა, რომელთა განსაზღვრული როლები უსაფრთხოების ზომების დასანერგად იყო დანიშნული, თავიანთ ვალდებულებებს თუ ასრულებს.

- უსაფრთხოების ზომების ადეკვატურობის და ეფექტურობის შემოწმება [DOK]

აუცილებელია რეგულარული შეფასება, არის თუ არა უსაფრთხოების ზომები ადეკვატური, რომლებიც უსაფრთხოების დასმულ მიზნებს მიღწევს. მათ შესამოწმებლად ადეკვატურობაზე შეიძლება, მაგალითად, წარსულის ინციდენტების შეფასება, თანამშრომელთა გამოკითხვა ან შეღწევადობის ტესტების განხორციელება. ამას მიეკუთვნება ასევე შესაბამისი მოვლენები ბიზნესპროცესების გარემოში ან კომპანიის სპეცდავალებების შესრულება.

მაგალითად, გარემოს ტექნიკური ან ნორმატიული პირობები შეიძლება შეიცვალოს. იმისათვის, რომ აქტუალური მდგომარეობა იყოს შენარჩუნებული, უსაფრთხოებაზე პასუხისმგებლები უნდა იყენებდნენ გარე ცოდნის წყაროებს, ესწრებოდნენ სპეცკონფერენციებს, ასევე ეცნობოდნენ სტანდარტულ და სპეცლიტერატურას, აგრეთვე ინტერნეტის ინფორმაციას. თუ ორგანიზაციის შიგნით ვერ ხერხდება საჭირო ცოდნის მიღება ან არაა ამის დრო, მაშინ აუცილებელი ხდება გარე ექსპერტების მოწვევა.

ამ კონტექსტში აზრი აქვს კითხვის დასმას, რომ არის თუ არა უსაფრთხოების გამოყენებული ზომები ეფექტური ან უსაფრთხოების მიზნები მიიღწევა თუ არა სხვა ღონისძიებებით რესურსების შენარჩუნებით ? ამასთანავე აუცილებელია შემოწმდეს, არის თუ არა პროცესები და ორგანიზაციული წესები პრაქტიკული და ეფექტური. ხშირად აქედან ჩნდება შესაძლებლობა აუცილებელი ორგანიზაციული ცვლილებების და რესტრუქტურიზაციის განსახორციელებლად.

- მენეჯმენტის შეფასებები

ხელმძღვანელობის დონე სისტემატურად უნდა იყოს ინფორმირებული ინფორმაციული უსაფრთხოების მენეჯმენტიდან, შეფასებათა შედეგების შესახებ შესაბამისი ფორმით. ამასთან ნაჩვენები უნდა იყოს პრობლემები, შედეგები და სრულყოფის შესაძლებლობები.

მენეჯემენტის რეპორტები უსაფრთხოების პროცესის მართვისათვის უნდა შეიცავდეს ხელმძღვანელობის დონისთვის ყველა საჭირო ინფორმაციას. ეს ინფორმაციებია, მაგალითად:

- უსაფრთხოების პროცესის არსებული მდგომარეობის მიმოხილვა;
- ხელმძღვანელობის მიერ მენეჯმენტის წინა პერიოდების ანალიზის შეფასება;
- უკუკავშირი კლიენტებთან და თანამშრომლებთან;
- მიმოხილვა ახალი საფრთხეებისა და უსაფრთხოების ხარვეზების შესახებ.

ხელმძღვანელობის დონე ღებულობს მენეჯმენტის ანგარიშებს ინფორმაციის სახით და გამოაქვს სათანადო გადაწყვეტილებანი, მაგალითად, უსაფრთხოების პროცესის სრულყოფისთვის, რესურსების მოთხოვნილებისადმი, ასევე

უსაფრთხოების ანალიზის შედეგებისათვის (მაგალითად, რისკების მინიმიზაცია, შთანთქმა ან მიღება). უსაფრთხოების პროცესის შედეგების რეგულარული კონტროლი ემსახურება იმას, რომ გამორიცხოს აღმოჩენილი შეცდომები და ხარვეზები, და მოახდინოს უსაფრთხოების ზომების ოპტიმიზაცია ეფექტურობის თვალსაზრისით.

ამ პროცესში ქმედებები არ უნდა იყოს ტექნიკური ღონისძიებებით შეზღუდული. ზოგჯერ აუცილებელია თანამშრომელთა ტრეინინგი და ინფორმირება. მნიშვნელოვანი მომენტია ასევე ტექნიკური ზომების და ორგანიზაციული პროცესების პრაქტიკულობის სრულყოფა, რათა უსაფრთხოების ზომების მიღება ამაღლდეს.

9. BSI–ის ISMS: IT–საბაზო დაცვა

9.1. შესავალი „IT-საბაზო–დაცვის" მეთოდიკაში

ინფორმაციული უსაფრთხოების მენეჯმენტის სისტემის აღწერა მოცემულია ამ დოკუმენტში და აგრეთვე ISO-Standards 27000, 27001 და 27002 სტანდარტებში, მაგრამ ძალიან ზოგადად, ისინი იძლევა გარემოს (ჩარჩოს) მხოლოდ საფუძვლებს. პრაქტიკაში ამ ზოგადი სპეციფიკაციების სარეალიზაციოდ საჭიროა მეტი საშუალება და მოქნილობა. დიდ პრობლემად ითვლება ISMS-ის დაყენება საკუთარ დაწესებულებაში, რაც არა მხოლოდ ხელს უწყობს უსაფრთხოების დასმული მიზნების მიღწევას, არამედ ითვლება საკმაოდ ეკონომიურ და ეფექტურ საშუალებად.

საკითხი, თუ როგორ შეიქმნას უსაფრთხოების კონცეფცია ორგანიზაციისთვის, ხშირად ურთულესი გადასაწყვეტია. მისი შექმნის ძირითადი სამუშაო ეტაპები ამ დროს არის რისკების შეფასება და უსაფრთხოების ღონისძიებების სწორად შერჩევა. რისკების შეფასების მეთოდების არჩევას განსაკუთრებული მნიშვნელობა აქვს, რადგან იგი გადამწყვეტ გავლენას ახდენს უსაფრთხოების კონცეფციის შექმნის სამუშაო დატვირთვაზე.

მეთოდიკა „IT-საბაზო–დაცვა" აღწერს მეთოდს, რომელიც ხშირ შემთხვევებში დანართებისთვის მისაღებად ითვლება. იგი ბევრად ეკონომიურია, ვიდრე რისკების ანალიზის კლასიკური რაოდენობრივი მეთოდები, რაც მრავალი წლის პრაქტიკულმა გამოცდილებამ აჩვენა. როგორც დამატებითი ღირებულება, IT-საბაზო–დაცვის–მეთოდებში არა მხოლოდ აღიწერება, თუ როგორ ფუნქციონირებს პრინციპში ISMS, არამედ IT-საბაზო–დაცვის–კატალოგებთან ერთად აღიწერება, თუ როგორ გამოიყურება კონკრეტული ღონისძიებების დანერგვა პრაქტიკულად.

ეს თავი იძლევა შესავალს IT-საბაზო–დაცვის–მეთოდების მნიშვნელოვან ელემენტებში და გვიჩვენებს, რომ IT-საბაზო–დაცვის მეთოდიკა სრულიად თავსებადია ISO 27001 სტანდარტთან. უფრო ვრცელი ასახვა ამ მასალის მოცემულია წიგნში BSI-Standard 100-2.

ინფორმაციული უსაფრთხოების მენეჯმენტის სისტემის დასაყენებლად და მხარდასაჭერად IT-საბაზო–დაცვის–მეთოდიკა აღწერს მიდგომას დანართებისთვის, რომელიც ბაზირებულია IT-საბაზო–დაცვის–მეთოდიკაზე და IT-საბაზო–დაცვის–კატალოგებზე. ამ წიგნში დეტალურად და უფრო პრაქტიკულადაა გადმოცემული აქ ნახსენები თემები. IT-საბაზო–დაცვის–კატალოგების ყოველი კომპონენტი ემორჩილება სასიცოცხლო–ციკლის მოდელს და მოიცავს სპეციალურ ზომებს დაგეგმვიდან დაწყებული მის წარმოებიდან მოხსნამდე.

9.2. უსაფრთხოების პროცესი IT–საბაზო დაცვის მიხედვით

ყველა გავრცელებული მეთოდი, საუკეთესო პრაქტიკული ნიმუში და სტანდარტები ინფორმაციული უსაფრთხოების მენეჯმენტისათვის ნაკლებად განხვავდება ერთმანეთისგან შესრულების ვერსიებში, რომლებიც გამოიყენება უსაფრთხოების პროცესებთან ან ხელმძღვანელობის მენეჯმენტის ამოცანებისთვის. დიდი განსხვავება მდგომარეობს იმ ტიპსა და მეთოდი, რომლითაც კონკრეტული უსაფრთხოების კონცეფცია შეიქმნა, ანუ რისკების შფასების კოფიგურირების და უსაფრთხოების ზომების არჩევის დროს. ამ მიზეზით აქ ასახულია უსაფრთხოების კონცეფციის შექმნის ძირითადი პროცედურა IT-საბაზო–დაცვის მიხედვით.

9.2.1. რისკების შეფასება ინფორმაციულ უსაფრთხოებაში

რისკების შეფასება ინფორმაციულ უსაფრთხოებაში მნიშვნელოვნად განსხვავდება სადაზღვევო მათემატიკის ან მართვის თეორიის კლასიკური მეთოდებისგან. დაზიანების (ზარალის) დონის და ხდომილობათა ალბათობების ზუსტი ანგარიში „კლასიკური“ ან რაოდენობრივი რისკების ანალიზით ხშირად შეუძლებელია, რადგან შესაბამისი რიცხვითი მასალა არ არსებობს. მაშინაც კი, როცა გაანგარიშება შესაძლებელია, შედეგების ინტერპრეტაცია საკმაოდ რთულია.

<u>მაგალითი:</u> კლასიკური რისკების ანალიზში რისკი გაითვლება ზარალის დონის გამრავლებით ხდომილობის ალბათობაზე. ამგვარად, თუ გამოთვლითი ცენტრის განადგურება თვითმფრინავის შეტაკებით 20 მლნ ევრო ღირს და სტატისტიკურად ეს შემთხვევა 20.000 წელიწადში ერთხელ ხდება, მაშინ თეორიული რისკი წელიწადში არის 1000 ევრო.

ასეთივე რისკი არსებობს, თუ ზარალი ერთი ლეპტოპის ქურდობისთვის (მონაცემთა დაკარგვის გარეშე) შეესაბამება 2000 ევროს. ასეთი შემთხვევა ორ წელიწადში ერთხელ ხდება.

მართალია, ამ ორი შემთხვევის რისკები მათემატიკურად ემთხვევა ერთმანეთს ღირებულებით, მაგრამ ეს ზარალის სცენარები რისკების მენეჯმენტის ფარგლებში სრულიად განსხვავებულად უნდა დამუშავდეს.

ბევრი სცენარისთვის არაა საკმარისი გამოცდილება, რათა ხდომილებათა ალბათობები დასაბუთებულად განისაზღვროს, იმიტომ, რომ ახალი ტექნოლოგიები დაინერგა ან მწირია დასაბუთებული საბაზო მონაცემები. თუნდაც საკმარისი მონაცემების არსებობისას, რათა ხდომილებათა ალბათობების და ზოგიერთი მოვლენის ზარალის დონეების განსაზღვრა რამდენადმე სრულყოფილად შეიძლებოდეს, არის კლასიკური

რისკების ანალიზზე ბაზირებული უსაფრთხოების კონცეფციის შექმნის ძალზე რთული და ძვირი გზა.

სუსტი ადგილების ინდივიდუალური ანალიზი უსაფრთხოების ყველა მნიშვნელოვანი პროცესისთვის მათთან დაკავშირებულ IT-კომპონენტებთან და შესაძლო ზარალის მოვლენების შეგროვება ხდომილობათა ალბათობების და ზარალის ზომების პარამეტრების მოწესრიგებით, მოითხოვს ფრმა სპეციალიზებულ ცოდნას და დიდი მოცულობის მონაცემთა სიმრავლეების დამუშავებას.

ამიტომაც IT-საბაზო–დაცვის მეთოდიკაში უკვე ჩართულია რისკების შეფასების ხარისხობრივი მეთოდი, რომელიც იძლევა აუცილებელ ინფორმაციას ბიზნესის დამაზიანებელ უსაფრთხოების ინციდენტების შესაფასებლად. IT-საბაზო–დაცვის მეთოდიკის გამოყენებისას ვარაუდობენ, რომ მიუხედავად ორგანიზაციის ტიპის და მიმართულებისა, ყველგან ბიზნესის შესატყვისი ინფორმაცია საიმედოდ უნდა მუშავდებოდეს, ინტეგრირებული და მასთან დაკავშირებული IT–სისტემები ინერგებოდეს და შესაბამისი გარემო პირობები არსებობდეს.

ამიტომ ხშირად არსებობს მსგავსი საფრთხეები. ბიზნეს-პროცესების და სპეცაპლიკაციების უსაფრთხოების პირობები არის ინდივიდუალური და შეიძლება განსხვავდებოდეს, პრაქტიკაში ისინი იწვევს უმეტესად უსაფრთხოების მსგავსს და თავსებად მოთხოვნებს.

BSI აანალიზებს IT-საბაზო–დაცვის მეთოდიკისთვის IT-საბაზო–დაცვის–კატალოგებში სუსტ ადგილებს და საფრთხეებს, ტიპური გამოყენების სფეროების (ველების) და კომპონენტებისთვის და აქედან განსაზღვრავს საშედეგო საფრთხეებს. განიხილება მხოლოდ ისეთი საფრთხეები, რომლებსაც ყურადღებიანი ანალიზის შედეგად აქვს

ხდომილებათა მაღალი ალბათობები ან ისეთი გადამწყვეტი ზეგავლენები გააჩნია, რომ უსაფრთხოების ზომები უნდა იყოს აუცილებლად მიღებული.

ტიპური საფრთხეები, რომელთა წინააღმდეგ თითოეულმა უნდა დაიცვას თავი, არის, მაგალითად, ზარალი ხანძრისგან, ქურდობა, კომპიუტერული ვირუსები ან აპარატურის დეფექტები. ამ მიდგომას აქვს ის უპირატესობა, რომ IT-საბაზო–დაცვის მომხმარებელი ინფორმაციული ქსელის დიდი ნაწილისთვის საფრთხეების და სუსტი ადგილების ანალიზს არ ატარებს ან ხდომილებათა ალბათობებს არ ანგარიშობს, რადგან ასეთი სამუშაოები ამოღებულია სამთავრებო ორგანოების მიერ.

გამოვლენილი საფრთხეების საფუძველზე IT-საბაზო–დაცვის–კატალოგები აღწერს დამტკიცებულ ტექნიკურ, ინფრასტრუქტურულ, საკადრო და ორგანიზაციულ სტანდარტულ–უსაფრთხოებათა ღონისძიებებს ტიპური ობიექტებისთვის.

ინფორმაციისა და ბიზნესპროცესებისთვის დაცვის მაღალი ან ძალიან მაღალი მოთხოვნილებებით ან სამუშაო გარემოსთვის, რომელიც IT-საბაზო–დაცვაში არ განიხილება, უნდა ჩატარდეს უსაფრთხოების დამატებითი ანალიზი და აუცილებლობის შემთხვევაში – რისკების ანალიზი. რისკების გამარტივებული ანალიზი აღწერილია IT-საბაზო–დაცვის–მეთოდიკაში [31].

როგორც რისკების შეფასება IT-საბაზო–დაცვის–მიხედვით, ასევე [31]-ში აღწერილი რისკების ანალიზი ბევრად მარტივი და იაფია, ვიდრე რისკების რაოდენობრივი ანალიზი. რისკების შეფასება IT-საბაზო–დაცვის–მიხედვით იძლევა იმ უპირატესობას, რომ დაწესებულებებს სხვადასხვა სფეროდან შეუძლია წარმოადგინოს ზოგადი და გასაგებად განსაზღვრული საფუძველი თავიანთი რისკების შესაფასებლად.

9.2.2. რისკების კლასიფიკაცია

რისკების კლასიფიკაციის ზოგადი მოთხოვნები IT-საბაზო–დაცვაში შემდეგი ბიჯებით მიმდინარეობს:

1. ორიენტაცია დაზიანების (ზარალის) სცენარით

უსაფრთხოების ინციდენტებით გამოწვეული დაზიანებები (ზარალი) და უარყოფითი ზემოქმედებები რომ შეძლებისდაგვარად ნათლად აღიწეროს, საჭიროა სხვადასხვა საფრთხეთა სცენარების განხილვა, მაგალითად:

- კანონების, დებულებების და ხელშეკრულებების დარღვევა;
- ინფორმაციული თვითგამორკვევის უფლების გაუფასურება;
- პირადი ხელშეუხებლობის დარღვევა;
- მოვალეობების შესრულების დარღვევა;
- უარყოფითი შიგა და გარე ზემოქმედებები;
- ფინანსური ზემოქმედებები.

სცენარების გათამაშების დროს უნდა იქნას გამოკვლეული, თუ რომელი საფრთხეები წარმოიქმნება კონფიდენციალობის, მთლიანობის და წვდომის დაკარგვისას.

მაგალითად, სცენარისთვის „კანონების დარღვევა“ სადისკუსიოა საკითხი თუ რომელი მონაცემები უნდა იქნას განხილული კონფიდენციალურად სამართლებრივი მოთხოვნებით და რა შედეგები შეიძლება მოჰყვეს ამ მოთხოვნების გაუფრთხილებლობით დარღვევას.

2. ზარალის კლასიფიკაცია: დაცვის მოთხოვნილებათა კატეგორიების განსაზღვრა

ხშირ შემთხვევებში პოტენციური ზარალის ზუსტი ანგარიში უსარგებლოა ან შეუძლებელია და უსაფრთხოების ღონისძიებათა შერჩევისათვის არაა საჭირო. ამიტომაც რეკომენდებულია ზარალის დაყოფა მცირე კლასებად. მცდელობა ზარალის „ზუსტი“

ანგარიშისთვის ხშირ შემთხვევაში საფრთხეს უქმნის უსაფრთხოებას, რადგან არასწორი სიზუსტით იქნება ნავარაუდევი და მასზე პასუხისმგებელ პირს ექნება „ყალბი უსაფრთხოების განცდა".

შესაძლო ზარალებიდან გამომდინარე IT-საბაზო–დაცვის ფარგლებში განისაზღვრება დაცვის მოთხოვნილებათა სამი კატეგორია, რომელშიც მოგვიანებით დაცვის ობიექტები (მაგალითად, IT-სისტემები) კლასიფიცირდება:

- „ნორმალური დაცვის მოთხოვნილება": ზარალის ზემოქმედება შეზღუდულია და მართვადი;
- „მაღალი დაცვის მოთხოვნილება": ზარალის ზემოქმედება შეიძლება იყოს მნიშვნელოვანი;
- „ძალიან მაღალი მოთხოვნილება": ზარალის ზემოქმედებამ შეიძლება მიიღოს ექსისტენციალური მუქარის კატასტროფული მასშტაბები.

ყოველმა დაწესებულებამ ინდივიდუალურად უნდა განსაზღვროს, თითოეული ზარალის სცენარისთვის როგორაა ინტერპრეტირებული „ნორმალური", „მაღალი" და „ძალიან მაღალი", ჩარჩოს რომელი პირობები დაედება საფუძვლად კლასიფიკაციას დაცვის მოთხოვნილებათა კატეგორიებში.

ვინაიდან ამას უშუალო გავლენა აქვს რისკების მართვასა და რესურსების მოთხოვნილებასთან, ეს გადაწყვეტილება უნდა მიღოს ორგანიზაციის უმაღლესმა ხელმძღვანელობამ.

დაცვის მოთხოვნების კატეგორიათა განსაზღვრა დაწესებულების სახეობისა და სიდიდის მიხედვით ძალზე განსხვავებულია და მხოლოდ უმაღლეს მართვის ორგანოს შეუძლია დაადგინოს იგი უსაფრთხოების მენეჯმენტთან თანამშრომლობით. BSI-ის შეუძლია მაგალითების დასახელება, რომლებიც ადაპტირებული იქნება შესაბამის პირობებთან.

მაგალითი ფინანსური ზარალის კლასიფიკაციისათვის:

დავუშვათ, მოცემულია ნორმალური დაცვის მოთხოვნილება, რომელიც დაწესებულებისთვის არის დასაშვები. მცირე საწარმოსთვის ეს ნიშნავს, რომ უსაფრთხოების ინციდენტის გამო ზარალი არ უნდა აღემატებოდეს 10 000 ევროს. მაღალი დაცვის მოთხოვნილება ნიშნავს, რომ ზარალით მიყენებული ფინანსური დანაკარგი არაა სასიცოცხლოდ საშიში. მცირე საწარმოსთვის ესაა 10 000 დან 100 000 ევრომდე ფარგლებში.

დაცვის ძალზე მაღალი მოთხოვნილება დაწესებულებისთვის ნიშნავს, რომ ფინანსური ზარალი მისთვის სასიცოცხლოდ მნიშვნელოვანია. ესაა 100 000 ევროზე მეტი მცირე საწარმოსთვის. დიდი დაწესებულებისთვის სხვა რიცხვები გვექნება.

9.2.3. რისკის შეფასება

9.2.3.1. სტრუქტურული ანალიზი: დაცვის ობიექტების იდენტიფიკაცია [DOK]

სტუქტურული ანალიზის ფარგლებში განსახილველი ინფორმაციული ქსელისთვის განისაზღვრება მოქმედების სფერო ან ბიზნესპროცესი, შესაბამისი დაცვის ობიექტები, როგორიცაა ინფორმაციები, აპლიკაციები, IT-სისტემები, ქსელები, ფართები და შენობები, აგრეთვე კომპეტენტური თანამშრომლები.

სტრუქტურული ანალიზის დროს დამატებით წარმოდგენილ უნდა იქნას ურთიერთობები და დამოკიდებულებები ცალკეულ დაცვის ობიექტებს შორის. გამოვლენილი დამოკიდებულებები ძირითადად გამოიყენება უსაფრთხოების ინციდენტების გავლენის დასადგენად ბიზნეს-პროცესებზე, რათა შემდგომ მოხდეს სათანადო რეაგირება.

მაგალითად: თუ „S-სერვერი" მოხვდება უსაფრთხოების ინციდენტის გავლენის ქვეშ, სასწრაფოდ უნდა გაირკვეს თუ

რომელი აპლიკაციები ან ბიზნესპროცესები იქნება ამით დაზარალებული.

9.2.3.2. დაცვის მოთხოვნების დადგენა: უსაფრთხოების ინციდენტების გავლენის ანალიზი განსახილველ ბიზნესპროცესებზე

სტრუქტურული ანალიზით დადგენილი ყოველი მნიშვნელობისთვის უნდა განისაზღვროს დაცვის აუცილებლობის ღონისძიება.

მაგალითად, IT-სისტემის ამოვარდნამ შეიძლება გამოიწვიოს დიდი ზარალი, ამიტომ დადგენილი მნიშვნელობა იქნება მაღალი, რადგან IT-სისტემას აქვს შესაბამისად დაცვის მაღალი დონე.

ამგვარად, პირველ რიგში უნდა განისაზღვროს დაცვის მოთხოვნები ბიზნესპროცესებისთვის. შემდეგ, აქედან გამომდინარე, დადგინდება დაცვის მოთხოვნები აპლიკაციებისთვის, რომლებიც სტრუქტურული ანალიზით გამოვლინდა. ამ დროს გათვალიწინებულ უნდა იქნას, თუ რომელი ინფორმაციები მუშავდება ამ აპლიკაციებით.

უმეტეს დაწესებულებებში ამ პოზიციაზე მოიაზრება საკმარისად მცირე საინფორმაციო ჯგუფები. მაგალითად, თუ ეს მოიცავს კლიენტთა მონაცემებს, საერთო წვდომის ინფორმაციას (მაგალითად, მისამართები, ღია სამუშაო საათები) ან სტრატეგიულ მონაცემებს ბიზნესის მართვისთვის, შემდეგ განიხილება აღნიშნული ინფორმაცია სად და რომელი IT-სისტემით მუშავდება, რათა შესაძლებელი იყოს ბიზნესპროცესების შესრულება.

აპლიკაციათა დაცვის მოთხოვნილება გადაიტანება IT-სისტემებზე, რომლებიც შესაბამის დანართებს უჭერენ მხარს. ფართების დაცვის მოთხოვნილება გამომდინარეობს აქ განთავსებული აპლიკაციების და IT-სისტემების დაცვის მოთხოვნილებიდან.

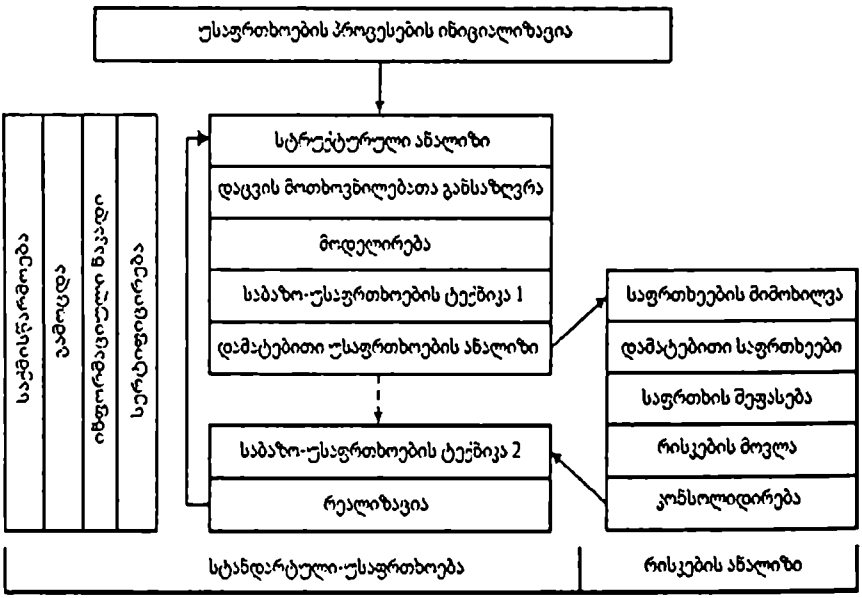
მაგალითად, კლიენტთა მონაცემების დამუშავების ბიზნესპროცესს აქვს დიდი მნიშვნელობა საწარმოო ოპერაციების მხარდასაჭერად. ეს ბიზნესპროცესი მუშაობს S-სერვერზე, რომელსაც აქვს მაღალი დაცვის მოთხოვნილება. სათავსოს, რომელშიც სერვერია განთავსებული, ექნება მინიმუმ მაღალი დაცვის მოთხოვნილება.

9.2.3.3. უსაფრთხოების დამატებითი ანალიზი [DOK]

IT-საბაზო დაცვის მეთოდების გამოყენება იძლევა შესაძლებლობას, უსაფრთხოების ისეთი დონე იყოს უზრუნველყოფილი, რომელიც იქნება საკმარისი და მისაღები ნორმალური დაცვის მოთხოვნებისთვის. თუ დაცვის მოთხოვნილება განსაზღვრული სფეროსთვის (მაგალითად, აპლიკაციისთვის ან IT-სისტემისთვის) უფრო მაღალია ან ამ სფეროსთვის არ არსებობს IT-დაცვის ზომები, მაშინ აუცილებელია IT-საბაზო დაცვის დანერგვით დამატებითი უსაფრთხოების ანალიზის ჩატარება.

BSI-ს აქვს დამუშავებული საკუთარი მეთოდი რისკების ანალიზისთვის, რომელიც ეფუძნება IT-საბაზო დაცვის დანერგვას. იგი აღიწერება BSI-Standard 100-3 წყაროში [31]. მეთოდის სახით შესაძლებელია ასევე კლასიკური რაოდენობრივი რისკების ანალიზის არჩევა განსახილველი სფეროსთვის. თუ განიხილება ინფორმაციის გადამუშავების მხოლოდ მცირე სფერო, მაშინ დანახარჯები დამატებითი რისკების ანალიზისათვის არაა მაღალი.

სტანდარტული უსაფრთხოების ღონისძიებების და რისკების ანალიზის კომბინაცია სფეროებისთვის, რომელთა დაცვის მოთხოვნილებები ნორმალურზე მაღალია, უფრო ეფექტურია, ვიდრე მხოლოდ რაოდენობრივი რისკების ანალიზის გამოყენება (ნახ.1.7).



ნახ.1.7. რისკების ანალიზის ინტეგრაცია უსაფრთხოების პროცესში

9.3. უსაფრთხოების კონცეფციის დანერგვა

IT-საბაზო დაცვის კატალოგები შეიცავს ტიპური სტრუქტურული ელემენტების (ბლოკების), საფრთხეების და ღონისძიებების კატალოგებს. სტრუქტურულ ბლოკებში აღწერილია ინფორმაციის უსაფრთხოების მენეჯმენტის ტიპური ამოცანები და საფრთხეებისა და სტანდარტული უსაფრთხოების ღონისძიებების IT-გამოყენების სფეროები.

ამავდროულად განიხილება ინფორმაციული უსაფრთხოების ორგანიზაციული, პერსონალური, ინფრასტრუქტურული და ტექნიკური ასპექტები.

IT-საბაზო დაცვი კატალოგები შეიცავს ბლოკებს შემდეგი სფეროებიდან:

- ინფორმაციული უსაფრთხოების ძირითადი ასპექტები (ორგანიზაცია, პერსონალი, საგანგებო მზადყოფნა);
- ინფრასტრუქტურის უსაფრთხოება (შენობები, გამოთვლითი ცენტრი);
- IT-სისტემის უსაფრთხოება (სერვერი, კლიენტი, ქსელის კომპონენტები);
- ქსელის უსაფრთხოება (ქსელის და სისტემის მენეჯმენტი);
- აპლიკაციათა უსაფრთხოება (ი-მაილები).

სტრუქტურული ანალიზის შემდეგ შესაძლებელია ბიზნესპროცესების მოდელირება ამ სტრუქტურული ბლოკების დახმარებით. აქ განხილული განსაზღვრის სფეროსთვის განსაზღვრულ იქნება IT-საბაზო დაცვის შესაბამისი ბლოკების ნაკრები (საინფორმაციო ქსელი). აქედან გამომდინარეობს რეკომენდებულ ღონისძიებათა ნაკრები, რომელიც შეიძლება მოიაზრებოდეს როგორც უსაფრთხოების კონცეფციის საფუძველი.

IT-საბაზო დაცვის კატალოგებში შემავალი ღონისძიებების სახით განიხილება კონკრეტული რეალიზაციის დახმარებები

გენერირებული მოთხოვნილებებისთვის როგორც ISO 27001 ან ISO 27002 სტანდარტებიდან, ასევე მრავალრიცხოვანი ტექნიკური ღონისძიებებიდან საიმედო წარმოებისთვის ტიპური IT-სისტემებისა და აპლიკაციებისთვის.

დეტალური სახელმძღვანელო სტრუქტურული ბლოკების შესარჩევად (მოდელირება საბაზო დაცვის მიხედვით) გვეხმარება უსაფრთხოებასთან დაკავშირებული ასპექტების გათვალისწინებაში. ასეთი დახმარებით სახელმწიფო ორგანიზაციებს ან კერძო ბიზნესს შეუძლია სასურველი მიზნების მიღწევა უსაფრთხოების სფეროში, გარე კონსულტანტების გარეშე ან მათი მცირე დახმარებით.

II ნაწილი
10. ITIL -ინფორმაციული ტექნოლოგიების ინფრასტრუქტურის ბიბლიოთეკა

10.1. შესავალი ITIL–ში. ძირითადი ტერმინები

ITIL - Information Technology Infrastructure Library არის ინფორმაციული ტექნოლოგიების ინფრასტრუქტურის ბიბლიოთეკა. იგი დღეისათვის ძალზე აქტუალური და საყოველთაოდ ცნობილი ცოდნის ბაზაა სერვისების მართვის სფეროში მთელი მსოფლიოს მასშტაბით [3,11,38]. ის ასახავს IT–სფეროს მსოფლიოს წამყვანი პრაქტიკოსების მიერ შემუშავებულ ფუნდამენტურ საფუძვლებს. ევროპაში არსებობს ITIL სერტიფიცირების ორი ცენტრი: EXIN – ჰოლანდიის საგამოცდო ინსტიტუტი და ISEB (Information Systems Examination Board) – ბრიტანეთის კომპიუტერული საზოგადოების განყოფილება [39,40].

ITIL განიხილავს სერვისების მართვას ურთიერთმოქმედების კონტექსტში: „სერვისების მიმწოდებელი– სერვისების დამკვეთი".

დამკვეთი (Customer) – ესაა საქონლის ან მომსახურების მყიდველი. IT–სერვისების მიმწოდებლისთვის დამკვეთი არის ადამიანი (ან ადამიანთა ჯგუფი), რომელიც აფორმებს შეთანხმებას მიმწოდებელთან IT–მომსახურების მისაღებად და პასუხს აგებს მიღებული მომსახურების ანაზღაურებაზე.

მიმწოდებელი (Service provider) – ესაა ორგანიზაცია, რომელიც აწვდის სერვისს ერთ ან რამდენიმე შიგა ან გარე დამკვეთს.

მომხმარებელი – ესაა IT–სერვისების გამომყენებელი თანამშრომელი დამკვეთ ორგანიზაციაში.

IT–მომსახურება (სერვისი) – დამკვეთებისთვის ფასეულობის მიწოდების ხერხი, რომელთა საშუალებითაც ისინი

ღებულობენ გამოსასვლელზე საჭირო შედეგებს მათთვის სპეციფიკური დანახარჯებისა და რისკების გარეშე.

შეიძლება განვიხილოთ სხვაგვარი განსაზღვრებაც. IT–მომსახურება – ესაა ერთი ან მეტი ტექნიკური ან პროფესიონალური შესაძლებლობა, რომელიც ხელს უწყობს ბიზნესპროცესს. ტერმინები „სერვისი" და „მომსახურება" ეკვივალენტურია. მათ აქვს შემდეგი მახასიათებლები:

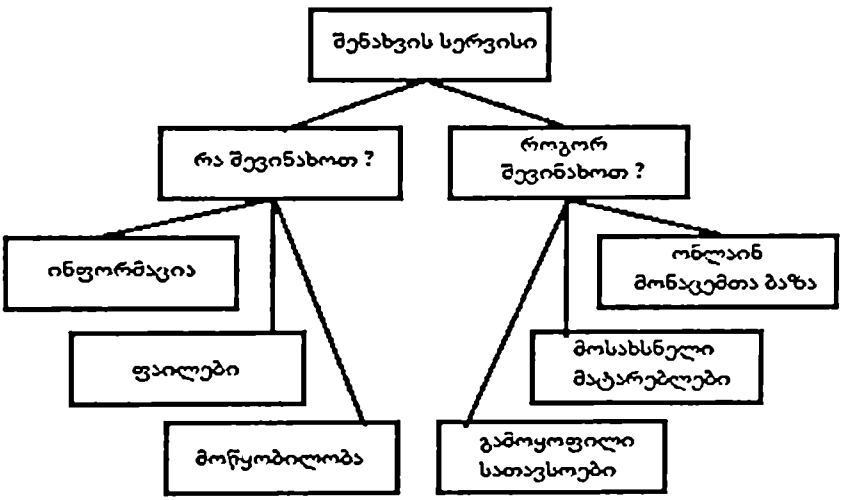
- აკმაყოფილებს დამკვეთის ერთ ან მეტ მოთხოვნას;
- მხარს უჭერს დამკვეთის ბიზნესმიზნებს;
- დამკვეთისგან აღიქმება როგორც ერთი მთლიანი პროდუქტი, რომელიც მზადაა გამოსაყენებლად.

განვიხილოთ დეტალურად ძირითადი ცნებები სერვისის განსაზღვრებაში.

შედეგები გამოსასვლელზე (outcomes) – ის, რასაც ღებულობს დამკვეთი საბოლოო ჯამში. ცხადია, რომ იგი განსხვავდება დამკვეთის საწყისი მოთხოვნებისგან გარკვეული შემზღუდველი ფაქტორების არსებობის გამო. სერვისის დანიშნულებაა ამ ფაქტორების შემცირების და მწარმოებლურობის ამაღლების გზით გამოსასვლელი შედეგების გაუმჯობესება. სერვისების გამოყენების შედეგია გამოსასვლელზე სასურველი შედეგების მიღების ალბათობის გაზრდა.

მომსახურების მოდელები, რომელთაც ITIL გვთავაზობს, გვეხმარება IT–სფეროს სირთულეების, ხარჯების, მოქნილობის და მრავალსახეობის მართვაში. ყოველ მოდელს აქვს გამოყენების ვარიანტების სიმრავლე კონკრეტული შემთხვევისგან დამოკიდებულებაში, რაც მისი გამოყენების იდეას ხდის უნივერსალურს, მოქნილს და ეფექტურს.

IT–სერვისის მოდელი შეიძლება განვიხილოთ ინფორმაციის შენახვის სისტემის მაგალითზე. სისტემა დანიშნულია ინფორმაციის შენახვის, მოწესრიგების და დაცვის განსახორციელებლად რაიმე სამუშაოს ან მოქმედების კონტექსტში. თუ მიმწოდებელი აძლევს დამკვეთს არა მხოლოდ დასამახსოვრებელ მოწყობილობას, არამედ აგრეთვე ინფორმაციის შენახვის სერვისსაც, მაშინ უნდა გაეცეს პასუხი კითხვებს „რა შევინახოთ“ და „როგორ შევინახოთ“ (ნახ.10.1). ამასთანავე პრინციპულად მნიშვნელოვანია მოვალეობების და პასუხისმგებლობების განაწილება მიმწოდებელსა და დამკვეთს შორის.



ნახ.10.1. ინფორმაციის შენახვის სისტემის სქემა

დამკვეთებს სურთ სასურველი შედეგების მიღება, მაგრამ სხვადასხვა მიზეზთა გამო, არ სურთ თანმხლები პასუხისმგებლობის აღება, ხარჯები და რისკები. მაგალითად,

ორგანიზაციას უნდა დაცული ინფორმაციის შენახვის სისტემის შექმნა რამდენიმე ტერაბაიტით ონლაინ-ვაჭრობის მხარდასაჭერად.

ასეთი სისტემის შესაქმნელად „ნულიდან“ ამ ორგანიზაციამ უნდა განვლოს გრძელი გზა, დაწყებული იმის გაგებით, თუ როგორ გააკეთოს, დამთავრებული ძვირადღირებული ტექნიკის შესყიდვით და კვალიფიციური პერსონალის დაქირავებით. ეს კი მეტად ძვირადღირებული სიამოვნება და დროის დიდი დანახარჯია.

შედარებით მარტივია ამ შემთხვევაში მიმწოდებლის სერვისების გამოყენება, რომელიც უკვე ფლობს ინფორმაციის შენახვის დიდ სისტემას, აქვს შესაბამისი გამოცდილება და შესაძლებლობები. ეს იქნება ინფორმაციის დაცული შენახვის სერვისის შეთავაზება.

სერვისის ფასი (value) – იგი იზომება ორი ცნების კონტექსტში:

- სერვისის სარგებლობა (Service Utility) – არის ის, რასაც ღებულობს დამკვეთი სერვისის გამოყენებით;
- სერვისის ხარისხის გარანტია (Service Warranty) – არის ის, თუ როგორ აძლევს მიმწოდებელი დამკვეთს სერვისს – წვდომის, მწარმოებლურობის და უსაფრთხოების ტერმინებში.

ITILv3-ის ლექსიკონის განსაზღვრებანი:

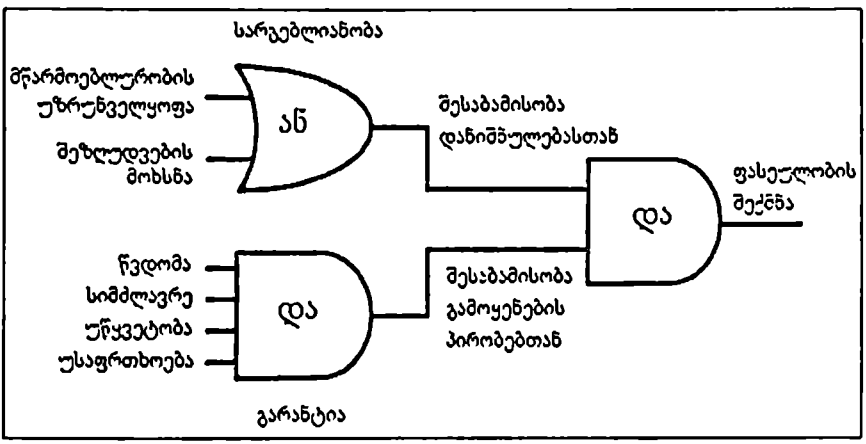
სარგებლიანობა – ფუნქციონალობა, რომელსაც იძლევა პროდუქტი ან სერვისი განსაზღვრულ მოთხოვნილებათა უზრუნველსაყოფად. ხშირად განისაზღვრება როგორც „რას აკეთებს პროდუქტი/სერვისი“.

სერვისის სარგებლიანობა – IT-მომსახურების ფუნქციონალობა დამკვეთის თვალსაზრისით.

გარანტია – დაპირება ან გარანტია იმისა, რომ პროდუქტი ან სერვისი დააკმაყოფილებს შეთანხმებულ მოთხოვნებს.

მომსახურების ხარისხის გარანტია – დარწმუნება იმაში, რომ IT–სერვისი შესაბამისი იქნება შეთანხმებულ მოთხოვნებთან. შესაძლებელია ფორმალური შეთანხმების არსებობა, ხელშეკრულება ან როგორც მარკეტინგული შეტყობინება.

ამგვარად, სარგებლიანობა ისაა, რასაც დამკვეთი ღებულობს, ხარისხის გარანტია – ის, თუ როგორ ღებულობს (ნახ.10.2).



ნახ.10.2. სერვისის ფასეულობის ფორმირების სქემა

დამკვეთს, შეიძენს რა სერვისს, უნდა შედეგის მიღება მისი გამოყენებით, ანუ ფასეულობის ამოღება.

სარგებლიანობა მიიღწევა ერთ-ერთი ხერხით:

1. დამკვეთის მიერ მოთხოვნილი მწარმოებლურობის უზრუნველყოფით;
2. არსებული შეზღუდვების მოცილებით ან შემცირებით.

მწარმოებლურობა (Performance) - შეფასებაა იმისა, რაც იქნა მიღწეული ან შემუშავებული სისტემის, ადამიანის, გუნდის, პროცესის ან IT– სერვისის მიერ [11].

მწარმოებლურობაში იგულისხმება დამკვეთის შესაძლებლობა, გააკეთოს მეტი ნაკლებ დროში ნაკლები დანახარჯებით, ანუ ნაკლები რესურსების გამოყენებით. სხვა სიტყვებით, ესაა გარკვეული ოპტიმიზაცია, რომელიც უზრუნველყოფს დამკვეთს, გადაწყვიტოს ამოცანა ნაკლები დროის და ფულის გამოყენებით.

შეზღუდვა – ესაა აკრძალვა ან შეუძლებლობა რაღაც ქმედებათა შესასრულებლად.

გარანტია შედგება ოთხი ძირითადი ასპექტისგან:

- წვდომა;
- სიმძლავრე;
- უსაფრთხოება;
- უწყვეტობა.

სერვისის ხარისხის გარანტიის შეფასება უფრო მარტივია, ვიდრე მისი სარგებლიანობისა ბიზნესისთვის. როცა ადამიანი აჭერს ღილაკს, ის ელოდება, რომ აინთება სინათლე. სამწუხაროდ, IT–სერვისების დროს არც ასე მარტივადაა საქმე. IT–სერვისის გამოყენების შედეგი დამოკიდებულია არა მხოლოდ სერვისის თვისებებზე, არამედ ამ სერვისის მართვაზეც. სწორედ აქ ჩნდება ტერმინი service management.

IT–სერვისების მართვა – ესაა სპეციალიზებული ორგანიზაციული შესაძლებლობების ერთობლიობა, დამკვეთისთვის ფასეულობის მისაწოდებლად სერვისის ფორმაში [11]. „სპეციალიზებულ შესაძლებლობებში“ იგულისხმება პროცესები, მეთოდები, ფუნქციები და როლები, რომელთა გამოყენება შეუძლია მიმწოდებელს დამკვეთისთვის სერვისის

მიწოდების მიზნით. გამოიყენება ასევე აღნიშვნა ITSM (IT Service Management), რომელიც „სერვისების მართვის“ ეკვივალენტურია.

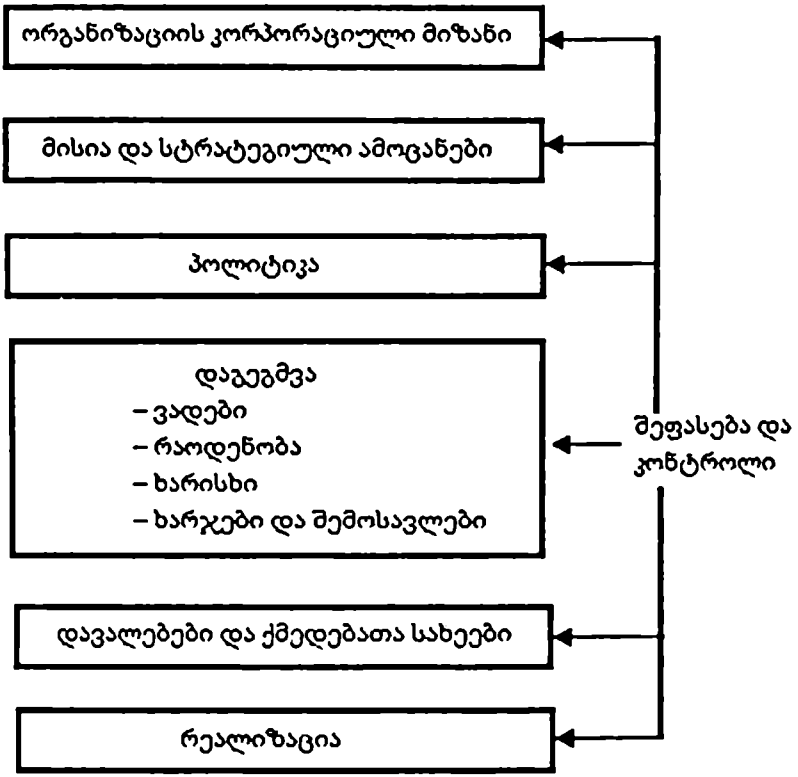
ხარისხი - ობიექტის მახასიათებელთა ერთობლიობაა, რომელიც მიეკუთვნება მის შესაძლებლობას, რათა დააკმაყოფილოს დადგენილი და შემოთავაზებული მოთხოვნები.

ორგანიზაციას შეუძლია ძალზე ძვირი IT–სერვისის ყიდვა, მაგრამ თუ მიმწოდებელს არ შეუძლია ხარისხიანი და საპასუხისმგებლო მართვის უზრუნველყოფა – მაშინ ეს შესყიდვა იქნება უაზრო. დამკვეთის დაკმაყოფილება ბევრადაა დამოკიდებული იმაზე, თუ რამდენად სწორად იქნა შეთანხმებული სერვისის პარამეტრები წინასწარ სერვისის მიმწოდებელთან.

ამგვარად, სერვის-მენეჯმენტის ძირითადი მიზანი ITIL კონტექსტში არის დამკვეთებისადმი საიმედო, სტაბილური IT–სერვისების მიწოდება, რომლებიც სრულად დააკმაყოფილებს მათ მოთხოვნებს მოცემულ სფეროში. ერთ-ერთი საკვანძო ტერმინი ITIL–ში არის „ორგანიზაცია“. IT–სერვისის დამკვეთი და IT-სევრისის მიმწოდებელი განიხილება, როგორც ორგანიზაციები.

ორგანიზაცია - ესაა ადამიანთა თანამშრომლობის განსაზღვრული ფორმა. ისმის კითხვა, რაში მდგომარეობს მიზანი ორგანიზაციად გაერთიანებისა ? ასეთი კორპორატიული მიზანი (vision) შეიძლება იყოს, მაგალითად, ფულის გამომუშავების სურვილი პერსონალური კომპიუტერების გაყიდვით ან სერვისის შეთავაზება ინტერნეტში ჩასართავად. იმისათვის, რომ ორგანიზაცია იყოს მიმზიდველი დამკვეთების, ინვესტორების და კომპანიის თანამშრომლებისთვის, საჭიროა ინფორმაციის მიწოდება, თუ რა უპირატესობა ექნებათ მათ ამ ორგანიზაციასთან თანამშრომლობისას.

კორპორატიული მიზნის გასაცნობად კომპანიას შეუძლია მისი წარმოდგენა თეზისის სახით თავის მისიაზე (mission) (ცხრ.10.3).



ნახ.10.3. ორგანიზაციის კორპორაციული მიზნის ფორმირება

მისია – ესაა ამოცანების მოკლე და ცხადად აღწერა, რომლებიც დგას ორგანიზაციის წინაშე და ის იდეალები, რომლებისაც მას (ორგანიზაციას) სწამს.

სტრატეგიული ამოცანები (objectives) – ესაა სრული აღწერა იმისა, რასაც უნდა მიაღწიოს ორგანიზაციამ გრძელვადიან

პერსპექტივაში. კარგად ფორმულირებული სტრატეგიული ამოცანები უნდა ფლობდეს ხუთ ძირითად თვისებას (შეესაბამებოდეს SMART პრინციპს):

- იყოს კონკრეტული (Specific);
- ექვემდებარებოდეს შეფასებას (Measurable);
- იყოს სიტუაციისადმი შესაფერისი და შესაბამისი (Appropriate);
- იყოს რეალისტური (Realistic);
- ჰქონდეს მკაფიო დროითი საზღვრები (Time-bound).

ორგანიზაციის პოლიტიკა (policy) – ესაა გადაწყვეტილებების და ზომების ერთობლიობა, მიღებული ორგანიზაციის მიერ სტრატეგიული ამოცანების დასასმელად და მათ გადასაწყვეტად.

ორგანიზაცია თავისი პოლიტიკის შემუშავების დროს განსაზღვრავს პრიორიტეტებს, რომლებიც მის წინაშეა სტრატეგიული ამოცანების და მათი გადაწყვეტის მიზნით. პრიორიტეტები შეიძლება შეიცვალოს დროის შესაბამისად. ზუსტად ჩამოყალიბებული კომპანიის პოლიტიკა (წესები) ხელს უწყობს ორგანიზაციის სტრუქტურის მოქნილობას, რადგან კომპანიის ყველა დონეზე შესაძლებელია სიტუაციის ცვლილებებზე სწრაფი რეაგირება [11].

პოლიტიკის რეალიზაცია კონკრეტული სახის ქმედებებისთვის მოითხოვს სტრატეგიის შემუშავებას. სტრატეგია მუშავდება განსაზღვრული პერიოდებისთვის და შედგება რამდენიმე ეტაპისგან. მნიშვნელოვანია აქ კონტროლის შესაძლებლობა სამუშაოთა შესრულებისას.

არსებობს სხვადასხვა მეთოდები. მაგალითად, ბიზნესში ცნობილია ბალანსირებულ შეფასებათა რუკა (Balanced Score Card - BSC). ამ მეთოდის შესაბამისად ორგანიზაციის სტრატეგიული

მიზნების ან პროცესების მიზნების საფუძველზე განისაზღვრება წარმატების კრიტიკული ფაქტორები (Critical Success Factor - CSF).

წარმატების კრიტიკული ფაქტორები (Critical Success Factor - CSF) – ესაა ფაქტორები, რომლებიც აუცილებლად უნდა განხორციელდეს პროექტის, პროცესის, გეგმის ან სერვისის წარმატებისათვის. ასეთი ფაქტორები ფორმულირდება კომპანიის ინტერესების რამდენიმე უმნიშვნელოვანესი სფეროსთვის, რომელთაც უწოდებენ ორგანიზაციის პერსპექტივებს (პროექციებს): დამკვეთები / ბაზარი, ბიზნესპროცესები, პერსონალი / ინოვაციები და ფინანსები. რამდენად წარმატებით რეალიზდება CSFs, გამოიყენებენ KPI-ს.

მწარმოებლურობის გასაღებური მაჩვენებელი (Key Performance Indicator ან KPI) – ესაა მეტრიკა, რომელიც გამოიყენება პროცესების, სერვისის ან ქმედებების სამართავად [11]. შესაძლებელია ეფექტურობის მრავალი მაჩვენებლის შეფასება, მაგრამ განსაკუთრებით მნიშვნელოვანია მხოლოდ KPI.

მაგალითად, ფაქტორი „სერვისის დაცვა ცვლილებების რეალიზაციისას“ შეიძლება გაიზომოს ისეთი KPI-ით, როგორიცაა „არაწარმატებული ცვლილებების რაოდენობის შემცირება %-ში“, „პროცენტული შემცირება, ცვლილებათა რაოდენობის, რომელთაც მივყავართ ინციდენტების აღმოცენებამდე“ და ა.შ.

სხვადასხვა გარემოებათა ზემოქმედების და ეფექტურობის შეფასების შედეგებისგან ზემოქმედებით საკონტროლო წერტილებში სტრატეგიული ამოცანები, მისიები და კორპორაციული მიზნები შეიძლება მნიშვნელოვნად შეიცვალოს.

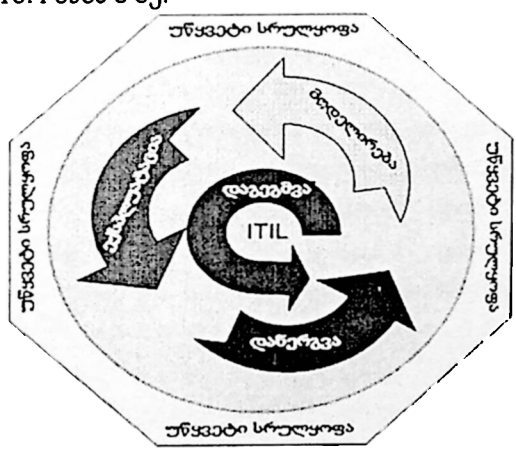
ამასთანავე IT-განყოფილების ან სერვისის მიმწოდებლების სტრატეგიული ამოცანები აგრეთვე უნდა შეიცვალოს ბიზნესის მიზნების მოთხოვნების შესაბამისად.

10.2. სერვისის სასიცოცხლო ციკლი

ITILv3 საფუძველს შეადგენს შემდეგი ექვსი პუბლიკაცია (ანუ ბირთვი):

1. შესავალი ITIL – ში
2. სერვისის დაგეგმვა (Service Strategy)
3. სერვისის პროექტირება (Service Design)
4. სერვისის დანერგვა (Service Transition)
5. სერვისის ექსპლუატაცია (Service Operation)
6. სერვისის უწყვეტი სრულყოფა (Continual Service Improvement).

ხუთი წიგნი შეესაბამება სერვისების სასიცოცხლო ციკლის ეტაპებს (შესავლის გარდა): ბიზნესის მოთხოვნების პირველადი ანალიზიდან დაწყებული, სტრატეგიის აგებისა და პროექტირების ეტაპებზე, და დამთავრებული სერვისების სრულყოფით ექსპლუატაციის პროცესში. სერვისის სასიცოცხლო ციკლი მოცემულია 10.4 ნახაზზე.



ნახ.10.4. სერვისის სასიცოცხლო ციკლი

სერვისის დაგეგმვა (ან სტრატეგიის აგება) – ესაა სერვისის სასიცოცხლო ციკლის საფუძველი. მისი შესაბამისი პუბლიკაცია აღნიშნავს სერვის-მენეჯმენტის ცნების ფუნდამენტურობას სერვისის სასიცოცხლო ციკლის კონტექსტში. წიგნში განიხილება შემდეგი საკითხები: IT–სერვისის ბაზრის განვითარება, სერვისების მიმწოდებელთა მახასიათებლები და ტიპები, სერვისის ძირითადი ხარისხები და რეალიზაციის სტრატეგია სასიცოცხლო პროცესის ციკლში. საკვანძო თემებია ასევე ფინანსური მართვა, მოთხოვნების მართვა, ორგანიზაციული განვითარება და სტრატეგიული რისკები.

მიმწოდებელმა უნდა გამოიყენოს სერვისის დაგეგმვის ეტაპი მიზნების დასასმელად, მომხმარებელთა და გასაღების ბაზრის მოლოდინის (სურვილების) გასარკვევად. სტრატეგიის აგების დანიშნულება, უპირველეს ყოვლისა, არის ის, რომ სერვისების მიმწოდებელმა შეაფასოს საკუთარი შესაძლებლობები და გადაწყვიტოს, შეძლებს თუ არა იგი განახორციელოს სერვისული პორტფელის მოთხოვნები ყველა ხარჯის და რისკის გათვალისწინებით.

სერვისების პორტფელი (ან პორტფოლიო) – ესაა სერვისების სრული ერთობლიობა, რომელიც წარმოჩინდება სერვისების მიმწოდებლის მიერ. პორტფელი გამოიყენება ყველა სერვისის მართვისათვის მთელი სასიცოცხლო ციკლის განმავლობაში. იგი შეიცავს სამ კატეგორიას:

1) სერვისები მუშავდება (Service Pipeline) – სერვისები , რომლებიც დამუშავების სტადიაშია;
2) სერვისების კატალოგი – უკვე გამოყენებადი ან შეთავაზებული სერვისების;
3) სერვისები, რომლებიც ამოღებულია ექსპლუატაციიდან (retired Services).

სერვისის დაპროექტება. ყოველი IT-სერვისისთვის ყველაზე მნიშვნელოვანია ბიზნესს წარუდგინოს გარკვეული სარგებელი ან ფასეულობა. ამიტომ მიმწოდებელმა უნდა გაითვალისწინოს ბიზნესის მიზნები.

პუბლიკაცია „სერვისების დაპროექტება“ არის სახელმძღვანელო სერვისების მოდელირებისა და სრულყოფისთვის, ასევე რეკომენდაციებისთვის მათ სამართავად პრაქტიკაში. ამ ეტაპზე აღიწერება ძირითადი პრინციპები და მოდელირების მეთოდები სტრატეგიული მიზნების გარდაქმნისათვის განსაზღვრული ხარისხის კონკრეტული სერვისების ერთობლიობაში. იგი მოიცავს ასევე ახალი სერვისების შექმნის, არსებულის ცვლილების და სრულყოფის საკითხებს სასიცოცხლო ციკლის ფარგლებში, რაც აუცილებელია მის ფასეულობათა ასამაღლებლად მომხმარებელთა თვალსაზრისით.

წიგნის საკვანძო თემებია ასევე სერვისების კატალოგი, სარგებლიანობა, მწარმოებლურობა და სერვისის უწყვეტობა, სერვისების მართვის დონე, რომლებიც განიხილება შემდგომ.

სერვისის დანერგვა. Transition – გადაადგილება, გადასვლა ან ერთი მდგომარეობის შეცვლა მეორით (პოზიციის, პერიოდის, სტადიის, თემის და სხვა). მისი შესაბამისი პუბლიკაცია ITIL ბიბლიოთეკაში არის სახელმძღვანელო იმაზე, თუ ეფექტურად როგორ მოხდეს მოთხოვნების რეალიზება, რომლებიც ფორმულირებული იქნება პროექტირების და სტრატეგიის აგების სტადიებზე, ექსპლუატაციის ეტაპზე რისკების, მტყუნებების და გაუმართაობების კონტროლით. განიხილება რისკების მართვის საკითხებიც.

სერვისის ექსპლუატაცია ახორციელებს სერვისის ბიზნეს-მნიშვნელობის „მიტანის“ ეტაპს მიმწოდებლიდან დამკვეთამდე. აქ მნიშვნელოვანია სერვისის მიწოდების ეფექტურობა და მისი ხარისხიანი თანხლება. წიგნი აღწერს, თუ როგორ შეიძლება

განხორციელდეს სერვისის სტაბილური ექსპლუატაცია, ცვლილების განხორციელების შესაძლებლობასთან ერთად დიზაინში, მასშტაბში, საზღვრებში და ა.შ. ორგანიზაციებს მიეცემათ ინსტრუქციები, მეთოდები და ინსტრუმენტები კონტროლის ორი მეთოდის სარეალიზაციოდ – პრევენციული (პროფილაქტიკური) და პროაქტიური.

წიგნში მოცემული ინფორმაცია სასარგებლო იქნება გადაწყვეტილების მისაღებად სერვისის წვდომის მართვის საკითხებში, სერვისზე მოთხოვნილების კონტროლისთვის, დატვირთვის ოპტიმიზაციისა და მიმდინარე პრობლემების გადასაწყვეტად.

აღწერილი ყველა ხერხი ითვალისწინებს ახალი მოდელების და არქიტექტურის შესაძლებლობებს, როგორიცაა განაწილებული სერვისები, გაანგარიშებები სქემით „კომუნალური სერვისი“ (utility computing), ვებ-სერვისი და ელ-კომერცია.

სიტყვა utility computing აღწერს ახალ შემოტანილ ბიზნეს–მოდელს, როცა სერვისების მიმწოდებელი ღებულობს ფულს სერვისის გამოყენების ფაქტზე, მაგალითად, მისი გამოყენების დროის მიხედვით. ტრადიციულ ბიზნესმოდელში კი მომხმარებელი იხდის სისტემის (სერვისის) ფლობისათვის.

ასეთი სერვისების პროვაიდერს შეუძლია თავისი რესურსების გამოყენების ოპტიმიზაცია მომხმარებელთა განსხვავებული საჭიროების გათვალისწინებით.

სერვისის უწყვეტი სრულყოფა მდგომარეობს სერვისის ფასეულობის ამაღლების მეთოდების და საშუალებების აღწერაში სასიცოცხლო ციკლის სხვადასხვა ეტაპზე სრულყოფის რეალიზაციის გზით. ეს ეტაპი აერთიანებს თავის თავში ხარისხის, ცვლილებების და მწარმოებლურობის სრულყოფის მართვის პრინციპებს, პრაქტიკასა და მეთოდებს. წიგნიდან ორგანიზაციებმა

შეიძლება მიიღონ რეკომენდაციები იმის შესახებ, თუ ეტაპობრივად როგორ სრულყონ მსხვილმასშტაბური სერვისები ხარისხობრივად, ექსპლუატაციის ეფექტურობისა და სერვისების მიწოდების შეუწყვეტლად. სახელმძღვანელო განკუთვნილია სრულყოფის შედეგების უკუკავშირის უზრუნველსაყოფად დაგეგმვის, მოდელირების და გარდაქმნების ეტაპებთან.

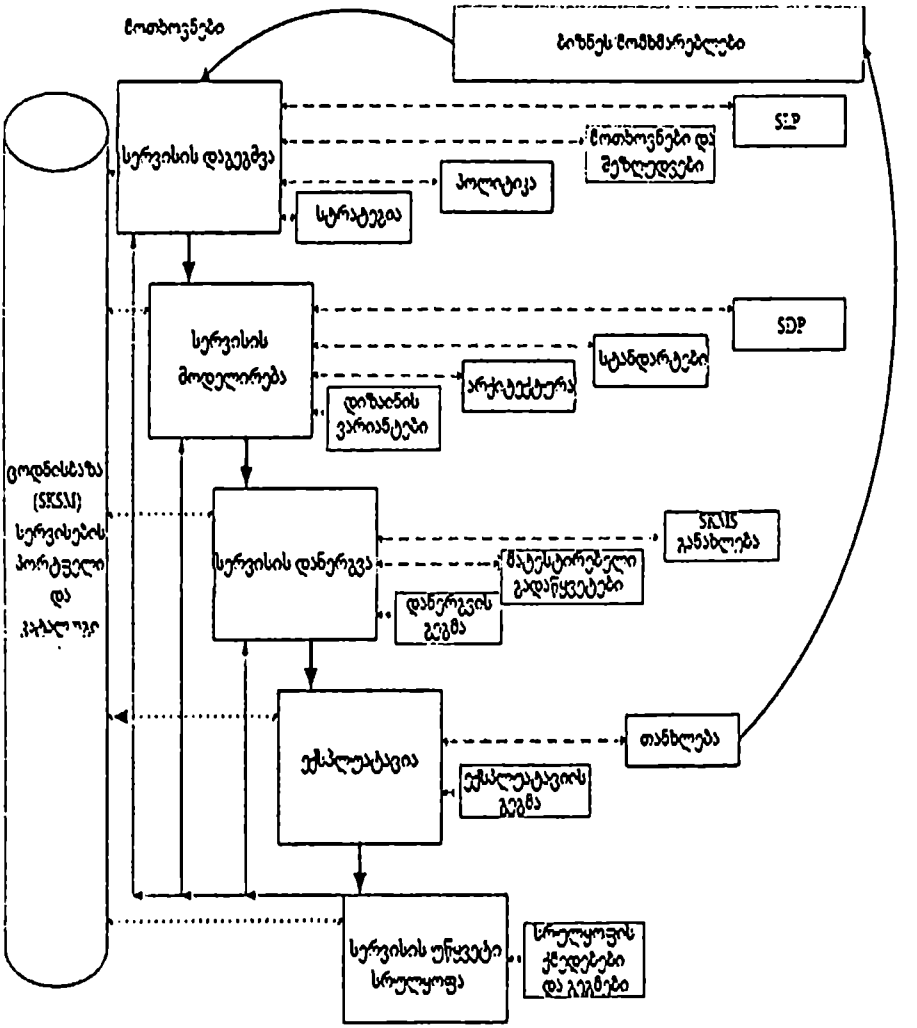
ნახაზი 10.5 გვიჩვენებს, თუ როგორაა დამოკიდებული სერვისის სასიცოცხლო ციკლის ეტაპები ბიზნესის მოთხოვნილებათა ცვლილებებზე.

მოთხოვნილებები იქმნება სერვისის დაგეგმვის ეტაპზე სერვისების დონეების პაკეტის ჩარჩოში (Service Level Package ან SLP). ესაა სარგებლიანობის განსაზღვრული დონე და გარანტიები ცალკეული სერვისების პაკეტისთვის. ყოველი SLP მუშავდება ცალკეული პროფილის ბიზნესქმედების მოთხოვნილებათა სარეალიზაციოდ.

ეს პროცესი გადადის სერვისის დაპროექტებაში, სადაც გადაწყვეტილებები, მიღებული პირველ ეტაპზე, გროვდება ერთად და რეალიზდება სერვისის საპროექტო დოკუმენტაციის სახით (Service Design Package ან SDP). ესაა დოკუმენტები, რომლებიც განსაზღვრავს სერვისის ყველა ასპექტს და მის მიმართ მოთხოვნებს სასიცოცხლო ციკლის ყოველ ეტაპზე [11].

ფაქტობრივად ესაა საპროექტო დოკუმენტაცია, რომელიც მუშავდება ახალი სერვისისთვის მნიშვნელოვანი ცვლილებების შესატანად ან სერვისის ექსპლუატაციიდან მოხსნის დროს.

SDP გადადის დანერგვის ეტაპზე, რომელზეც ხდება სერვისის ტესტირება, გადის შეფასებას და ვალიდაციას. შედეგად განახლდება სერვისების ცოდნის მართვის სისტემა და სერვისი გადადის ექსპლუატაციის სტადიაზე.



ნახ.10.5. სერვისის სასიცოცხლო ციკლის ეტაპების ძირითადი კავშირები, შესასვლელები და გამოსასვლელები

10.3. სერვისების ცოდნის ბაზის მართვის სისტემა

სერვისების ცოდნის ბაზის მართვის სისტემა (Service Knowledge Management System ან SKMS) – ესაა ინსტრუმენტების და მონაცემთა ბაზების ერთობლიობა, რომლებიც გამოიყენება ცოდნის და სერვისების შესახებ ინფორმაციის სისტემატიზაციისთვის. იგი ინახავს, მართავს, განაახლებს და წარმოადგენს მთელ ინფორმაციას, რომელიც საჭიროა მიმწოდებლისთვის სერვისის მართვისათვის სასიცოცხლო ციკლის ყველა ეტაპზე.

ბუნებრივია, რომ მთელი სასიცოცხლო ციკლის განმავლობაში სერვისი უნდა გაუმჯობესდეს ამის აუცილებლობის შემთხვევაში და შესაბამისი შესაძლებლობების დროს.

IT–ინფრასტრუქტურის მართვის წარმოდგენა პროცესების კომპლექსის სახით საშუალებას იძლევა უნიფიცირებულ იქნას სერვისების მიმწოდებლებისა და დამკვეთების მრავალი ასპექტი. ყოველი პროცესისთვის განისაზღვრება როლები, მიზნები, ამოცანები, მეთოდები და საშუალებები, აგრეთვე შემავალ-გამომავალი ინფორმაცია.

ამგვარად, ITILv3-ის ძირითადი დანიშნულებაა IT–სერვისების ხარისხიანი წარმოდგენა და მხარდაჭერა ბიზნესის მოთხოვნების შესაბამისად. პრინციპული განსხვავება მე-3 და მე-2 ვერსიებს შორის ისაა, რომ შეიქმნა სერვისების მართვის პრინციპების აღწერის მიდგომა.

სერვისების მართვის პროცესების დაჯგუფებასთან ერთად სასიცოცხლო ციკლის ცალკეული პერიოდების მიხედვით, ITILv3 გვთავაზობს IT–სერვისზე ვისაუბროთ ბიზნესისთვის დამატებითი ფასეულობის შეთავაზების კონტექსტში.

ITILv2–ში IT–სამსახური სერვისებს სთავაზობდა ბიზნესს თავისი არსებული ინფრასტრუქტურის ბაზაზე, ცდილობდა რა

ბიზნესისთვის გასაგებ ტერმინებში ჩამოეყალიბებინა მომსახურების (სერვისების) ხარისხის მახასიათებლები.

ITILv3 გვთავაზობს სრულიად ახალ მიდგომას. IT–სამსახური აანალიზებს ბიზნესის მიზნებს და ამოცანებს და, აქედან გამომდინარე, გვთავაზობს სერვისებს, რომლებიც ნამდვილად სჭირდება ბიზნესს ამჟამად.

ITIL–ის გამოყენება არაა სავალდებულო, როგორც ეს, მაგალითად, უსაფრთხოების ან აუდიტის სტანდარტებითაა გათვალისწინებული, მაგრამ ITIL ბოლო ათი წლის განმავლობაში მთელ მსოფლიოში გახდა დე-ფაქტო სტანდარტი IT–სერვისების მართვის სფეროში.

11. სერვისების სტრატეგიის აგება

11.1. სტრატეგიის აგება – სერვისების სასიცოცხლო ციკლის ეტაპი

სერვისების თანამედროვე მსხვილი მიმწოდებლები მსგავსი მახასიათებლებით და შესაძლებლობებით ხასიათდებიან. მათ შორის მთავარი განმასხვავებელი თავისებურება სტრატეგიაა, რომელსაც კონკრეტული მიმწოდებელი იყენებს სერვისებისთვის.

სტრატეგიის აგების დროს სერვისის მიმწოდებელი ორიენტირებული უნდა იყოს, უპირველეს ყოვლისა, თავისი პოტენციური დამკვეთის მიზნებზე. ამიტომ ცხადად უნდა ესმოდეს თუ რა როლი უნდა შეასრულოს მიწოდებულმა IT-სერვისმა დამკვეთის ბიზნესში.

IT-სფეროს სწრაფი განვითარება უკვე დღეს მოითხოვს მიმწოდებლებისგან არა მხოლოდ დამკვეთების მოთხოვნებზე ოპერატიულ რეაგირებას, არამედ იმის ცოდნასაც, თუ მომავალში რა დასჭირდება დამკვეთს. ამიტომაც სტრატეგიის აგება არის ფუნდამენტური ეტაპი სერვისის სასიცოცხლო ციკლში. მიმწოდებელს უნდა ესმოდეს, რომ დამკვეთი მისგან ყიდულობს არა კონკრეტულ პროდუქტს, არამედ საშუალებებს თავიანთი ბიზნესმოთხოვნების დასაკმაყოფილებლად.

სტრატეგიის ასაგებად მიმწოდებელმა უნდა გაითვალისწინოს ფაქტორების სიმრავლე, რომელთაგან ძირითადია:

1. ყველაფერი, რაც IT-სერვისების ირგვლივაა, რთულია: ეს ეხება არა მხოლოდ კონკრეტული სერვისების ინდივიდუალურ თავისებურებებს, არამედ იმ სირთულეებს, რომლებიც აღმოცენდება IT-სფეროში ცვალებადი და ურთიერთ-დამოუკიდებული ფაქტორების სიმრავლის შედეგად. საჭიროა განვასხვავოთ მოკლევადიანი და გრძელვადიანი დაგაგმვა, რადგან

ბაზრის, მომხმარებელთა და თვით IT-სფეროს ქცევები განსხვავებულია განსახილველი პერიოდისგან დამოკიდებულებით. პირველი რიგის ამოცანად განიხილება მეთოდების შემუშავება, რომლებიც დაეხმარება ორგანიზაციებს გადაწყვეტილების მისაღებად და შემდგომი ქმედებების სტრატეგიის განსაზღვრაში;

2. დამკვეთების მოთხოვნები ყოველთვის არაა ცხადი, გასაგები და კორექტულიც კი. მრავალი მათგანი იკარგება საპროექტო დოკუმენტაციიდან სერვისის რეალიზაციაზე გადასვლის პროცესში. სტრატეგიული აზროვნების ყველაზე მნიშვნელოვანი ასპექტია იმის გაცნობიერება, თუ რა უნდა იქნას მიღებული შედეგად. ის, რასაც დამკვეთი ღებულობს თავისი სერვისის ტექნიკური მოთხოვნების სანაცვლოდ, არის საფუძველი მისი დაგეგმვის. დამკვეთთა მოთხოვნების და მიზნების გაგება გვთავაზობს არა მხოლოდ ცოდნას, თუ როდის და რატომ წარმოიშვა კონკრეტული მოთხოვნები, არამედ ცხადად მიუთითებს თუ ვინაა IT–სერვისის საბოლოო მომხმარებელი;

3. კონტექსტისგან დამოუკიდებლად, რომელშიც მუშაობს მიმწოდებელი, სტრატეგიის აგების დროს მან უნდა გაითვალისწინოს კონკურენციის არსებობა. სახელმწიფო და კერძო IT–ორგანიზაციები მონაწილეობენ კონკურენციაში. სერვისების მიმწოდებლისთვის აუცილებელია ცოდნა, თუ რა მდგომარეობა უჭირავს მას ამ ბაზარზე და მისი სერვისები რითი განსხვავდება კონკურენტების ანალოგიური სერვისებისგან.

სერვისების დაგეგმვა, როგორც სასიცოცხლო ციკლის ეტაპი, საშუალებას აძლევს მიმწოდებელს გაერკვეს შემდეგ საკითხებში:

1. რომელი სერვისების შეთავაზება ღირს ?
2. ვის უნდა შევთავაზოთ სერვისები ?

3. რა სარგებელს (შედეგს) მიიღებენ მომხმარებლები სერვისის გამოყენებით ?

4. რა სარგებელს (შედეგს) მიიღებენ ინვესტორები სერვისის გამოყენებით ?

5. როგორ განვითარდეს შიგა და გარე გასაღების ბაზრები ?

6. როგორ განისაზღვროს სერვისის ხარისხი ?

7. როგორ იღებენ გადაწყვეტილებას დამკვეთები სერვისების მიმწოდებლების ამორჩევისას კონკურენციის პირობებში ?

8. როგორ გაკონტროლდეს სერვისის ფასეულობის შექმნა ფინანსური მართვის ტერმინებში ?

9. როგორ განაწილდეს არსებული რესურსები დასახული მიზნების უფრო ეფექტურად მისაღწევად ?

მომხმარებლები აფასებენ IT–სერვისის გამოყენების შედეგებს ყველაზე ხშირად ეკონომიკური ტერმინებით. IT–ორგანიზაციისთვის აუცილებელია ფიქრი როგორც ინვესტიციებზე სერვისების განვითარების მიზნით, ასევე ბიზნესზე მათი დანერგვის გზით.

სერვისისთვის მნიშვნელოვანია საბაზრო ადეკვატური ფასი, მწარმოებლურობა, სტაბილურობა (დამკვეთი ითვალისწინებს ამათ). სერვის-მენეჯმენტის წარმატება დამოკიდებულია, უპირველეს ყოვლისა, დამკვეთის და მწარმოებლის ურთიერთგაგებაზე. ამიტომაც წარმატების მიღწევის მიზნით (სერვისების აგებისათვის) არის შემოთავაზებული ITIL პუბლიკაციები.

11.2. ფუნქციები და პროცესები სერვისის სასიცოცხლო ციკლში

პუბლიკაციაში "ITILv3. სერვისების სტრატეგიის აგება" განისაზღვრება და ფართოდ გამოიყენება ფუნქციების და პროცესების ცნებები სერვისის სასიცოცხლო ციკლში.

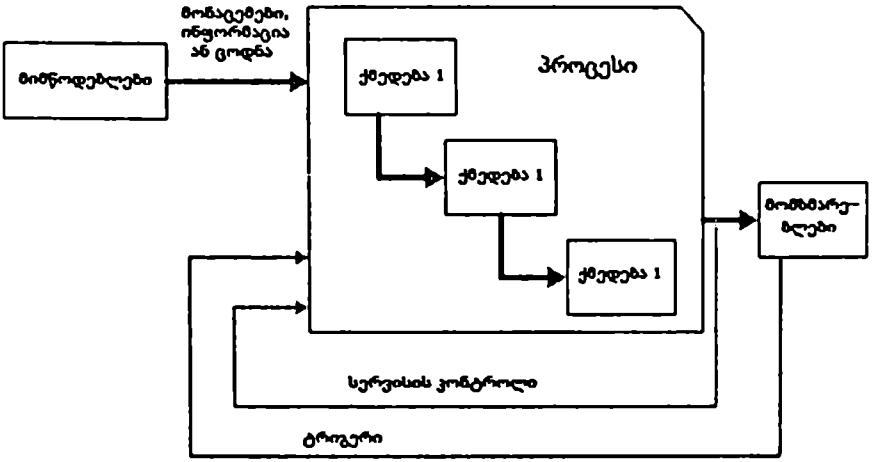
ფუნქციები (Functions) – ორგანიზაციის ნაწილია, სპეციალიზებული იმისთვის, რომ შესრულდეს განსაზღვრული სახის სამუშაოები და პასუხი გაეცეს შესაბამისი შედეგების ფორმირებას. ფუნქციებს აქვს სამუშაოების შესასრულებლად ყველა აუცილებელი შესაძლებლობა და რესურსი. შესაძლებლობები მოიცავს სამუშაოს საკუთარ მეთოდებს და დაგროვებულ გამოცდილებას. ფუნქციები უზრუნველყოფს ორგანიზაციის სტრუქტურირებას და სტაბილურობას [11].

ფუნქციები განსაზღვრავს პასუხისმგებლობას, უფლებებს და როლებს დასმული მიზნების მისაღწევად. ფუნქციათა კოორდინაცია ზოგადი პროცესების საშუალებით არის ნებისმიერი ორგანიზაციის აგების განუყოფელი ნაწილი.

საყურადღებოა, რომ ფუნქციები – ეს არაა ყოველთვის განყოფილებები, ანუ „ერთი ფუნქცია – ერთი განყოფილება" არაა ჭეშმარიტი. მაგალითად, ITILv3–ში გაჩნდა ისეთი ფუნქციები, როგორიცაა Technical Management, Applications Management, რაც მიუთითებს პროფესიულ კომპეტენციაზე (ინჟინრები და ადმინისტრატორები), და არ შეიძლება იყოს განყოფილების დასახელება.

პროცესი – ქმედებათა სახეების სტრუქტურირებული ერთობლიობაა, რომელიც დაპროექტებულია განსაზღვრული მიზნის მისაღწევად. პროცესი შეიძლება შეიცავდეს როლს, პასუხისმგებლობას, ინსტრუმენტებს და კონტროლის მეთოდებს, რომლებიც აუცილებელია შედეგების ფორმირებისთვის. პროცესს

შეუძლია განსაზღვროს პოლიტიკები, სტანდარტები, ხელმძღვანელობა, ქმედებათა სახეები და სამუშაო ინსტრუქციები, როცა ეს აუცილებელია (ნახ.11.1).



ნახ.11.1. საბაზო პროცესის სქემა

პროცესების ძირითადი მახასიათებლებია აქტიურობა, მიმდევრობითობა, ერთი მეორეზე დამოკიდებულება. ტერმინი „ატიურობა“ ფართოდ გამოიყენება ITIL-ში. აქტიურობა – ესაა ქმედებათა ერთობლიობა, დაპროექტებული განსაზღვრული შედეგის მიღების მიზნით.

პროცესებს აქვს შემდეგი მახასიათებლები:

1. პროცესები გაზომვადია, ანუ შესაძლებელია პროცესის გაზომვა (შეფასება) რომელიმე შესატყვისი მეთოდით. მენეჯერები ცდილობენ თავდაპირველად გაზომონ ფასი და ხარისხი, ხოლო პრაქტიკოსი მომხმარებლები – პროცესის ხანგრძლივობა და პროდუქტიულობა;

2. პროცესები ემსახურება კონკრეტული შედეგების მიღწევას. პროცესის არსებობის მიზეზია კონკრეტული შედეგის წარმოდგენა, რომელიც შეიძლება იდენტიფიცირდეს და დაითვალოს;

3. პროცესებს ჰყავს მომხმარებლები – ყოველი პროცესი აწვდის თავის შედეგს მომხმარებელს ან ინვესტორს. ისინი შე ძლება იყოს ორგანიზაციის შიგნით ან გარეთ, ოღონდ პროცესი ყველა შემთხვევაში უნდა აკმაყოფილებდეს მოსალოდნელ შედეგს;

4. პროცესი პასუხს აგებს განსაზღვრულ შედეგზე;

5. პროცესი რეაგირებას უნდა ახდენდეს განსაზღვრულ მოვლენებზე. სანამ მიმდინარეობს პროცესი, იგი კავშირში უნდა იყოს სპეციალურ საინიციალიზაციო ტრიგერთან.

ფუნქციისა და პროცესის ცნებებს ხშირად ურევენ. შეცდომის მიზეზი ხშირად არის აზრი, რომლის თანახმადაც თუ შედეგის დათვლა შეიძლება, მაშინ ის პროცესია.

მაგალითად, არსებობს მცდარი აზრი, რომ დატვირთვის მართვა არის პროცესი ITSM. ჯერ ერთი, დატვირთვის მართვა – ესაა ორგანიზაციის შესაძლებლობა თავისი შიგა პროცესებით და მეთოდებით.

ეს ფუნქცია მთლიანად არის დამოკიდებული კონკრეტული ორგანიზაციის აგებაზე. ანუ შეცდომაა რომ ვთქვათ – დატვირთვის მართვა შეიძლება იყოს მხოლოდ პროცესი. დიახ, შესაძლებელია დატვირთვის გაზომვა და კონტროლი და შესაძლებელია განისაზღვროს, არის ის ადეკვატური თუ არა დასახული მიზნებისთვის, მაგრამ მიუხედავად ამისა, შეცდომაა ჩაითვალოს, რომ თუ შეიძლება გაზომვა, მაშინ ის პროცესია. ფუნქციები სტრუქტურირებას უკეთებს რესურსებს და შესაძლებლობებს პროცესებისთვის. პროცესები კი მიმართავენ ყველაფერ ამას დასმული მიზნის მიღწევისკენ.

11.3. სერვისის ფასეულობაზე გავლენის მომხდენი ფაქტორები

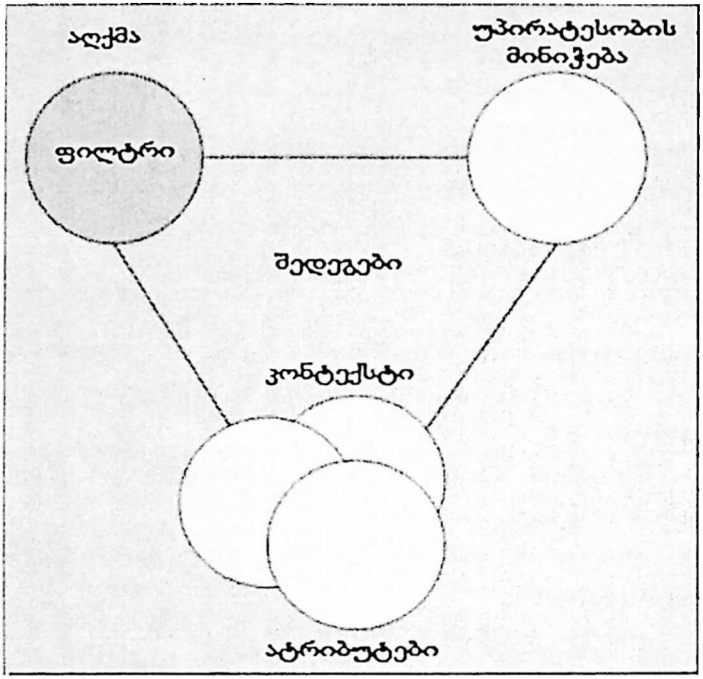
ზოგჯერ სერვისის ფასეულობა შეიძლება გამოიხატოს ეკონომიკური ტერმინებით, ზოგჯერ არა. მიუხედავად ამისა მაინც შესაძლებელია სერვისის მთლიანობაში შეფასება.

სერვისის ფასეულობა განისაზღვრება არა მხოლოდ მომხმარებელთა საბოლოო მიზნების დაკმაყოფილებით. იგი დამოკიდებულია აგრეთვე მომხმარებელთა მიერ სერვისის აღქმაზე, რომელიც, თავის მხრივ, დამოკიდებულია მრავალ ფაქტორზე:

- სერვისის ატრიბუტებზე, რომლებიც ფასეულობის ინდიკატორია დამკვეთისთვის;
- დამკვეთის გამოცდილებაზე ანალოგიური სერვისების გამოყენებისას;
- კონკურენტების დამსახურებაზე და ა.შ.
- დამკვეთის თვითშეფასებისა და მის პოზიციაზე ბაზარზე;

11.2 ნახაზზე ნაჩვენებია განხილული ცნებების ურთიერთდამოკიდებულება.

მომხმარებლები უგულოდ ყიდულობენ საქონელს, რომლის ფასში არსებობს გაურკვევლობა. ამიტომაც, რაც უფრო არაბუნებრივია სერვისის ფასეულობა, მით მეტი მნიშვნელობა აქვს მისი დიფერენციაციის და განსაზღვრის პროცესებს.



ნახ.11.2. სერვისის ფასეულობის ფორმირება

დამკვეთს, თავისი გამოცდილებიდან და სხვა ფაქტორების ცოდნიდან გამომდინარე, გამოუმუშავდება რაღაც ეტალონური ფასის მნიშვნელობა. მიმწოდებლისთვის ამ ეტალონური ფასის ცოდნას დიდი მნიშვნელობა აქვს დამკვეთთან დიალოგის გასამართად, ბაზრის და ანალოგიურ დამკვეთებთან მუშაობის გამოცდილების გასაანალიზებლად.

11.4. სერვისების მიმწოდებელთა ტიპები

სერვისების მიმწოდებლები ორგანიზაციასთან მიმართებით შეიძლება იყოს შიგა ან გარე. ITILv3–ში განიხილება სამი ტიპის მიმწოდებელი:

1. ტიპი 1

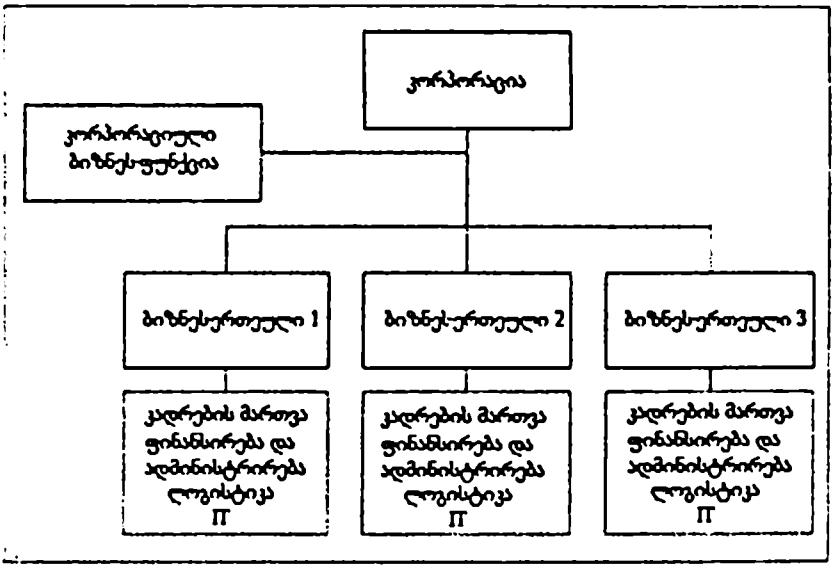
ITILv3-ში ფართოდ გამოიყენება ცნება ბიზნესერთეული (**business unit** ან **BU**). იგი ბიზნესის სეგმენტია, რომელსაც აქვს თავისი საკუთარი მეტრიკები, გეგმები, შემოსავლები და ხარჯები. თითოეული ბიზნესერთეული ფლობს და მართავს აქტივებს, რომლებიც გამოიყენება საქონლის და სერვისების შესაქმნელად განსაზღვრული ფასეულობით.

ბიზნესერთეული არის ორგანიზაციული ერთეული და შეიძლება იყოს კორპორაციის ნაწილი ან სხვა ორგანიზაცია. პირველი ტიპის მიმწოდებლები (ნახ.11.3) მიმაგრებულია იმ ბიზნესერთეულებზე, რომლებსაც ისინი ემსახურებიან, და ფინანსირდებიან მისი ბიუჯეტიდან.

ისინი პირდაპირ ექვემდებარებიან ბიზნესს, ხოლო საკვანძო გადაწყვეტილებებს (სერვისების პორტფელის განსაზღვრა, შედეგების შეფასების კრიტერიუმები, ინვესტიციის მოცულობები) ღებულობენ ორგანიზაციის ტოპ-მენეჯერები.

სერვისების პირველი ტიპის მიმწოდებელთა ძირითადი მიზანია ფუნქციური მთლიანობის და ეფექტიანობის უზრუნველყოფა ბიზნესერთეულისთვის, რომელთანაც ისინი არიან მიმაგრებული. ანუ, ისინი აწვდიან მას IT–სერვისებს ბიზნესის ვიწრო წრის მოთხოვნილებათა დასაკმაყოფილებლად. ამ ტიპის მიმწოდებელთა წარმატება არ იზომება ეკონომიკურ ტერმინებში, ვინაიდან მათი ძირითადი მიზანი არაა მოგების

მიღება, ესაა მხოლოდ აუცილებელი სერვისების მიწოდება კონკრეტული ბიზნესერთეულებისთვის.



ნახ.11.3. სერვისების 1–ელი ტიპის მიმწოდებლები

ამ მოდელს აქვს ღირსებებიც და ნაკლოვანებანიც. ძირითადი ნაკლოვანებაა ის, რომ ფაქტობრივად, სერვისების მიმწოდებლის განვითარება შეზღუდულია ბიზნესერთეულის შესაძლებელი განვითარებით, რომელსაც ის ემსახურება. ის, რომ გადაწყვეტილებას იღებს ორგანიზაციის ხელმძღვანელი, ესეც ერთგვარი ნაკლოვანებაა, რადგან ის მთლიანად ვერ ერკვევა IT–სფეროს ტექნიკურ ნიუანსებში. დადებითი მომენტია ის, რომ ბიზნესი არ ეჯახება პრობლემებს, რომლებიც აღმოცენდება სერვისების გარე მიმწოდებლებთან ურთიერთობისას. ასევე

სერვისების პირველი ტიპის მიმწოდებელი არ ეჯახება თავისუფალი ბაზრის სირთულეებს.

ზოგადად, სერვისების მიმწოდებლები, რომლებიც ემსახურებიან ერთზე მეტ დამკვეთს, ეჯახებიან მრავალგვარ რისკს. მათი ახლო თანამშრომლობა დამკვეთთან რისკების აცილების საწინდარია. ამავდროულად, სერვისების გარე მიმწოდებლებს აქვთ მოქმედების და განვითარების მეტი თავისუფლება, ავტონომიურობა და მასშტაბურობა..

აღნიშნული თავისებურებების გამო, პირველი ტიპის მიმწოდებელი უფრო მიესადაგება ისეთ ბიზნესს, სადაც IT ჩადებულია კონკურენტული უპირატესობის საფუძველში და, აქედან გამომდინარე, მოითხოვს საგულდაგულო კონტროლს უშუალოდ ორგანიზაციის ხელმძღვანელობისგან.

2. ტიპი 2

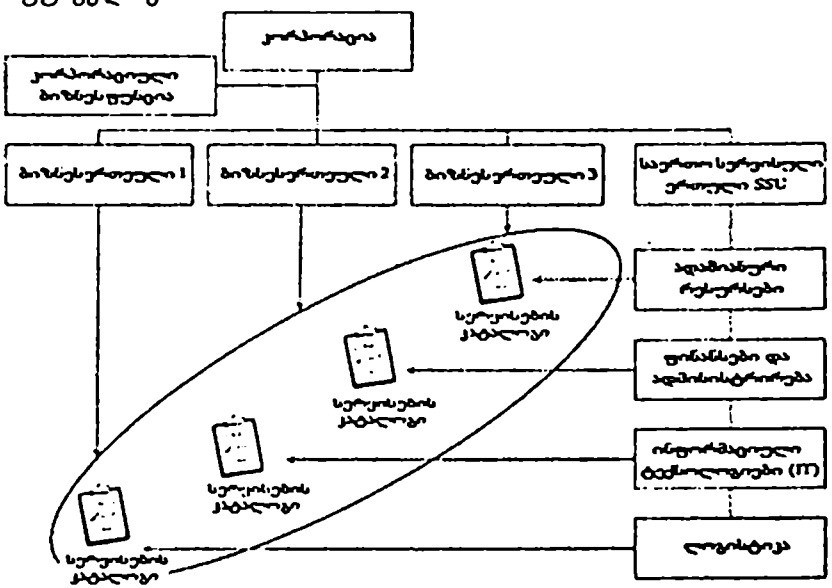
ისეთი საქმიანი ფუნქციები, როგორიცაა ფინანსური მენეჯმენტი, კადრების მართვა და ლოგისტიკა, ყოველთვის არაა კონკურენტული უპირატესობის საფუძველი. აქედან გამომდინარე, ორგანიზაციის ხელმძღვანელის და ტოპ-მენეჯერებისთვის არაა აუცილებელი აკონტროლონ და მართონ ეს სფეროები. ამის ნაცვლად ასეთ ფუნქციათა სერვისები ერთიანდება ცალკე სერვისულ ერთეულში – სერვისების საერთო მიმწოდებელი (Service Shared Unit ან SSU).

SSU (ნახ.11.4), როგორც სერვისების მიმწოდებელი, ფლობს მეტ თავისუფლებას, ვიდრე პირველი ტიპის მიმწოდებელი. მას შეუძლია შექმნას, განავითაროს და მხარი დაუჭიროს თავისი სერვისების გასაღების შიგა ბაზარს, ანალოგიურად თავისუფალ ბაზარზე მომუშავე მიმწოდებლებისა. ამავდროულად, SSU-ს შეუძლია გამოიყენოს კორპორაციის შესაძლებლობები 1-ელი

ტიპის მიმწოდებლების ანალოგიურად. ე.ი. SSU იმყოფება 1 და 3 ტიპის მიმწოდებლების გადაკვეთაზე.

სერვისების მეორე ტიპის მიმწოდებლები ფაქტობრივად, ადუბლირებენ (ემულირება) გარეშე მიმწოდებელთა საქმიანობას, იყენებენ რა მათ მუშა მოდელებს, ბიზნესპრაქტიკას და სტრატეგიებს. აქედან გამომდინარეობს ის, რომ სერვისების გარე მიმწოდებლები მათი ძირითადი კონკურენტები არიან.

SSU სერვისების საბოლოო მომხმარებლები არიან ბიზნეს-ერთეულები, ინვესტორები და მთლიანად კორპორაცია. ამასთანავე, მე–2 ტიპის მიმწოდებლებმა შეიძლება უკეთესი ფასები შესთავაზონ, ვიდრე გარე მიმწოდებლებმა, კორპორაციაში მათი მუშაობის, შიგა ხელშეკრულებების და ბიუჯეტიდან ფინანსირების საფუძველზე.



ნახ.11.4. მეორე ტიპის პროვაიდერის სქემა

მე-2 ტიპის მწარმოებლები, როგორც 1-ელი ტიპისა, ღებულობენ უპირატესობას შედარებით ჩაკეტილი ბაზრიდან. მაგრამ ამავე დროს სერვისების მომხმარებლები ადარებენ მათ გარე მიმწოდებლებს. მეორე ტიპის ცუდი მიმწოდებელი ჩანაცვლდება გარე მიმწოდებლით. ეს აიძულებს ხელმძღვანელობას გამოიყენოს უკეთესი პრაქტიკა, აითვისოს ახალი საბაზრო სივრცეები, განსაზღვროს სტრატეგიები და განავითაროს თავისი სერვისების განსხვავებული მახასიათებლები.

3. ტიპი 3 –სერვისების გარე მიმწოდებლები

სერვისის გარე მიმწოდებლები თავიანთი დამკვეთი ორგანიზაციის გარეთ არსებობენ, განსხვავებით წინა ორი განხილული ტიპისგან. ისინი მოქმედებენ ღია ბაზარზე და აქედან გამომდინარე, ეჯახებიან რიგ სირთულეებს და რისკებს. თუ 1-ელი და მე-2 ტიპის მიმწოდებლებს ყოველთვის ჰყავთ დამკვეთები, მე–3 ტიპისას უხდება მუდმივად მათი ძებნა, ყურადღების მიქცევა, ამიტომაც უნდა იყვნენ კონკურენტუნარიანი. ეს სირთულეები კომპენსირდება მოქნილობით, მასშტაბურობით და ქმედებების და გადაწყვეტილებების თავისუფლებით.

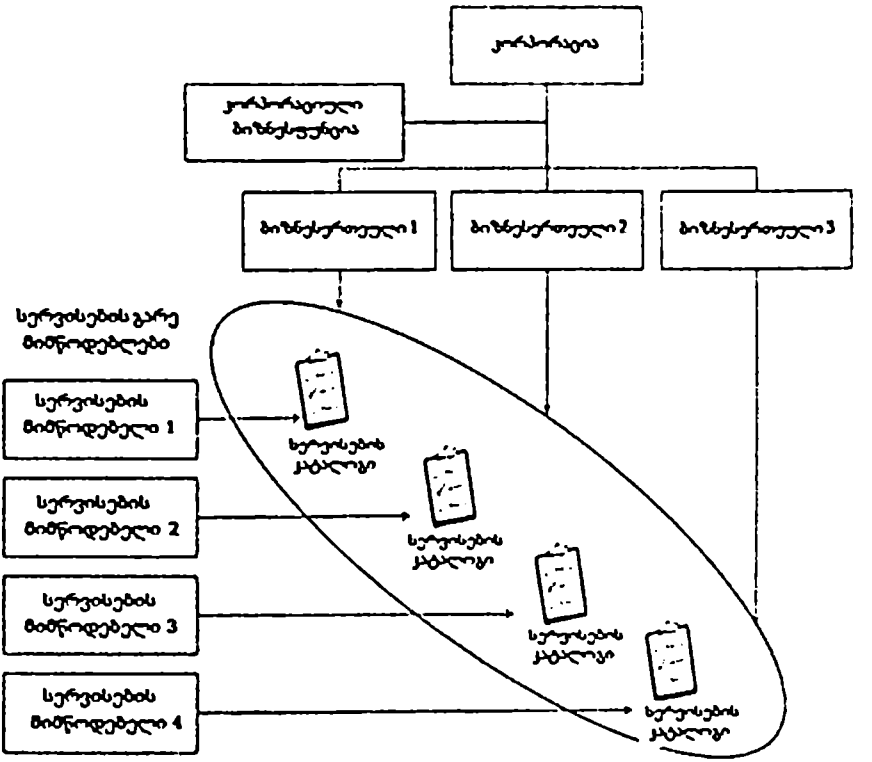
მე-3 ტიპის მიმწოდებლებს გააჩნიათ დიდი პრაქტიკული გამოცდილება, ვინაიდან ისინი ემსახურებიან მრავალი სფეროს სხვადასხვა დამკვეთებს (განსხვავებით 1 და 2 ტიპისა, რომლებიც შეზღუდული გამოცდილებით არიან ერთ კორპორაციაში ან ბაზრის ვიწრო ფრაგმენტზე). IT–სფეროსთვის ძალიან მნიშვნელოვანია, რათა სერვისების მიმწოდებელს ჰქონდეს გამოცდილება IT–სერვისების წარმოდგენისთვის, ამიტომაც ეს კრიტერიუმი ხშირად გადამწყვეტია მიმწოდებლის არჩევისას.

მე-3 ტიპის მიმწოდებლების არჩევის მოტივაციისთვის აგრეთვე გაითვალისწინება გამოცდილება, ცოდნა, რესურსები და

ფართო შესაძლებლობები სერვისების მასშტაბირებისთვის. აღასთანავე, ბიზნესი ყოველთვის მიისწრაფვის ხარჯების შემცირებისკენ, გარე მიმწოდებლებს კი შეუძლიათ კონკურენტუნარიანი ფასების შეთავაზება, ხარჯების შემცირების და მოთხოვნებზე სწრაფი რეაგირების გზით. ამიტომაც, ხშირად ორგანიზაციებისთვის უფრო ხელსაყრელია გარე მიმწოდებლების გამოყენება, ვიდრე შიგა მიმწოდებლების შენახვა და მთელი აქტივების მართვა, რაც სერვისის დამოუკიდებელი რეალიზაციისთვისაა საჭირო.

შეიძლება ითქვას, რომ მე-3 ტიპის პროვაიდერები იმყოფებიან საერთო სერვისული მოდელის მართვის გავლენის ქვეშ (ნახ.11.5). ეს გამოიხატება იმით, რომ მათი რესურსები და შესაძლებლობები განაწილებულია კლიენტებს შორის, რომელთა შორის ზოგი მათივე კონკურენტია. აქედან გამომდინარე, კონკურენტები იღებენ ერთმანეთის ფასებზე წვდომის უფლებას, და ამცირებენ მათ მნიშვნელობებს. ასეთ დროს მნიშვნელოვანია უსაფრთხოების უზრუნველყოფა, ეს განსაკუთრებული ასპექტია IT–სერვისის გამოყენებისას, ხოლო როდესაც გარემო არის საერთო კონკურენტებისთვის, მაშინ ის იღებს განსაკუთრებულ მნიშვნელობას.

ყოველ მიმწოდებელს აქვს ღირსებები და ნაკლოვანებებიც. დამკვეთის მიერ მიმწოდებლის ამორჩევა დამოკიდებულია მრავალ ფაქტორზე: საოპერაციო ხარჯებზე, ინდუსტრიის თავისებურებებზე, მის კომპეტენციებზე და რისკებზე. ორივე მხარისთვის სასარგებლოა საოპერაციო ხარჯების წარმოშობის პროცესის გაგება: დამკვეთს – რათა აირჩიოს მიმწოდებელი, ხოლო მიმწოდებელს – იმის გასაგებად, თუ როგორ შეარჩიოს დამკვეთი. ოპერაციული ხარჯები – ესაა ყველა ხარჯი, რასაც გაიღებს ბიზნესი სერვისების მიმწოდებელთან მუშაობისას.



ნახ.11.5. სერვისების მესამე ტიპის მიმწოდებლები

გარდა თვით სერვისების ღირებულებისა, ესაა ხარჯები კვალიფიციური მიმწოდებლის მოსაძებნად, მოთხოვნების განსაზღვრის მიზნით სერვისების პორტფელისთვის, მოლაპარაკებების წარმართვაზე, მწარმოებლურობის შეფასებაზე, დავების გადაწყვეტაზე, ცვლილებების შეტანისა და სრულყოფის მიზნით.

ენდობა თუ არა დამკვეთი გარე ან შიგა მიმწოდებლების განსაზღვრულ საქმიან აქტივობას, დამოკიდებულია შემდეგი კითხვების პასუხებზე:

1. სჭირდება თუ არა საქმიან აქტიურობას სპეციფიკური აქტივები ?
2. რამდენად ხშირად გამოიყენება საქმიანი აქტიურობა ბიზნესციკლში ?
3. რამდენად რთულია საქმიანი აქტიურობა ?
4. რთულია მაღალი დონის მწარმოებლურობის განსაზღვრა ?
5. რთულია მწარმოებლურობის დონის განსაზღვრა ?
6. რამდენად მჭიდროდაა იგი დაკავშირებული ბიზნესის სხვა აქტიურობებთან და აქტივებთან ? მისი გამოყოფა გამოიწვევს პრობლემებს და გაზრდის ბიზნესპროცესების სირთულეს ?

მაგალითად, თუ აქტიურობა გამოიყენება იშვიათად ან ერთეულ შემთხვევაში, მაშინ ის უკეთესია მიეცეს გარე მიმწოდებელს; თუ ის მარტივი, რუტინულია და არ იცვლება დროში ანუ სტაბილურია – ესეც გარე მიმწოდებელს.

თუ საქმიანი აქტიურობის მწარმოებლურობა რთული გასაზომი, შესაფასებელი და გასაკონტროლებელია, მაშინ ის უკეთესია მიეცეს შიგა მიმწოდებელს. თუ აქტიურობა მჭიდრო კავშირშია ბიზნესთან, ხოლო მისი გამოყოფა გამოიწვევს სირთულეებს, მაშინ უკეთესია მისი დატოვება ორგანიზაციის შიგნით.

უნდა აღინიშნოს, რომ პასუხები დასმულ შეკითხვებზე შეიძლება შეიცვალოს დროის მიხედვით, მდგომარეობების შეცვლის, ახალი ტექნოლოგიების ან მოთხოვნების გაჩენის გამო.

11.5. დაგეგმვის ფუნდამენტური საფუძვლები

„სტრატეგიაში ყველაფერი ადვილია, მაგრამ ეს არ ნიშნავს, რომ ყველაფერი მარტივია".

ადამიანები, რომლებიც პასუხისმგებლები არიან გადაწყვეტილების მიღებაზე, ხშირად ხელმძღვანელობენ გონივრული (კონცეპტუალური) მოდელებით და სჯერათ, რომ ისინი მიიყვანს მათ სასურველ შედეგებამდე. პრობლემები აღმოცენდება მაშინ, როცა არასწორი მოდელის გამოყენებას ცდილობენ პრაქტიკული ამოცანის გადაჭრისას და არ ესმით ამავდროულად სისტემის ან პროცესის თავისებურებანი. სამუშაოს თეორიული ცოდნის და ფუნდამენტური პრინციპების გარეშე შეუძლებელია იმის გაგება, თუ რატომ არ მოერგო თითქოს იდეალური გადაწყვეტა კონკრეტული პრობლემის გადაჭრას.

სერვისის სტრატეგიის დამუშავება, უპირველეს ყოვლისა, მიმართულია ამ სერვისის ფასეულობის სრულყოფაზე. როგორც ზემოთ აღინიშნა, სწორედ სტრატეგია განსაზღვრავს სერვისების მიმწოდებლის უნიკალურობას. ის სჭირდება არა მხოლოდ ცალკე მიმწოდებლებს, რომლებიც ცალკე კომერციული ორგანიზაციაა. იმისათვის, რომ საჭირო იყოს თავის კორპორაციაში, სერვისის შიგა მიმწოდებლებსაც სჭირდებათ პოზიციირება და მკაფიო გეგმების აგება.

დამკვეთები მუდმივად ცდილობენ თავიანთი ბიზნესის მოდელის და სტრატეგიის სრულყოფას. ისინი ეძებენ გადაწყვეტებს, რომლებიც მისცემს უფრო მაღალ მწარმოებლურობას და ეფექტურობას. მაგრამ ამავდროულად უნდათ რომ ხარჯები გაიზარდოს მცირედით ან არ გაიზარდოს საერთოდ. ასეთი გადაწყვეტა ხშირად არის ინოვაციური პროდუქტები ან სერვისები.

სერვისების მიმწოდებლის პოზიცია დამკვეთის ბიზნესში და მისი შეფასება შეიძლება იცვლებოდეს დროში მრავალი გარემოების, პირობის და ფაქტორის გამო, რომლებიც არ ექვემდებარება სერვისების მიმწოდებლის კონტროლს. სტრატეგიული შეხედულება სერვისების მართვის პროცესზე მოითხოვს დამკვეთთან ურთიერთობაში აკურატულ მიდგომას.

პირველი, რაც სერვისების მიმწოდებელმა უნდა გაითვალისწინოს სტრატეგიის შემუშავებისას არის ის, რომ მას ჰყავს კონკურენტები. მაშინაც კი, თუ სერვისის ფასეულობა, რომელსაც იგი სთავაზობს, ძნელად გასაზომი ან შესაფასებელია, ის მაინც უნდა იყოს უკეთესი დამკვეთისთვის სხვა ალტერნატივებთან შედარებით.

მეორე – აუცილებელია მკაფიოდ განისაზღვროს წარმოდგენილი სერვისის ფასეულობა. ფასეულობა, არის ის, რაც მიმწოდებელს ხდის უნიკალურს დამკვეთისთვის. ის შეიძლება იყოს მატერიალური (მოგების გაზრდა ან ხარჯის შემცირება) და სოციალური (სიცოცხლის გადარჩენა ან გადასახადის შეკრება).

მესამე – როცა მენეჯერები ლაპარაკობენ სტრატეგიის შემუშავებაზე, ყველაზე ხშირად გულისხმობენ დროის ხანგრძლივ ინტერვალს, რომლის განმავლობაშიც ორგანიზაცია გადავა ერთი მდგომარეობიდან მეორეში. IT–სერვისების მართვის სფეროში ყველაფერი შედარებით სხვაგვარადაა.

პირველი პრობლემა ისაა, რომ გარემოს პირობები სწრაფად იცვლება. ბიზნესის ცვლილების ტემპი ჩქარდება, დამოუკიდებლად ორგანიზაციის ზომებისა და მოღვაწეობის სფეროსი. ერთი შესაძლებლობები აღმოცენდება, მეორე – იკარგება. სამყარო არ ელოდება, ვინმე შეასრულებს თუ არა გეგმას, და ის, რაც დღეს იყო კარგი, ხვალ შეიძლება გახდეს აბსოლუტურად უვარგისი. ამიტომ სტრატეგიის აგებისას სერვისების

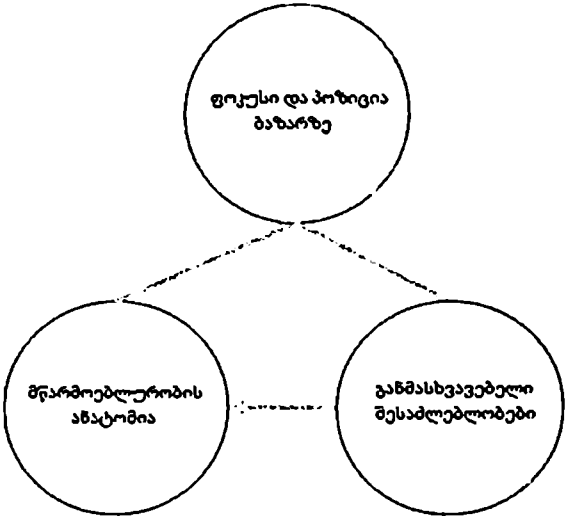
მიმწოდებლისთვის სასიცოცხლოდ აუცილებელია შეინარჩუნოს მოქნილობა, განავითაროს ინოვაციური გადაწყვეტები და სწრაფად იმოქმედოს ცვლად პირობებზე.

მეორე პრობლემა მდგომარეობს სერვისის ფასეულობის განსაზღვრაში. მაშინ, როცა სტრატეგია არის რთული, მის საფუძველში ჩადებული პრინციპები მარტივია. ფაქტობრივად არსებობს ორი გზა, რომელთა დახმარებითაც ერთი მიმწოდებელი შეიძლება გახდეს მეორეზე უკეთესი – ან აიძულოს დამკვეთი სერვისებისთვის გადაიხადოს მეტი ან უნდა შეამციროს სერვისების ღირებულება.

აქედან ისმის ორი კითხვა – რა განაპირობებს მოტივაციას, რომ დამკვეთმა გადაიხადოს მეტი, ან როგორ მოხდეს ნაკლები რესურსების გამოყენება და ამით შემცირდეს ხარჯები ? მიმწოდებელს შეუძლია სერვისის ფასეულობის შექმნა განსხვავებული მახასიათებლების წყალობით, მაგრამ შეიძლება უუნარო იყოს შეინარჩუნოს მათი უნიკალურობა დროთა განმავლობაში. უფრო მეტიც, ფასეულობათა განსაზღვრის პირობები იცვლება. მოვიტანოთ მაგალითი "ITILv3.Service Strategy" წიგნიდან.

სერვისების მიმწოდებლებს გადააქვთ თავიანთი წარმოება სხვა ქვეყნებში, მაგალითად, ნაკლები გადასახადების მქონეში. პირველმა, ვინც ეს სქემა გამოიყენა, მიიღო უპირატესობა თავიანთ კონკურენტებთან შედარებით, რადგან ხარჯების შემცირების ანგარიშზე შეამცირეს სერვისების ფასები. მაგრამ, როცა მიმწოდებლების უმრავლესობა მუშაობს ამ სქემით, მაშინ სერვისები ყველასთან გაიაფდა. ეს ხელსაყრელია მომხმარებლისთვის, მაგრამ ცუდად აისახა სერვისების მიმწოდებლებზე – დაიკარგა განმასხვავებელი თვისებები. ანუ ფასეულობა შეიქმნა, მაგრამ სერვისების მწარმოებლებმა ის ვერ შეინარჩუნეს.

კონკურენტული უპირატესობის მიღწევა თითქმის ყველა შემთხვევაში ეფუძნება სამი საბაზო მდგენელის ბალანსს, რეგულირებას და განახლებას: ბაზარზე ფოკუსი და პოზიცია, განმასხვავებელი (განსაკუთრებული) შესაძლებლობები, მწარმოებლურობის ანატომია (ნახ.11.6).



ნახ.11.6. კონკურენტული უპირატესობის მიღწევა

ბაზარზე ფოკუსი და პოზიცია – ესაა სერვისების მწარმოებლის მიერ ბაზარზე თავისი პოზიციის წარმოდგენა. გასაღების ბაზარი განისაზღვრება შედეგებით, რომელთა მიღებაც უნდათ მიმწოდებლებს ერთი ან რამდენიმე სერვისით. ამ კატეგორიაში შედის სერვისების პორტფელის აგება და მართვა, ოპტიმალური მასშტაბის არჩევა, ალტერნატიული ბაზრების / ახალი დამკვეთების იდენტიფიკაცია და ჩართვა სტრატეგიაში.

სერვისების ყველა ტიპის მიმწოდებლებისთვის მეტად მნიშვნელოვანია გასაღების ბაზრის განსაზღვრა, მისი დინამიკის და თავისი საბოლოო მომხმარებლის მიზნების გაგება. პირველი და მეორე ტიპის მიმწოდებლებს სტრატეგიის აგების ეს ასპექტი ადვილად გამოსდით, რადგან მათ წინასწარ იციან თავიანთი მომხმარებელი და გასაღების ბაზარი. ეს კი გარკვეული საწყისი უპირატესობაა.

განმასხვავებელი შესაძლებლობები – შესაძლებლობათა ერთობლიობის შექმნის და გამოყენების პროცესების წარმოდგენა, რომლებიც უნიკალური და განუმეორებელია ამ მიმწოდებლისთვის. ასეთი შესაძლებლობების საშუალებით სერვისების მიმწოდებელი წარუდგენს დამკვეთს ფასეულობას. სტრატეგიის აგების ეს ნაწილი ასახავს რესურსების, შესაძლებლობების და ფასეულობის შექმნის პროცესის ურთიერთქმედებას. რაც მეტი განმასხვავებელი შესაძლებლობა აქვს სერვისების მიმწოდებელს, მით მეტია შანსი დამკვეთის დათანხმებისა. განმასხვავებელი შესაძლებლობები ძევს კონკურენტული უპირატესობის მოპოვების საფუძველში.

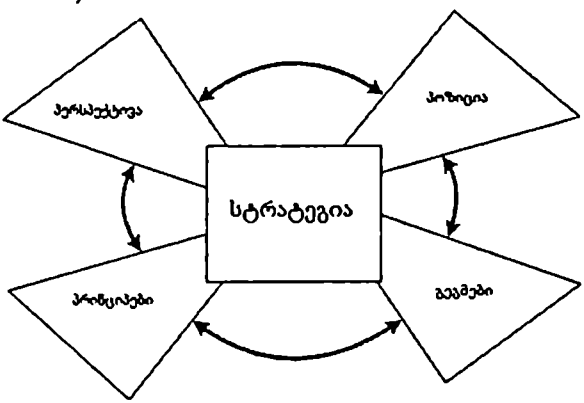
სერვისების მიმწოდებლებმა მკაფიოდ უნდა იცოდნენ, თუ რომელ განმასხვავებელ შესაძლებლობებს შეაქვს დიდი წვლილი დამკვეთის მიერ სასურველი შედეგების მიღწევის პროცესში. უფრო მეტიც, მან უნდა განავითაროს ეს განმასხვავებელი შესაძლებლობები და თვალყური ადევნოს იმას, რომ ისინი იყოს გასაგები და თვალსაჩინო დამკვეთისთვის.

მწარმოებლურობის ანატომია – ესაა ორგანიზაციული და ქცევითი თავისებურებების შექმნის პროცესის წარმოდგენა, რომელთა დახმარებითაც სერვისების მიმწოდებელი მოძრაობს დასახული მიზნისკენ კონკურენციის პირობებში.

მწარმოებლურობის ანატომია შეიცავს თავის თავში მსოფლიოში დადგენილ ორგანიზაციულ შეხედულებებს, რომლებიც კონკრეტული ორგანიზაციის ხელმძღვანელობას შეუძლია გამოიყენოს პრაქტიკაში. მაგალითად, „სერვისები არის სტრატეგიული აკტივები“ ან „სერვისების უწყვეტი სრულყოფა და განახლება არის რეალური და მუდმივი აუცილებლობა“.

11.6. ოთხი „P“ სტრატეგიის ასაგებად

წიგნში "ITILv3.Service Strategy" აღიწერება სტრატეგიის აგების ოთხი შესასვლელი წერტილი, ე.წ. „Four Ps of Strategy“ – Perspective (პერსპექტივა), Positions (პოზიცია), Plans (გეგმები) и Patterns (პრინციპები). სწორედ ეს განსაზღვრავს სტრატეგიის ფორმას (ნახ.11.7).



ნახ.11.7. სტრატეგიის ოთხი "P"

პერსპექტივა – განსაზღვრავს სერვისების მიმწოდებლის განვითარების მიმართულებას, მის ფასეულობებს და საერთო მიზანს. სტრატეგიული პერსპექტივა აფორმირებს ურთიერთობის

ფილოსოფიას დამკვეთთან და სერვისების წარმოდგენის მეთოდებს. მაგალითად, სერვისების მეორე ტიპის მიმწოდებელს საერთაშორისო იურიდიული კომპანიისთვის შეუძლია მისი ფორმირება ეს შემდეგნაირად: „ჩვენ ვიქნებით საუკეთესო პროვაიდერი ჩვენ კლასში ჩვენი იურიდიული ფირმისთვის".

სერვისების მესამე ტიპის მიმწოდებლისთვის შესაფერისი იქნება „ფოკუსირება მომხმარებელზე, ხოლო სხვა დანარჩენი დაერთვება მას" ან „ჩვენი მიზანია მომხმარებელთა ცხოვრების გაუმჯობესება". პერსპექტივა, განსხვავებით გეგმებისა და პოზიციებისგან, შედარებით მუდმივი და მდგრადია ცვლილებებისადმი.

წიგნში "ITILv3.Service Strategy" მოყვანილია მაგალითი შვეიცარული საათების ინდუსტრიაზე. XX საუკუნის 70-იანი წლების დასაწყისში დაიწყეს საათებში კვარცის გამოყენება რხევითი სისტემის საშუალებად. ამან გამოიწვია წარმოების 10–ჯერ გაიაფება, ხარისხის შენარჩუნებით მაღალ დონეზე. მიუხედავად ამისა, შვეიცარელმა მწარმოებლებმა გაითვალეს, რომ ამ ტექნოლოგიის გამოყენება ეწინააღმდეგება საათების წარმოების პროფესიულ ოსტატობას. იაპონელი მწარმოებლები კი პირიქით, აქტიურად იყენებდნენ კვარცს და აგდებდნენ ბაზრიდან შვეიცარულ საათებს. ეს ხდებოდა მანამდე, სანამ შვეიცარელებმა არ შეცვალეს თავიანთი მარკეტინგული კამპანია, გააკეთეს პერეორიენტაცია მდიდარ კლიენტებზე, ე.წ. luxury – ბაზრის სეგმენტი. დღეისათვის შვეიცარული საათები თავისებური ნიმუშია ხარისხის, სტილის და თავისი მფლობელის სიმდიდრის მოწმეა.

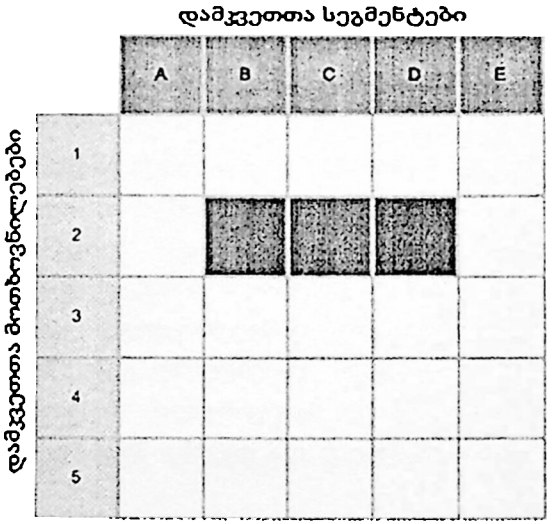
პოზიცია. პოზიცირება გულისხმობს პასუხების გაცემას რიგ შეკითხვებზე, მაგალითად:

– უნდა ამაღლდეს სერვისების ფასები ან შემცირდეს ხარჯები ?

– უნდა გამახვილდეს ყურადღება ხარისხის გარანტიაზე თუ სარგებლიანობაზე ?

პირველი ტიპის პროვაიდერს შეუძლია პოზიციის აგება ლოზუნგით: „ვიცი, რაც უნდა ვაწარმოო“ ან „ვგრძნობ მომხმარებელს“. პოზიცირება ხშირად ეფუძნება ბიზნესის მიმდინარე მოთხოვნებს და გამოისახება იმით, თუ რითი განსხვავდება ეს მიმწოდებელი სხვებისგან მომხმარებლის თვალსაზრისით. გამოყოფენ სამი ტიპის ყველაზე მეტად გავრცელებულ პოზიციას:

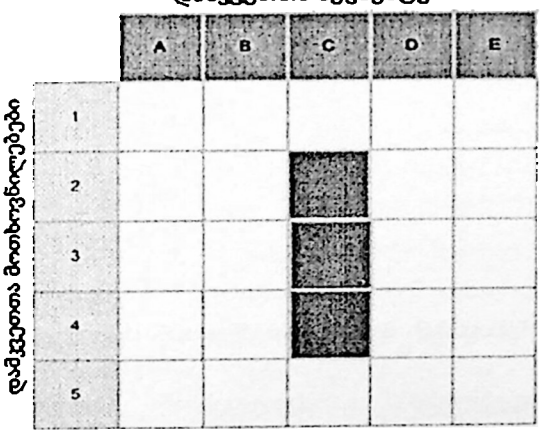
• პოზიცირება სერვისების სახის საფუძველზე (variety-based positioning) გულისხმობს, რომ მიმწოდებელი სპეციალიზდება დამკვეთების მოთხოვნილებათა განსაზღვრულ სახეზე (ნახ.11.8).



ნახ.11.8. პოზიცირება სერვისების სახის საფუძველზე

ეს მიდგომა გულისხმობს სერვისების სპექტრის შემცირებას, მაგრამ მათი შესაძლებლობების გაზრდას კონკრეტული ახის მოთხოვნილებების მაქსიმალური დაკმაყოფილებისათვის. განვითარება შესაძლებელია უპირატესად ახალი შესაძლებლობებით სერვისების არსებულ კატალოგში და არა ახალი სერვისების შემოტანით. ანუ სერვისების მიმწოდებელს შეუძლია თავიდან მოემსახუროს ერთ ბიზნესერთეულს, შემდეგ – რამდენიმე ბიზნესერთეულს კომპანიის ჩარჩოში ან რამდენიმე კომპანიას რეგიონის ჩარჩოში.

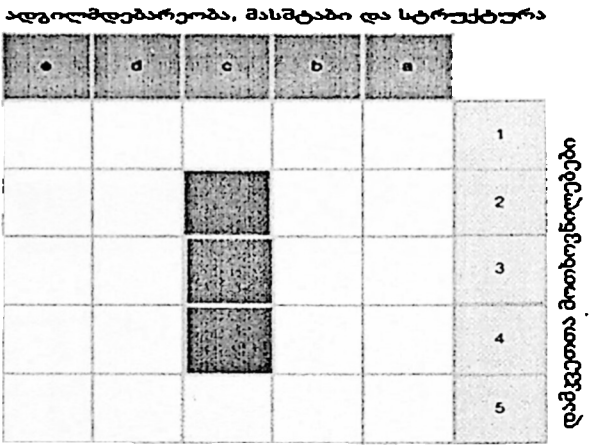
- პოზიცირება მოთხოვნილებათა საფუძველზე (needs-based positioning) გულისხმობს, რომ სერვისების მიმწოდებელი ცდილობს დააკმაყოფილოს განსაზღვრული ტიპის დამკვეთის ყველა ან თითქმის ყველა მოთხოვნილება (ნახ.11.9).



ნახ.11.9. პოზიცირება მოთხოვნილებათა საფუძველზე

ეს მოითხოვს სერვისების კატალოგის გაფართოებას, რადგან მიმწოდებელმა უნდა დააკმაყოფილოს სხვადასხვა სახის მოთხოვნილებები. განვითარება შესაძლებელია უპირატესად ახალი სერვისების დამატებით კატალოგში.

• პოზიცირება წვდომის საფუძველზე (access-based positioning) გულისხმობს, რომ სერვისების მიმწოდებელი თავის განსაკუთრებულ თავისებურებად სთავაზობს მზადყოფნას სერვისების მისაწოდებლად დამკვეთის ადგილმდებარეობის, მასშტაბის და სტრუქტურის გათვალისწინებით.



ნახ.11.**10.** პოზიცირება წვდომის საფუძველზე

მიმწოდებლები განსხვავდებიან სამუშაოს ზომით, სტრუქტურით და საზღვრებით. ზოგიერთი კორპორაციის თანამშრომლები მობილურები არიან, მაგრამ მიუხედავად ამისა, უნდათ წვდომის მიღება ყველა კომუნიკაციასთან. სხვა ორგანიზაციის თანამშრომლები მუშაობენ სტაციონარში, მაგრამ პლანეტის შორეულ კუთხეებში. პოზიცირების ეს სახე

გულისხმობს ბიზნესის მოთხოვნების დაკმაყოფილებას, ყველა თანმხლები თავისებურებების გათვალისწინებით. ამ შემთხვევაში ბუნებრივია ვიწრო სპეციალიზაცია. მოცემული ფირმის სტრატეგია ძალზე საშიშია, რადგან იგი ძალზე დაუცველია: მოულოდნელი ცვლილება ბიზნესში ან ბაზრის სეგმენტზე იწვევს მოთხოვნილების მკვეთრ დაქვეითებას და, შესაბამისად, სერვისების მიმწოდებლის კრახს.

გეგმა – აღწერს გადაწყვეტილებათა და ქმედებათა მიმდევრობას საწყისი მდგომარეობიდან სტრატეგიულ მიზნობრივში გადასასვლელად. განსაკუთრებით განიხილება ბიუჯეტის, სერვისების პორტფელის, ახალი სერვისების განვითარების, ინვესტიციების და სრულყოფის საკითხები. გეგმა შეიძლება დეტალიზებულ იქნას, მაგალითად, „როგორ შეგვიძლია ფასიანი ან იაფი სერვისების მიწოდება“.

პრინციპი – აღწერს ორგანიზაციის ფუნდამენტურ გზას. პრინციპი ამ შემთხვევაში არის ქმედებების და გადაწყვეტილებების მიმდევრობა, რომლებიც დროში შედარებით მუდმივია. პრინციპები ფორმირდება საუკეთესო შედეგების საფუძველზე, თუ რამემ როდისმე მოიტანა წარმატება, ის შეიძლება კიდევ იყოს გამოყენებული განმეორებით. სერვისების მიმწოდებელი, რომელიც იძლევა სპეციალიზებულ სერვისებს, მოითხოვს მაღალ კვალიფიკაციას, იყენებს ე.წ. „მაღალი კლასის“ სტრატეგიას. ის, ვინც იძლევა საიმედო სერვისებს, იყენებს „ხარისხის მაღალი გარანტიის“ სტრატეგიას.

მოთხოვნები და პირობები დინამიკურია, ამიტომ სერვისების მიმწოდებელს შეუძლია დაიწყოს ერთი ფორმის სტრატეგიით, და დაამთავროს სხვა სტრატეგიით. მაგალითად, მიმწოდებელმა შეიძლება დაიწყოს პერსპექტივის აგებით, ანუ ორგანიზაციის მიზნის და მიმართულების განსაზღვრით. შემდეგ

მას შეუძლია პოზიცირების გამოყენების გადაწყვეტა, დაფუძნებული ორგანიზაციის შესაძლებლობებზე, რესურსებსა და პოლიტიკაზე. ეს შეიძლება მიღწეულ იქნას გულდასმით მოფიქრებული გეგმით. მიაღწევს რა ერთხელ სასურველ შედეგებს, სერვისების მიმწოდებელს შეუძლია მართოს თავისი პოზიცია კარგად გაგებული გადაწყვეტებით და ქმედებებით – პრინციპებით.

12. სერვისის მახასიათებლები

12.1. სერვისის შესაძლებლობების და ფასეულობის განსაზღვრა

ორგანიზაციები ცდილობენ ბიზნესის მოთხოვნების დაკმაყოფილებას, მათ ხელში არსებული აქტივების გამოყენებით. აქტივები შეიძლება ეკუთვნოდეს ბიზნესს ან იყოს მისაწვდომი სხვადასხვა საფინანსო შეთანხმებების შედეგად. ამ მიზნის მისაღწევად მენეჯერები ცდილობენ გამოიყენონ აქტივებში ჩადებული სრული პოტენციალი. ამავდროულად, ბიზნესის გარშემო არსებობს მრავალი შეზღუდვის ფაქტორი, რომლებიც ამცირებს აქტივების გამოყენების შედეგიანობას და, შესაბამისად, მთელი ორგანიზაციის შემოქმედებას. შეზღუდვის მთავარი ფაქტორებია რისკები და ხარჯები, რომლებიც წარმოიქმნება ბიზნესგარემოში არსებული სირთულეების, წინააღმდეგობების და გაურკვევლობების გამო.

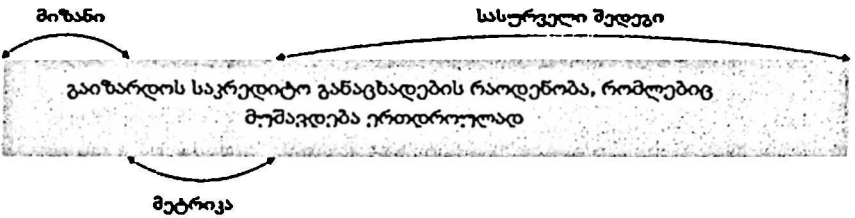
მენეჯერების ერთ-ერთი ძირითადი ამოცანაა ყველაზე მართებული საშუალებების შერჩევა დასახული მიზნების მისაღწევად. სერვისები არის სწორედ ის საშუალებები, რომლებიც შეიძლება გამოიყენონ მენეჯერებმა ბიზნესის აქტივების მწარმოებლურობის ასამაღლებლად. აქედან გამომდინარეობს, რომ

სერვისის ფასეულობა ყველაზე კარგია გაიზომოს დამკვეთის საბოლოო შედეგების გაუმჯობესებით, რაც გამოიწვია აქტივების მწარმოებლურობის გაზრდამ ამ სერვისის გამოყენებით. მნიშვნელოვანია იმის გაგება, რომ ყველა სერვისი არაა გამიზნული აქტივების მწარმოებლურობის ამაღლებისთვის, თუმცა ეს არის სერვისების ყველაზე მაღალი კლასი. ზოგიერთი სერვისი დანიშნულია არსებული მწარმოებლურობის დონის შესანარჩუნებლად, ზოგიც – მწარმოებლურობის აღსადგენად სხვადასხვა არასასურველი მოვლენების შემდეგ, მაგალითად, დაზიანების შემდეგ.

საერთოდ შეიძლება ითქვას, რომ სერვისების გამოყენების ძირითადი ასპექტი არის – თავიდან იქნას აცილებული ან შესუსტდეს დამკვეთის აქტივების მწარმოებლურობის მერყეობა. დამკვეთის აქტივების მწარმოებლურობა უნდა იყოს სერვის-მენეჯმენტის ძირითადი საკითხი, რადგანაც დამკვეთის აქტივების გარეშე არ არსებობს საფუძველი სერვისების ფასეულობის დასადგენად.

სერვსების დამკვეთები თავიანთი მხრიდან ცდილობენ წარმოადგინონ გარკვეული ფასეულობა თავისი კლიენტებისთვის. ბიზნესის აქტივები არის მათთვის ფასეულობის უზრუნველყოფის და მისი გაზრდის საშუალება. მაგალითად, ფასეულობა ბანკისა, რომელიც იძლევა ფულს კრედიტით, იქმნება კრედიტისთვის განაცხადების ოპერატიული დამუშავებით (ნახ.12.1).

შედეგად ბანკის კლიენტები იღებენ წვდომას საჭირო საფინანსო საშუალებებთან, ხოლო ბანკი იღებს სარგებელს კრედიტის პროცენტის სახით. საკრედიტო პროცესი არის ბიზნესის აქტივი, რომლის მწარმოებლურობა განსაზღვრავს ბიზნეს-მოღვაწეობის შედეგებს.



ნახ.12.1. გამოსასვლელზე შედეგების ანალიზის მაგალითი

სერვისების მიმწოდებლისთვის ძალზე მნიშვნელოვანია ბიზნესის გაგება, რომელსაც ის ემსახურება. ეს მოიცავს თავის თავში ბიზნესის აქტივების იდენტიფიკაციას და შედეგებს, რომლისკენაც ის ისწრაფვის.

მიმწოდებელი უნდა ეძებდეს შესაძლებლობებს თავისი სერვისების დასანერგად, ვინაიდან ზოგიერთი ბიზნესპროცესი ცუდად ერგება სერვისების დანერგვას მწარმოებლურობის ამაღლების მიზნით. სხვა პროცესების მხარდაჭერა შეიძლება მხოლოდ იმ სერვისებით, რომლებიც იმყოფება პროექტირების და დაგეგმვის ეტაპებზე.

სერვისების მიმწოდებლისთვის ყველაზე მეტი შესაძლებლობა იმალება ბიზნესპროცესებში, რომელთა მწარმოებლურობა იყო მაღალი, მაგრამ დაეცა არასასურველი მოვლენების გამო ან ბიზნესგარემოს ცვლილებებით.

სერვისის ფასეულობის განსაზღვრა მარტივდება, როდესაც ჩნდება ბიზნესპროცესების გამოსასვლელების ვიზუალიზირების შესაძლებლობა, რომელთათვისაც დანიშნულია სერვისი.

დამკვეთის შედეგების ასახვა სერვისებზე სრულდება კონფიგურაციების მართვის სისტემების (Configuration Management System ან CMS) ჩარჩოში. ესაა ინსტრუმენტების და მონაცემთა ბაზების ერთობლიობა, რომლებიც გამოიყენება სერვისების

მიმწოდებლის მიერ კონფიგურაციის მონაცემთა სამართავად. CMS ასევე შეიცავს ინფორმაციას ინციდენტების, პრობლემების, ცნობილი შეცდომების, ცვლილებების და ვერსიების შესახებ.

იგი შეიძლება შეიცავდეს, აგრეთვე, მონაცემებს თანამშრომლების, მიმწოდებლების, ადგილმდებარეობების, ბიზნესერთეულების, დამკვეთების და მომხმარებლების შესახებ. CMS-ს აქვს ინფორმაციის შეკრების, შენახვის, მართვის, განახლებისა და წარმოდგენის ინსტრუმენტები ყველა საკონფიგურაციო ერთეულისთვის და მათი ურთიერთ-დამოკიდებულების შესახებ.

CMS იმყოფება კონფიგურაციების მართვის პროცესის მმართველობის ქვეშ და გამოიყენება IT-სერვისების მართვის ყველა პროცესის მიერ.

წიგნში "ITILv3.Service Strategy" გამოყოფილია ორი საკვანძო როლი – საქმიან დამოკიდებულებათა მენეჯერები და პროდუქტების მენეჯერები.

დამკვეთებთან მტკიცე ურთიერთობების დამყარება ეხება საქმიან დამოკიდებულებათა მენეჯერებს (Business Relationship Managers ან BRM). მათი ამოცანაა დამკვეთზე ფოკუსირება, მისი ბიზნესპროცესების და შედეგების განსაზღვრა. ბევრ ორგანიზაციაში BRM ცნობილია როგორც სარეკლამო აგენტები, წარმომადგენლები ან გაყიდვების მენეჯერები.

BRM მჭიდროდ თანამშრომლობს პროდუქტების მენეჯერთან (Product Managers), რომლებიც პასუხისმგებლები არიან სერვისების განვითარებასა და მართვაზე სასიცოცხლო ციკლის ყველა ეტაპზე. ისინი ასევე პასუხს აგებენ საწარმოო პოტენციალზე, სერვისების გავრცელების არხებზე, გადაწყვეტილებებზე და პაკეტებზე, რომლებიც სერვისების კატალოგებშია წარმოდგენილი. თუ BRM

ფოკუსირებულია დამკვეთზე, პროდუქტების მენეჯერი – სერვისებზე.

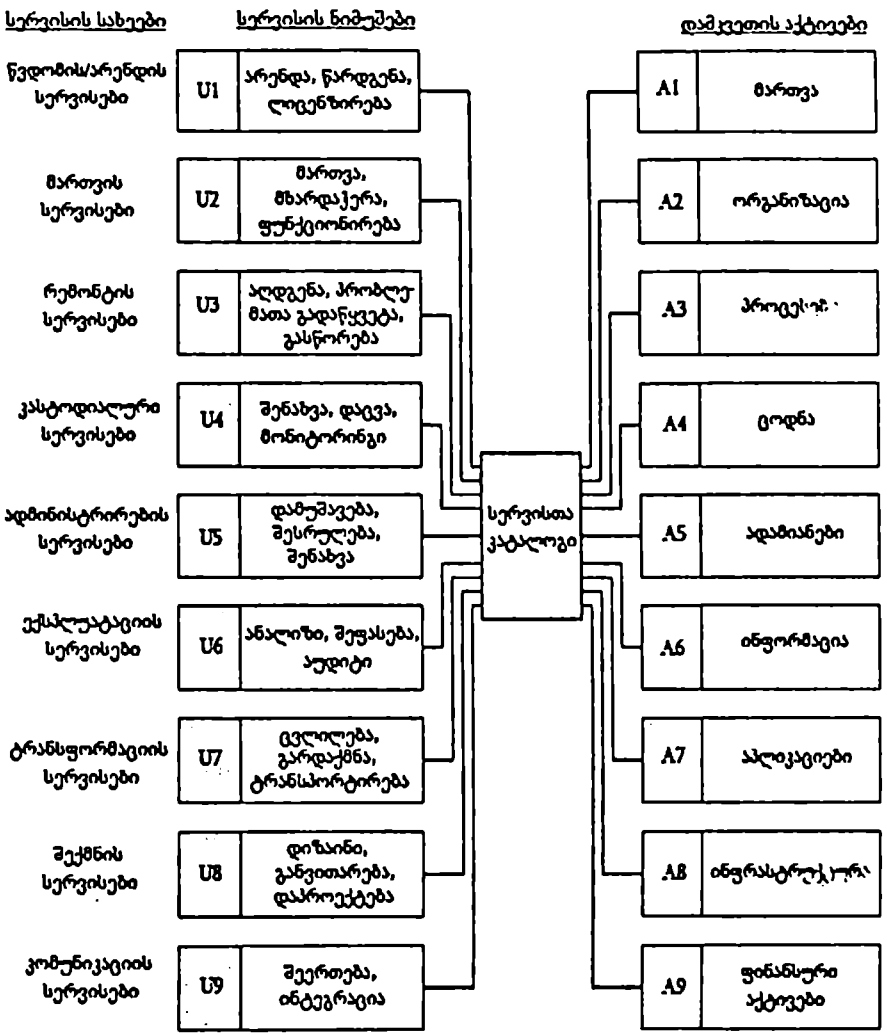
სერვისების ფასეულობის ფორმირება დამკვეთის შედეგებისგან დამოკიდებულებით გარანტიაა იმისა, რომ მენეჯერები დაგეგმავენ და მართავენ სერვისებს დამკვეთის სარგებლის თვალსაზრისით.

სერვისები განსხვავებულია იმის მიხედვით, თუ როგორ და რა კონტექსტში ქმნის ფასეულობას. სერვისის პროფილი ანალოგიურია ბიზნესმოდელის. იგი განსაზღვრავს, თუ როგორ იქცევიან სერვისების მიმწოდებლები დამკვეთის ინტერესებში, რათა შექმნან ფასეულობა (ნახ.12.2).

დამკვეთის აქტივები არის კონტექსტი, რომელშიც იქმნება სერვისის ფასეულობა, რადგან ისინი მოქმედებს შედეგებზე, რომელთა მიღება სურს დამკვეთს.

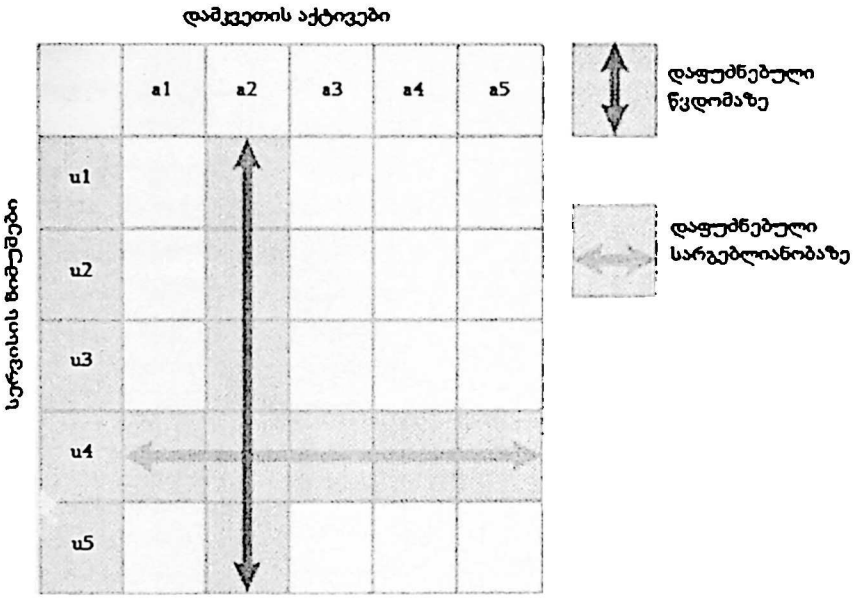
დამკვეთებს აქვთ განსხვავებული ტიპების აქტივები (Ay), რომლებიც დამოკიდებულია ისეთ ფაქტორებზე, როგორიცაა ინდუსტრიის თავისებურებანი, კლიენტები, კონკურენტები, გამოყენებადი ბიზნესმოდელები და სტრატეგიები. სერვისის პროფილის და დამკვეთის აქტივის კომბინაცია წარმოადგენს პუნქტს სერვისების კატალოგში.

რამდენიმე სერვისი კატალოგში შეიძლება მიეკუთვნებოდეს ერთ პროფილს (Ux). ამავე დროს სერვისის რამდენიმე პროფილი შეიძლება ეხებოდეს დამკვეთის ერთ აქტივს იმ სტრატეგიის დროს, რომელიც დაფუძნებულია აქტივებზე.



ნახ.12.2. სერვისების მიმწოდებლის ბიზნესმოდელების კავშირი დამკვეთის აქტივებთან

თუ მიმწოდებელი იყენებს სტრატეგიას, დაფუძნებულს სარგებლიანობაზე, მაშინ ერთი სერვისის პროფილი შეიძლება გამოყენებულ იქნას მომხმარებელთა რამდენიმე ტიპის აქტივების მხ ..დასაჭერად (ნახ.12.3).



ნახ.12.3. პოზიცირება წვდომის და სარგებლიანობის საფუძველზე

ამგვარად, მიმწოდებლის სტრატეგია განსაზღვრავს სერვისების კატალოგის შინაარსს და სტრუქტურას. მიმწოდებლისთვის მოხერხებულია სერვისების ვიზუალიზაცია მოდელების სახით, რომლებიც შედგება სერვისების პროფილების და მომხმარებელთა აქტივების სხვადასხვა კომბინაციისგან. ამ დროს ზოგიერთ კომბინაციას შეუძლია დიდი სარგებლის მოტანა

დამკვეთისადმი, სხვებთან შედარებით, მიუხედავად იმისა, რომ ისინი შედგება სერვისის ერთი და იმავე პროფილების და აქტივებისგან. ასეთი ვიზუალიზაციის შემდეგ, მენეჯერებმა უნდა ჩაატარონ ანალიზი.

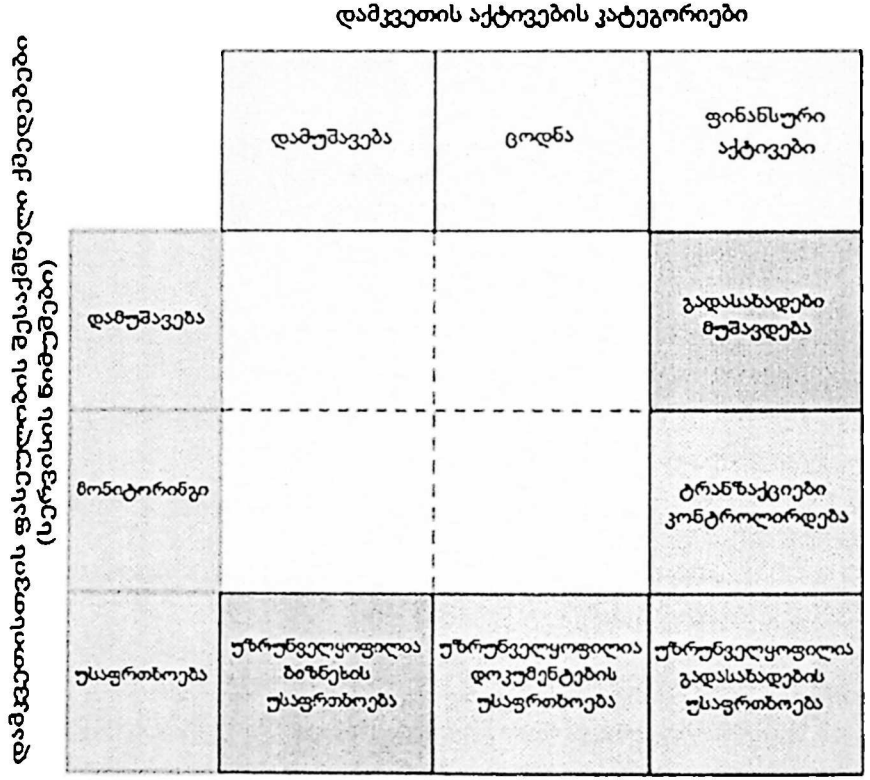
თუ ბევრი მოდელი შეიცავს პროფილს „უსაფრთხოება“, ეს მიუთითებს შესაძლებლობის არსებობის შესახებ მისი ამ სფეროში შესათავაზებლად. ვიზუალიზაციის წარმოდგენილი პრინციპი შეიძლება სასარგებლო იყოს სერვის-მენეჯმენტის ფუნქციების და პროცესების კავშირებისა და კოორდინაციისთვის.

12.2. სერვისების პორტფელის ფორმირება

მას, შემდეგ, რაც სერვისების მიმწოდებელმა განსაზღვრა შესაძლებლობები გასაღებისთვის, მან უნდა შექმნას შესაბამისი გაყიდვის წინადადებები. გასაღების ბაზარი განისაზღვრება დამკვეთის ბიზნესპროცესების ერთობლიობით და მათი შედეგებით, რომლებიც შეიძლება მომსახურებულ იქნას მიმწოდებლის სერვისებით. შედეგების მაგალითისთვის, რომელთა მიღება სურს მომხმარებელს ბიზნესპროცესის გამოსასვლელზე, შეიძლება განხილულ იქნას:

- ელ–კომერციის საიტი საიმედოდ უნდა იქნას მიერთებული საწყობის მართვის სისტემასათან;
- აუცილებელია განხორციელდეს უსაფრთხოება და კონტროლი საკვანძო ბიზნესაპლიკაციებზე;
- აუცილებელია ბიზნესის უწყვეტობის უზრუნველყოფა;
- ანგარიშების გადახდის ონლაინ–სისტემამ უნდა შემოგვთავაზოს მეტი სერვისები გადახდებისთვის და ა.შ.

ზემოთ აღწერილია შედეგები, რომელთა მიღწევა სურს დამკვეთს. თითოეული მათგანი კავშირშია ბიზნესის ერთ ან მეტ აქტივთან: ადამიანებთან, ინფორმაციასთან, ინფრასტრუქტურასთან და ა.შ. აქტივების მწარმოებლურობა იზრდება სერვისების დახმარებით. ყოველი შედეგი შეიძლება მიღებულ იქნას სხვადასხვა გზით (ნახ.12.4). დამკვეთი აირჩევს იმას, რომელსაც ახლავს ნაკლები რისკები და ხარჯი.



ნახ.12.4. გასაღების ბაზრის განსაზღვრა იმის მიხედვით, თუ რა უნდა დამკვეთს

დამკვეთები ხშირად უკმაყოფილონი არიან სერვისების მიმწოდებლების, მიუხედავად შეთანხმებული ვადების და პირობების დაცვისა. ეს გამოწვეულია, პირველ რიგში, იმით, რომ დამკვეთს არ ესმის კარგად სერვისის ფასეულობა.

სერვისებს ხშირად განსაზღვრავენ რესურსების კონტექსტში, რომელსაც დამკვეთი ღებულობს ამ რესურსების გამოყენების შედეგად. ასეთი განსაზღვრება არ გვიჩვენებს, თუ რითია სერვისი სასარგებლო და როგორ დაეხმარა ის დამკვეთს მიზნების მიღწევაში.

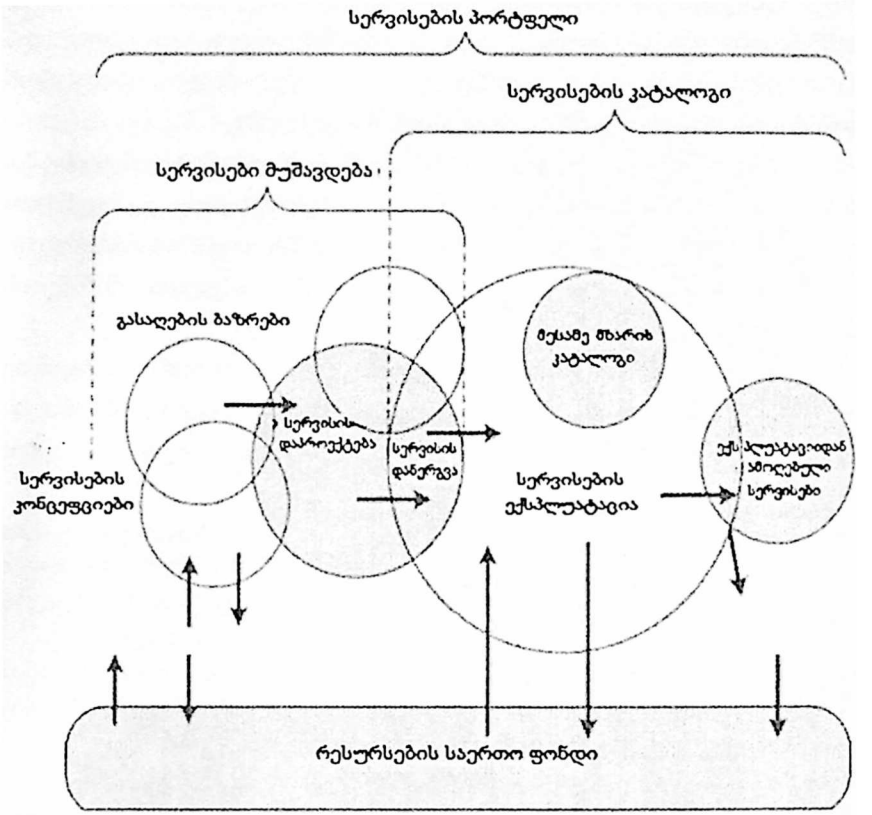
აქედან გამომდინარე, დამკვეთი ვერ პოულობს სერვისზე ხარჯის გაღების გამართლებას. უფრო მეტიც, იგი უარს ამბობს სერვისების სრულყოფაზე, თუ მან ზუსტად ვერ გაიგო, სჭირდება თუ არა მის ბიზნესს ეს სრულყოფა.

სრულყოფა გამართლებული და დაფინანსებული იქნება დამკვეთის მიერ, თუ მათი სარგებლიანობა ბიზნესისთვის ნათელია. ამიტომაა ძალზე საჭირო განისაზღვროს სერვისები შედეგების თვალსაზრისით, რომლებსაც მიიღებს დამკვეთი.

ITILv3-ში ფართოდ გამოიყენება ისეთი ცნებები, როგორიცაა სერვისების პორტფელი და სერვისების კატალოგი. აუცილებელია მათი დაყოფა და გაგება.

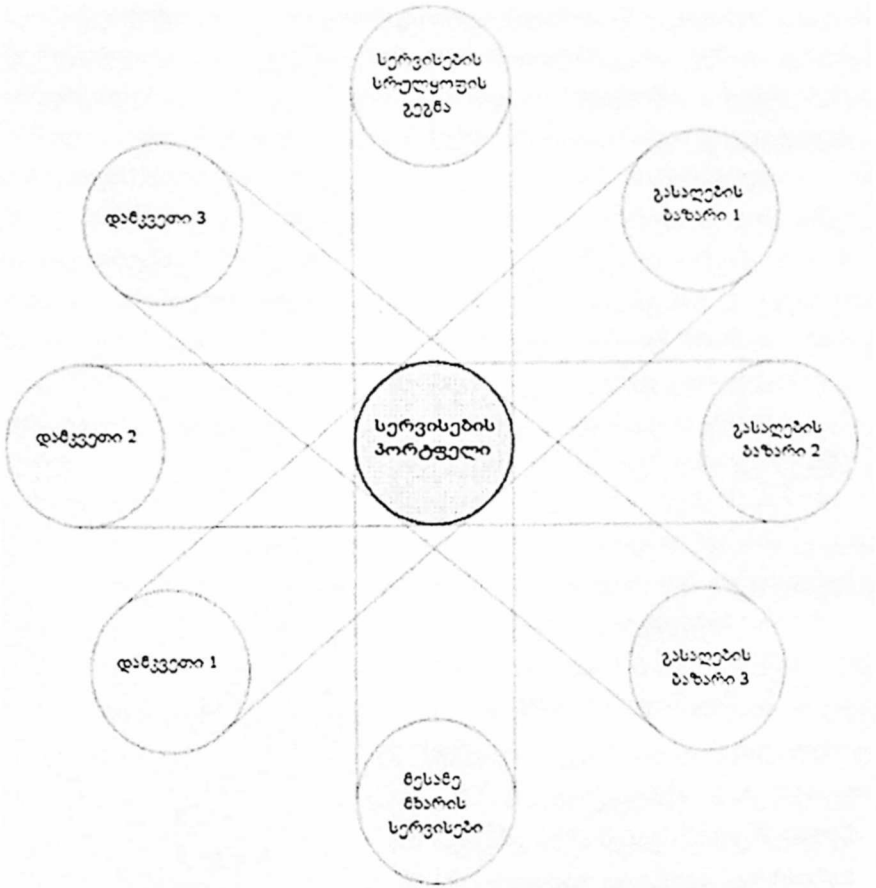
სერვისების პორტფელი (Service Portfolio) – არის სერვისების სრული ერთობლიობა, რომელიც იმართება სერვისების მიმწოდებლის მიერ. იგი გამოიყენება ყველა სერვისის სრული სასიცოცხლო ციკლის სამართავად. ის სამი ნაწილისგან შედგება (ნახ.12.5):

- სერვისების კატალოგი ასახავს სერვისებს, რომლებიც ექსპლუატაციაშია ან სრულ მზადყოფნაშია;
- სერვისები მუშავდება;
- სერვისები, რომლებიც გამოსულია ექსპლუატაციიდან.



ნახ.12.5. სერვისების პორტფელის სტრუქტურა

სერვისების პორტფელი ასახავს მიმწოდებლის არსებულ ვალდებულებებს კონტრაქტების მიხედვით, აგრეთვე სერვისების შეძენის განვითარებას და სრულყოფას მიღებული გეგმების და სტრატეგიების შესაბამისად (ნახ.12.6).



ნახ.12.6. სერვისების პორტფელი

სერვისების პორტფელში შედის ასევე მესამე მხარის სერვისები, რომლებიც დამკვეთის შეთავაზების განუყოფელი ნაწილია. ამავე დროს, ზოგიერთი მათგანი დამკვეთისთვის ხილვადია, ზოგი – არა.

სერვისების პორტფელის გამოყენება მენეჯერს ეხმარება სერვისებში ინვესტიციათა პრიორიტეტების განლაგებაში და რესურსის სწორად განაწილებაში. ცვლილებები სერვისის პორტფელში იმართება პოლიტიკით და პროცედურით.

სერვისების პორტფელი ასახავს ყველა რესურსს, რომლებიც იქნა გამოყოფილი ადრე ან გამოიყენება ახლა სერვისების მთელ სასიცოცხლო ციკლში. სერვისების პორტფელის კონტროლი და მართვა დავალებული აქვს სერვისების პორტფელის მენეჯმენტს (Service Portfolio Management ან SPM). იგი განიხილავს სერვისებს წარმოდგენილ ფასეულობათა ტერმინებში ბიზნესისთვის.

SPM როგორც უწყვეტი და დინამიკური პროცესების ერთობლიობა შეიცავს შემდეგს:

1. რესურსების განაწილება;
2. სერვისების სრული ჩამონათვალის განსაზღვრა, სერვისების პორტფელის შემოწმება და დამტკიცება;
3. ხარჯების და რისკების მინიმიზაცია;
4. სერვისების ფასეულობათა მაქსიმიზაცია;
5. მოთხოვნილებისა და შეთავაზების ბალანსის დაცვა.

SPM-ის ძირითადი ამოცანაა რისკების და ხარჯების მართვა სერვისების ფასეულობათა ამაღლების მიზნით. SPM ეხმარება მენეჯერებს, გაიგონ დამკვეთთა მოთხოვნები სერვისების ხარისხზე, აგრეთვე გაითვალონ ხარჯები შესაბამისი სერვისების მიწოდებაზე. მენეჯერთა ამოცანაა მოიძიონ ხერხები ხარჯების შესამცირებლად შემოთავაზებული სერვისების ხარისხის მართვის პროცესში.

ყოველი შესასვლელი, გამოსასვლელი და გადაადგილება სერვისების პორტფელში მტკიცდება მხოლოდ გამოყოფილი შესაბამისი ბიუჯეტის და ინვესტიციების უკუგების გეგმის არსებობის დროს,

სერვისების კატალოგი (Service Catalogue) – ესაა სერვისების პორტფელის ერთადერთი ნაწილი, რომელსაც მოაქვს მოგება და ამოისყიდის დამკვეთის ხარჯებს სერვისებზე. ესაა პორტფელის ის ნაწილი, რომელსაც ხედავს დამკვეთი. კატალოგის ელემენტებია სერვისები, რომლებიც ექსპლუატაციის სტადიაშია ან მზადყოფნაშია. ამგვარად, კატალოგიდან სერვისების შეთავაზება დამკვეთზე შეიძლება იმწამსვე.

ნებისმიერი სერვისი შეიძლება შევიდეს კატალოგში მხოლოდ მას შემდეგ, რაც მასთან დაკავშირებულ დანახარჯებზე და რისკებზე გაწეული იქნება მენეჯერებისა და დამმუშავებლებისგან სათანადო ყურადღება. ამავდროულად, სერვისის ფასი შეიძლება შეიცვალოს კონკრეტული დამკვეთის მიხედვით.

სერვისების კატალოგის ფორმირება არის სტრატეგიის აგების ეტაპის მნიშვნელოვანი ნაწილი, რადგან იგი სერვისების მიმწოდებლის არსებული შესაძლებლობების პროექციაა.

ზოგად შემთხვევაში დამკვეთს არ აინტერესებს ის სერვისები, რომლებიც დამუშავების სტადიაშია ან გამოსულია ექსპლუატაციიდან. ფაქტობრივად, ის სერვისები, რომლებიც მიმწოდებელმა შეიძლება შესთავაზოს მას მომავალში, დღეისათვის არ წარმოადგენს მისთვის ფასეულს. ე.ი. ფასეულია მხოლოდ კატალოგში არსებული სერვისები.

იმისათვის, რომ სერვისი დამატებულ ან ამოღებულ იქნას კატალოგიდან, აუცილებელია მათი თანხმობა, ვინც მარეგულირებელი დანერგვის ეტაპს შემდეგი მიზეზების გამო:

- თუ ელემენტი დამატებულია სერვისების კატალოგში, იგი მისაწვდომი უნდა იყოს დამკვეთებისთვის. ე.ი. უნდა არსებობდეს სრული რწმენა იმაზე, რომ სერვისი დასრულებული პროდუქტია, რომელიც სრულად იქნება მხარდაჭერილი

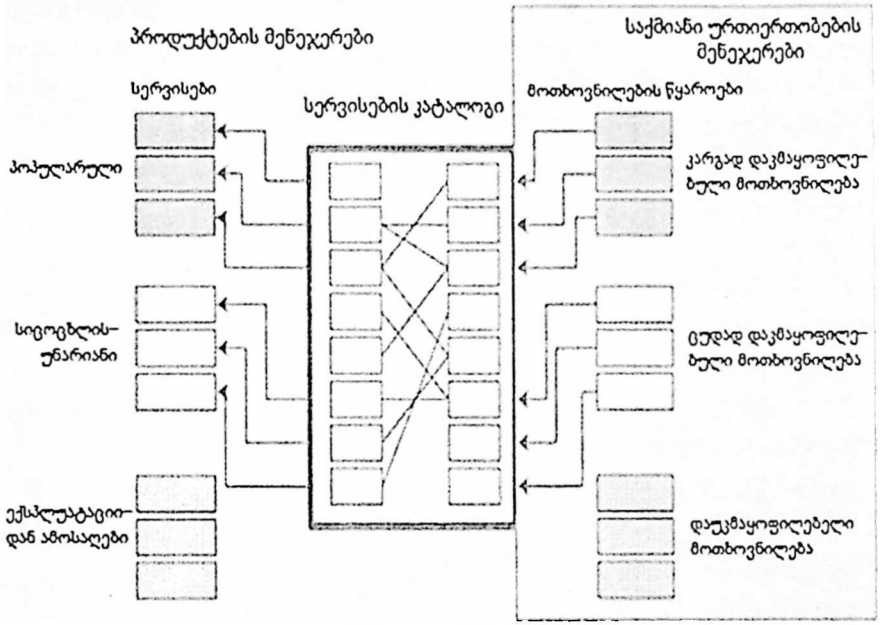
მიმწოდებლის მიერ. ნაჩქარევად დამატებულმა სერვისებმა შეიძლება მოუტანოს დიდი ზარალი როგორც დამკვეთს, ასევე მიმწოდებელს;

- სერვისების უმეტესობა კატალოგში იმყოფება ექსპლუატაციაში, ანუ ისინი დამკვეთთან გარკვეული შეთანხმების ობიექტებია. არადამტკიცებული ცვლილებები კატალოგში გამოიწვევს იმას, რომ შეთანხმების პირობები აღარ სრულდება;
- სერვისის დამატება კატალოგში ნიშნავს რესურსების გამოყოფას არსებული და პოტენციური დამკვეთებისთვის. აქ მნიშვნელოვანია რესურსების განაწილების პროცესი, რადგან შეიძლება შეიქმნას სიტუაცია, როცა მოთხოვნილი რესურსები დაკავებულ იქნება არარენტაბელური სერვისების მხარდასაჭერად.

სერვისების კატალოგი ასევე ემსახურება მოთხოვნილებების და შეთავაზებების კავშირს. შედეგებთან მიბმული დამკვეთის აქტივები, რომლებსაც ბიზნესი ელოდება მათგან, არის მოთხოვნილების წყარო (ნახ. 12.7).

დამკვეთებს აქვთ მოლოდინი სერვისების ხარისხის და სარგებლიანობის გარკვეული დონისთვის. თუ სერვისების კატალოგის რომელიმე ელემენტს შეუძლია ამ მოლოდინის დაკმაყოფილება, მაშინ დამკვეთსა და მიმწოდებელს შორის შედგება გარიგება. ამგვარად, სერვისების კატალოგი ემსახურება იმას, რომ დამკვეთმა შეიძინოს სერვისი.

სწორედ სერვისების კატალოგში ხდება სერვისების დაყოფა შემადგენელ ნაწილებად – აქტივები, სისტემები და პროცესები. ისინი აისახება შესასვლელი წერტილებით მათი გამოყენების და მხარდაჭერის კონტექსტში.



ნახ.12.7. სერვისების კატალოგის და მოთხოვნილებათა მართვის ურთიერთქმედება

კატალოგში ელემენტები ჯგუფდება სერვისის მიხედვით (Lines of Service ან LOS) ბიზნესაქტივობის თანამთხვევის საფუძველზე, რომლისთვისაც მათ ხელისშეწყობა შეუძლია. ეს ეხმარება განაწილებული რესურსების მართვას, სათანადო დონეზე სერვისების მწარმოებლურობის და მოთხოვნილებათა მხარდაჭერის მიზნით.

სერვისები კატალოგში ითვლება სიცოცხლისუნარიანად, თუ ისინი ფუნქციონირებენ ფინანსურ ბარიერზე მაღლა. ანუ, თუ ისინი ამოისყიდიან მათზე გაწეულ ხარჯებს და მოაქვთ გარკვეული მოგება სერვისის მიმწოდებლისთვის. ამავე დროს

მიმწოდებელი ცდილობს განავითაროს და სრულყოს ეს სერვისები უფრო მეტი მოგების მისაღებად: სთავაზობს ახალ შესაძლებლობებს, მანევრირებს ფასით და მაქსიმალურად უახლოვებს მათ თვისებებს იმას, რასაც დამკვეთები მოითხოვენ.

თუ სერვისის მწარმოებლურობა ეცემა ფინანსური ბარიერის ქვემოთ, მაშინ მიმწოდებელმა უნდა გადაწყვიტოს, ჩამოწეროს სერვისი თუ არა. ამასთანავე შესაძლებელია, რომ ცუდი მწარმოებლურობის სერვისები იმყოფებოდეს კატალოგში ობიექტური მიზეზების გამო. მაგალითად, დამკვეთთან ადრე დადებული შეთანხმების საფუძველზე.

სერვისების კატალოგში შეიძლება იყოს ასევე მესამე მხარის სერვისები. ისინი წარმოდგენილია მიმწოდებლების მიერ თავის სერვისებთან ერთად.

სერვისები დამუშავებაშია (Service Pipeline) – ესაა სერვისების პორტფელის ნაწილი, რომელიც შედგება იმ სერვისებისგან, რომლებიც ახლა ვითარდება, მაგრამ ჯერ მიუწვდომელია დამკვეთებისთვის. ისინი მისაწვდომი გახდება პროექტირების, ტესტირების და განთავსების შემდეგ. სერვისების პორტფელის ეს ნაწილი ასახავს სერვისების მიმწოდებლის პოტენციალს და სტრატეგიას.

ექსპლუატაციიდან მოხსნილი სერვისები (Retired Services) – ესაა სერვისების პორტფელის ის ნაწილი, რომელიც შედგება სამრეწველო ექსპლუატაციიდან ამოღებული სერვისებისგან. ინფორმაცია მათ შესახებ ინახება, რათა კვლავ შესაძლებელი იყოს მათი საჭიროების შემთხვევაში გამოყენება (ბიზნესის და IT-ის შეთანხმების საფუძველზე). ასეთი სერვისები მიუწვდომელია დამკვეთთათვის.

12.3. ფინანსების მართვა

ფინანსების მართვა (Financial Management) – ესაა ფუნქცია და პროცესები, პასუხისმგებელი ბიუჯეტის მართვაზე, სერვისების მიმწოდებლის ხარჯების აღრიცხვის და მათი ანაზღაურების მიზნით. ფინანსების მართვა სტრატეგიული ინსტრუმენტია ყველა ტიპის სერვისების მიმწოდებლისთვის. შიგა მიმწოდებლებიც კი ვალდებულნი არიან, იმოქმედონ ფინანსური გამჭვირვალობის დონეების და ბიზნესერთეულების აღრიცხვის შესაბამისად, რომელთაც ის ემსახურება.

ფინანსების მართვა აძლევს ბიზნესს და IT-ს რაოდენობრივ ფინანსურ შეფასებას სერვისების ფასეულობაზე, აქტივების ღირებულებაზე, რომლებიც საფუძვლად უდევს ამ სერვისების გამოყენებას, ასევე მეთოდები და ინსტრუმენტები ოპერატიული პროგნოზირებისათვის. ფინანსების მართვა არის საშუალება ისეთი რთული საკითხის გადასაწყვეტად, როგორიცაა ბიზნესის მიერ IT–სფეროს აღქმა.

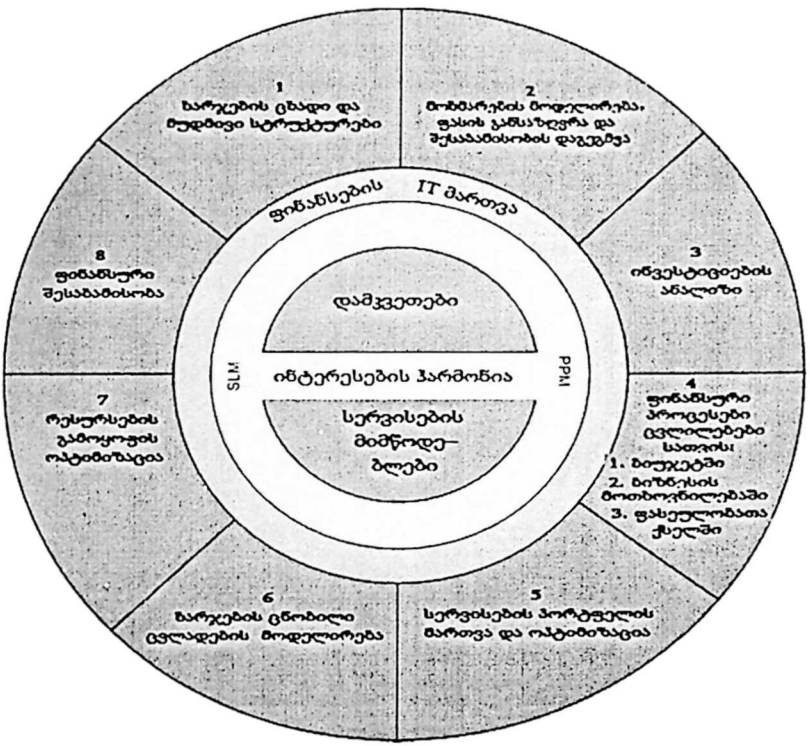
IT–ორგანიზაციები სულ უფრო ხშირად იყენებენ ფინანსების მართვას ისეთ პროცესებში, როგორიცაა:

- გადაწყვეტილების მიღება;
- ცვლილებების დაჩქარება;
- სერვისების პორტფელის მართვა (SPM);
- ფინანსური კონტროლი;
- ოპერატიული მართვა;
- ფასეულობის შექმნა და ფიასირება[6].

ITIL–ის ორგანიზაციებში, რომლებიც აწარმოებს ბიზნესს, ყველაზე ხშირად იგულისხმება დამკვეთები, ხოლო სერვისის მიმწოდებლები გამოდიან მხოლოდ როგორც ბიზნესის ხელშემწყობები. არსებითად, IT–ორგანიზაციები, აწვდიან რა

სერვისებს, ასევე აწარმოებენ ბიზნესს, ხოლო ნებისმიერი ბიზნესისთვის ფუნდამენტურად მნიშვნელოვანია ფინანსების სწორი მართვა.

სერვისების მიმწოდებელი თვალყურს უნდა ადევნებდეს ბალანსს მოთხოვნილებასა და შეთავაზებას შორის, მინიმალურად უნდა ამცირებდეს ხარჯებს და ზრდიდეს სერვისების ფასეულობას. 12.8 ნახაზზე მოცემულია ის მომენტები, რომლებიც საერთოა ბიზნესის და IT ორგანიზაციისთვის.



ნახ.12.8. საერთო ბიზნესსა და IT-ს შორის

ფინანსების მართვა ინფორმაციის წყაროა, რომელიც ხელს უწყობს IT–ორგანიზაციას პასუხი გასცეს შემდეგ კითხვებს:

1. რომელი სტრატეგიაა ყველაზე ეფექტიანი: უფრო მაღალი მოგების მიღება, ხარჯების შემცირება თუ სერვისების ფართო არჩევის უზრუნველყოფა ?
2. რომელ სერვისებზეა ხარჯები ყველაზე მეტი და რატომ ?
3. რომელი ტიპის სერვისები და რა მოცულობით არის ყველაზე მოთხოვნადი ? როგორი ფინანსური დაბანდებებია საჭირო მათ მხარდასაჭერად ?
4. რამდენად ეფექტურია წარმოდგენილი სერვისების გამოყენებული მოდელები კონკურენტების ანალოგიურ მოდელებთან ?
5. მიიყვანა თუ არა სერვისების დაპროექტების სტრატეგიულმა მიდგომამ კონკურენტუნარიან ფასამდე ამ სერვისებზე ? რაზეა უკეთესი ორიენტაციის აღება: რისკების შემცირებაზე თუ ხარისხის ამაღლებაზე ?
6. რა ძირითადი ნაკლოვანებანი აქვს ჩვენს სერვისებს ?
7. რომელ ფუნქციურ სფეროებზეა საჭირო კონცენტრირება სერვისების უწყვეტი სრულყოფის სტრატეგიის აგებისას ?

ფინანსების მართვისგან მიღებული ინფორმაციის გარეშე შეუძლებელია ამ კითხვებზე კორექტული პასუხის გაცემა. ფინანსების სწორი მართვის არარსებობა ანეიტრალებს სტრატეგიის აგების, დიზაინის და სხვა ნებისმიერი ტექნიკური გადაწყვეტის არსს. ფინანსების მართვა უზრუნველყოფს ხარჯების გამჭვირვალობას და მიზანშეწონილობას ამ სერვისებზე როგორც ბიზნესისთვის, ასევე თვით მიმწოდებლისთვისაც,

ფინანსების მართვა მოიცავს შემდეგ ძირითად ამოცანებს:

- სერვისების ფასეულობის შეფასება;
- მოთხოვნის მოდელირება;

- სერვისების პორტფელის მართვა;
- სერვისების უზრუნველყოფის ოპტიმიზაცია;
- შესაბამისობის დაგეგმვა;
- ინვესტიციების ანალიზი სერვისებში;
- საბუღალტრო ანგარიშგების ფორმირება;
- შესაბამისობა;
- ხარჯების ცვლადების მოდელირება.

ამჯერად უფრო დეტალურად დავახასიათოთ ეს ამოცანები.

1. სერვისების ფასეულობის შეფასება (Service Valuation) – ესაა სრული ხარჯების შეფასება მიმწოდებლისთვის მის მიერ წარმოდგენილ სერვისზე და ამ სერვისის სრული ფასეულობა ბიზნესისთვის. სერვისის ფასეულობის შეფასება გამოიყენება იმისთვის, რომ დახმარება გაეწიოს ბიზნესს და მიმწოდებელს, რათა მოახერხონ შეთანხმება სერვისის ფასეულობაზე. ამ პროცესის ძირითადი მიზანი სერვისის ფასის განსაზღვრაა, რომელსაც დამკვეთი ჩათვლის სამართლიანად, და მიმწოდებელს მისცემს მოგებას და სერვისის მხარდაჭერას.

როგორც უკვე აღინიშნა, სერვისის ფასეულობა შედგება ორი ძირითადი პარამეტრისგან – სარგებლიანობა და ხარისხის გარანტია. ეს პარამეტრები მოითხოვს ფინანსურ გამოსახვას. აქედან სერვისების ფასეულობის შეფასება იყენებს ორ საკვანძო კონცეფციას:

1.1. უზრუნველყოფის ფასი (Provisioning Value) – ესაა ფაქტობრივი ფასი სერვისის უზრუნველსაყოფად მიმწოდებლისთვის. იგი შეიცავს ხარჯებს რესურსებზე, რომლებიც აუცილებელია მის ასამოქმედებლად. ძირითადი მათგანი მოცემულია ქვემოთ:

- ლიცენზიების ფასი პროგრამულ უზრუნველყოფაზე;
- მოწყობილობის შესყიდვა ან არენდა;

- ადამიანური რესურსები;
- კომუნალური მომსახურება, ქსელის მხარდაჭერა, ინფორმაციული ცენტრის და სხვა ხარჯები მომსახურების საშუალებებზე;
- გადასახადები, ამორტიზაცია, პროცენტები სესხების მიხედვით.

ამ ხარჯთა ჯამი წარმოადგენს მინიმალურ ფასს სერვისზე – ეს იგივე ფინანსური ზღუდეა, რომლის ქვემოთაც მიმწოდებელი ვერ გადავა კომერციული წინადადების ფორმირებისას.

1.2. სერვისის ფასეულობის პოტენციალი (Service Value Potential) – ესაა შეფასება, დაფუძნებული სერვისის ფასეულობაზე დამკვეთის თვალსაზრისით ან წარმოდგენილი სერვისის სარგებლიანობის და გარანტიის ზღვრული მნიშვნელობები დამკვეთის საკუთარი აქტივების გამოყენებასთან შედარებით.

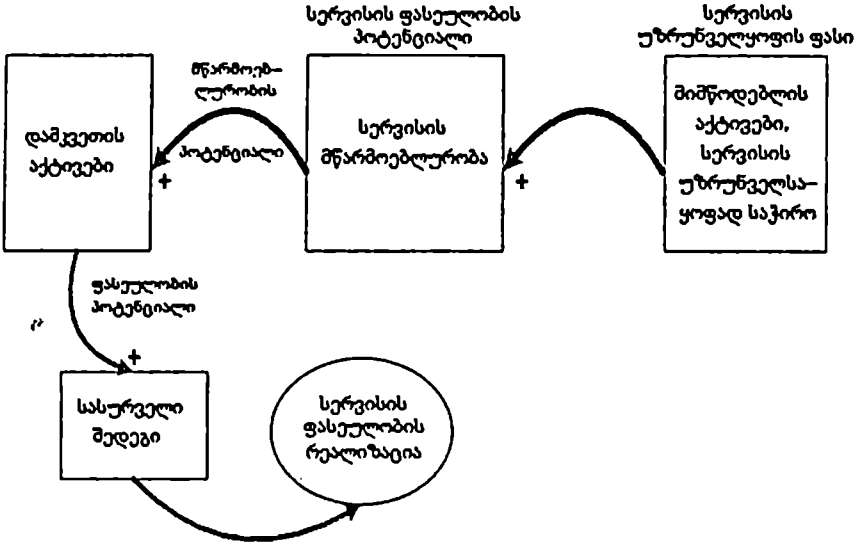
თავიდან საფუძვლის სახით წარმოდგენილია სერვისის ელემენტები, რომელთაც შეუძლია დამკვეთისთვის ფასეულობის მოტანა. შემდეგ ყოველი ელემენტი ფასდება ცალ-ცალკე მათთვის მინიჭებული ფასეულობების შესაბამისად. ბოლოს, ყველა ელემენტის ჯამი იკრიბება დანახარჯებთან ერთად, რომელიც მისი წარმოდგენისთვისაა საჭირო, რათა განისაზღვროს სერვისის საბოლოო ფასი.

ორი კონცეფციის ურთიერთკავშირი მოცემულია 12.9 ნახაზზე.

2. მოთხოვნის მოდელირება

მოთხოვნის არასაკმარისად ცოდნამ და მისმა გავლენამ ყველა პროცესზე შეიძლება გამოიწვიოს დიდი ხარჯები და რისკები. კერძოდ, მოთხოვნა მჭიდროდაა დაკავშირებული სერვისების რაოდენობაზე, რომლებსაც დამკვეთი „აწარმოებს“.

ეს მოითხოვს ფინანსების მართვისგან ბიუჯეტის შესაძლო რხევების პროგნოზირების და გაზომვის უნარს მოთხოვნის ყოველი ცვლილებისას.



ნახ.12.9. მომხმარებლის აქტივები, როგორც სერვისის ფასეულობის ფორმირების საუძველი

სერვისებზე მოთხოვნის შესაფასებლად, გადაწყვეტილების მისაღებად და კონტროლისთვის საკვანძოდ ითვლება ინფორმაცია სერვისების კატალოგიდან და სიმძლავრეების მართვიდან.

სიმძლავრეების მართვა (Capacity Management) – პროცესია, რომელიც პასუხისმგებელია სერვისების სიმძლავრეების და IT-ინფრასტრუქტურის დროულ და ხარჯებით ეფექტიან შესაბამისობაზე მოთხოვნილებებთან, რომლებიც შეთანხმებულია სერვისის დონის მიზნობრივ მაჩვენებლებთან. სიმძლავრეების მართვა ითვალისწინებს ყველა რესურსს, რომელიც აუცილებელია

სერვისის უზრუნველსაყოფად, აგრეთვე აწარმოებს ბიზნესის მოთხოვნილებების მოკლევადიან, საშუალოვადიან და გრძელვადიან დაგეგმვას [11].

მნიშვნელოვან როლს მოთხოვნის მოდელირებისას თამაშობს საერთო ღირებულების დამკვეთის მიერ სერვისის გამოყენების განსაზღვრა. საერთო ღირებულების გამოყენება (Total Cost of Utilization ან TCU) – ესაა დამკვეთის სრული დანახარჯები სერვისის გამოყენებაზე მისი მთლიანი სასიცოცხლო ციკლის განმავლობაში.

მოთხოვნის მოდელირება ემსახურება ბიზნესის მიერ სერვისის მოსალოდნელი გამოყენების შეფასებას და ამ დროს სერვისების მიმწოდებლის აუცილებელი რესურსების შეფასებას. სერვისების კატალოგი გავლენას ახდენს მოთხოვნის მოდელირებაზე, მაგრამ ყველა IT–ორგანიზაციისთვის უნდა არსებობდეს უკუკავშირიც – მოთხოვნის მოდელირება უნდა ახდენდეს გავლენას სერვისების კატალოგზე.

3. სერვისების პორტფელის მართვა

უზრუნველყოფის სრული ღირებულების ფინანსური შეფასება ეხმარება მიმწოდებელს თავისი სერვისების შესადარებლად კონკურენტთა ანალოგებთან. ეს შედარება აუცილებელია საკვანძო გადაწყვეტილების მისაღებად – სასარგებლოა თუ არა მიმწოდებლისთვის ამა თუ იმ სერვისის შეთავაზება.

4. სერვისების უზრუნველყოფის ოპტიმიზაცია (Service Provisioning Optimization ან SPO) – ესაა სერვისის ფინანსებისა და შეზღუდვების ანალიზი გადაწყვეტილების მისაღებად, იმ შემთხვევაში, როცა სერვისის უზრუნველყოფის ალტერნატიული მიდგომა იძლევა ხარჯების შემცირების ან ხარისხის

გაუმჯობესების შესაძლებლობას. ფინანსების მართვა არის საკვანძო SPO-თვის, რომლის ძირითადი კანდიდატებია სერვისები, რომლებიც აღნიშნულია კატალოგში წასაშლელად.

სერვისის უზრუნველყოფა შეიძლება გახდეს არასარგებლიანი მიმწოდებლისთვის, თუ კონკურენტებს შუძლიათ უკეთესი ხარისხის ან სარგებლიანობის ან დაბალი ფასის შეთავაზება. სერვისის წაშლა შეიძლება იყოს სხვა ფაქტორების შედეგიც. მაგალითად, ბანალური დაბერება. ფინანსების მართვა უზრუნველყოფს IT-ორგანიზაციას ინფორმაციით არსებული ხარჯების შესახებ სერვისზე, ალტერნატიული მეთოდების არსებობაზე, მათი გამოყენების შესაძლებლობებზე სხვა სერვისებთან კომბინაციაში, ფინანსურ სტრუქტურებში და ა.შ. ეს ინფორმაცია მეტად მნიშვნელოვანია სერვისების პორტფელის ფორმირებისთვის.

5. მიმნდობი დაგეგმვა

ფინანსების მართვის ერთ-ერთი მიზანია სერვისების სათანადო დაფინანსების და თანხლების უზრუნველყოფა. დაგეგმვა ასრულებს სერვისებზე მოთხოვნის რაოდენობრივ შეფასებას მომავლისთვის. შემავალი მონაცემები უნდა შეიკრიბოს IT–ორგანიზაციის და ბიზნესის საქმიანობის ყველა სფეროდან და უნდა ასახავდეს მთლიან სურათს.

„მიმნდობი“ აქ ნიშნავს გარკვეული დამაჯერებლობის არსებობას, რომ ფინანსურ მართვაში გამოყენებულ მოთხოვნისა და შეთავაზების მონაცემებს და მოდელებს აქვს ჭეშმარიტების მაღალი დონე. ინფორმაციის შესაბამისობა მნიშვნელოვანია ორი ძირითადი მიზეზით:

- მონაცემები თამაშობს კრიტიკულ როლს ფინანსების მართვის მიერ დასმული მიზნების მისაღწევად;
- არაკორექტული მონაცემების არსებობა არყევს მიღებული გადაწყვეტილების მნიშვნელობას.

რადგან ფინანსური მართვა იძლევა ინფორმაციას მრავალი გადაწყვეტილებისათვის სერვის-მენეჯმენტში, ამიტომ მისი საიმედოობის (ჭეშმარიტების) დონე უნდა იყოს მაღალი. ნებისმიერი უნდობლობა (ეჭვი) ამ ინფორმაციის სიზუსტეზე, გამოიწვევს მთლიანად ფინანსების მართვის ფასეულობის უნდობლობას.

6. ინვესტიციების ანალიზი სერვისებში

ინვესტიციების ანალიზის მიზანია ღირებულებითი მაჩვენებლების მოპოვება სერვისის მთელი სასიცოცხლო ციკლის განმავლობაში. ღირებულებითი მაჩვენებლები ეფუძნება სერვისთა ფასეულობების და მათ მთლიან სასიცოცხლო ციკლზე ხარჯების მოპოვებას.

7. ხარჯების აღრიცხვა

ხარჯების აღრიცხვა სერვის-მენეჯმენტის სფეროში მოითხოვს ტრადიციული საბუღალტრო აღრიცხვისგან განსხვავებულ მეთოდებს და საშუალებებს.

ხარჯების აღრიცხვა (Accounting) – პროცესია, რომელიც პასუხს აგებს ფაქტობრივი ხარჯების იდენტიფიკაციის შესახებ სერვისების უზრუნველყოფაზე, მათ შედარებაზე გეგმიურ ხარჯებთან და ბიუჯეტის გადახრების სამართავად. ფინანსების მართვა ასრულებს დამაკავშირებელ როლს კორპორაციულ საფინანსო სისტემასა და სერვის-მენეჯმენტს შორის.

ხარჯების აღრიცხვის ფუნქციის შედეგები შესავალი მონაცემებია დაგეგმვისათვის და ხელს უწყობს მომარაგების და მოხმარების პროცესების კარგად გაგებას და დეტალიზაციას.

ხარჯების კლასიფიკაციისთვის განიხილავენ შემდეგ ხერხებს:

- კაპიტალური / საექსპლუატაციო ხარჯები – კლასიფიკაცია ასახავს საბუღალტრო აღრიცხვის განსხვავებულ მეთოდოლოგიებს, რომლებსაც ითხოვს ბიზნესი და რეგულატორები;
- პირდაპირი / ირიბი ხარჯები:
  - პირდაპირი ხარჯები ეხება კონკრეტულ სერვისს, რომელიც მათი ერთადერთი მომხმარებელია;
  - ირიბი ხარჯები ან „განაწილებული" ხარჯები – ესაა ხარჯები, რომლებიც განაწილებულია მრავალ სერვისს შორის ისე, რომ თითოეული სერვისი იყენებს საერთო თანხის რაღაც ნაწილს.
- მუდმივი / ცვლადი ხარჯები – ეს კლასიფიკაცია ეყრდნობა შეთანხმებულ ვალდებულებებს დროის ან ფასის მიხედვით. ასეთი კლასიფიკაციის სტრატეგიული არსი იმაშია, რომ ბიზნესი უნდა მიისწრაფოდეს მუდმივი ხარჯების ოპტიმიზაციისკენ და ცვლადი ხარჯების მინიმიზაციისკენ, მაქსიმალური პროგნოზირების და სტაბილურობის უზრუნველსაყოფად;
- ხარჯების ერთეულები – ესაა ადვილად გასათვლელი (მაგ., თანამშრომელთა რაოდენობა, ლიცენზიების რაოდენობა პროგრამებზე) ან გაზომვადი ობიექტები (მაგ., ცენტრალური პროცესორის დატვირთვა, ელექტროენერგიის გამოყენება). ხარჯების ერთეული აიდენტიფიცირებს მოხმარების ერთეულს, გათვლილს კონკრეტული სერვისისთვის.

8. შესაბამისობა (compliance) – დამაჯერებლობის უზრუნველყოფა სტანდარტების ან სახელმძღვანელო

დოკუმენტაციის ერთობლიობის დაცვაში, რაღაცის სისრულეში და მთლიანობაში, განსაზღვრული დადგენილი წესების გამოყენებაში.

ფინანსების მართვის კონტექსტში შესაბამისობა ნიშნავს მეთოდების და პრაქტიკის გამოყენებას სათანადო სიზუსტით და ხანგრძლივობით. ეს ეხება ფინანსური აქტივების, კაპიტალიზაციის შეფასებას, შემოსავლის განსაზღვრას, წვდომის და უსაფრთხოების კონტროლს და ა.შ. შესაბამისობა ადვილად მისაღწევია, თუ გამოყენებული მეთოდები და პრაქტიკა დოკუმენტირებულია.

სერვისების მიმწოდებლისთვის მეტად აუცილებელია შეთავაზებული სერვისების შესაბამისობის უზრუნველყოფის ფასის ცოდნა. სერვისები, რომელთა წარმოდგენა შესაძლებელია მოცემული ფასით ერთ სფეროში, შესაძლოა ვერ იქნას იმავე ფასით შეთავაზებული მეორე სფეროში, სწორედ სტანდარტებთან შესაბამისობის პრობლემების, კანონების, დადგენილი ნორმების გამო.

9. ცვლადი ხარჯების მოდელირება

ცვლადი ხარჯების მოდელირება (Variable Cost Dynamics ან VCD) – ესაა ტექნიკა, რომელიც გამოიყენება იმის გასაგებად, თუ როგორ ხდება სრულ ხარჯებზე კომპლექსური ცვლადი ელემენტების (ცვლადების) სიმრავლის ზემოქმედება, რომელთაგან ყველას თავისი წვლილი შეაქვს სერვისების უზრუნველყოფაში.

ქვემოთ მოყვანილია მოკლე ჩამონათვალი ხარჯების შესაძლო ცვლადებისა, რომლებიც შეიძლება განხილულ იქნას ანალიზისთვის:

- მომხმარებელთა რაოდენობა და ტიპები;
- ლიცენზიების რაოდენობა პროგრამებზე;
- მიწოდების მექანიზმები;
- მონაცემთა საცავის თანხლების ღირებულება;

- რესურსების რაოდენობა და ტიპები;
- ერთი ახალი შენახვის მოწყობილობის დამატების ღირებულება;
- ერთი ახალი მომხმარებლის დამატების ღირებულება.

ხარჯების ცვლადების რაოდენობა დამოკიდებულია გასაანალიზებელი სერვისის ტიპზე. ამის გამო VCD შეიცავს სცენარების დიდ რაოდენობას და ვარაუდს, რომელთაგან თითოეული იყენებს თავისი ინსტრუმენტების ერთობლიობას, ხარჯების ცვლადების გასათვლელად.

12.4. ინვესტიციების დაბრუნება

ინვესტიციების დაბრუნება ტრადიციული გაგებით ნიშნავს ინვესტიციის ამონაგებს, ანუ თანაფარდობას მიღებულ მოგებასა და კაპიტალდაბანდებას შორის. ITIL კონტექსტში ინვესტიციის დაბრუნებას აქვს ოდნავ სხვა მნიშვნელობა. ინვესტიციების დაბრუნება, ფაქტობრივად არის აქტივების შესაძლო გამოყენების ზომა სერვისის ფასეულობის გაზრდისათვის. მოვიყვანოთ განსაზღვრება ITILv3-ის ოფიციალური ლექსიკონიდან:

ინვესტიციის ამონაგები (Return on investment ან ROI) – მოსალოდნელი საინვესტიციო სარგებლის მიღების საზომი. მარტივ შემთხვევაში ესაა ინვესტიციების სუფთა მოგება, გაყოფილი ინვესტირებული აქტივების ღირებულებაზე [11].

კომპანიები იყენებენ ROI-ს გადაწყვეტილების მისაღებად სერვის-მენეჯმენტის განვითარების ინვესტირებასთან მიმართებით, რომელსაც თავისთავად არ მოაქვს ცხადი ტაქტიკური უპირატესობები ბიზნესისთვის. ROI-ს იყენებენ სამი მდგენელის პოზიციიდან, რომლებიც ყველა პროექტშია – კომპანიის პერსონალი, პროცესები და ტექნოლოგიები. შემდეგ წარმოებს მათი

გარდაქმნა გამომავალ რაოდენობრივ პარამეტრებში, რომლებიც შეესაბამება შემოთავაზებული სერვისების სარგებლიანობას და მათი უზრუნველყოფის ღირებულებას.

ინვესტიციების განხილვა ასეთ კონტექსტში მნიშვნელოვნად აადვილებს მოსალოდნელი სარგებლის პოვნას და შესაბამისად ROI მაჩვენებლის განსაზღვრას. ასეთი მიდგომის სხვა შედეგია მრავალფეროვანი, ცოდნის თვალსაზრისით, კროს-ფუნქციური გუნდების შექმნა, რომლებიც ინაწილებენ ერთმანეთში პასუხისმგებლობას პროექტის წარმატების მიზნით. ამ შემთხვევაში ადამიანები სხვადასხვა განყოფილებიდან მუშაობენ ერთად და არავის შეუძლია პასუხისმგებლობა დააკისროს მხოლოდ IT-ს ან – პირიქით, რადგან აშკარაა ადამიანთა ურთიერთპასუხისმგებლობა.

ITIL-ში წარმოდგენილია ROI-ს სამი მიდგომა:

• ბიზნეს-კეისი – ესაა ბიზნესის საკვანძო ასპექტების განსაზღვრა, რომლებიც დამოკიდებულია სერვის-მენეჯმენტზე;

• წინასაპროგრამო ROI – ესაა ტექნიკა ინვესტიციის რაოდენობრივი ანალიზისთვის სერვის-მენეჯმენტში (გამოიყენება ინვესტირებამდე);

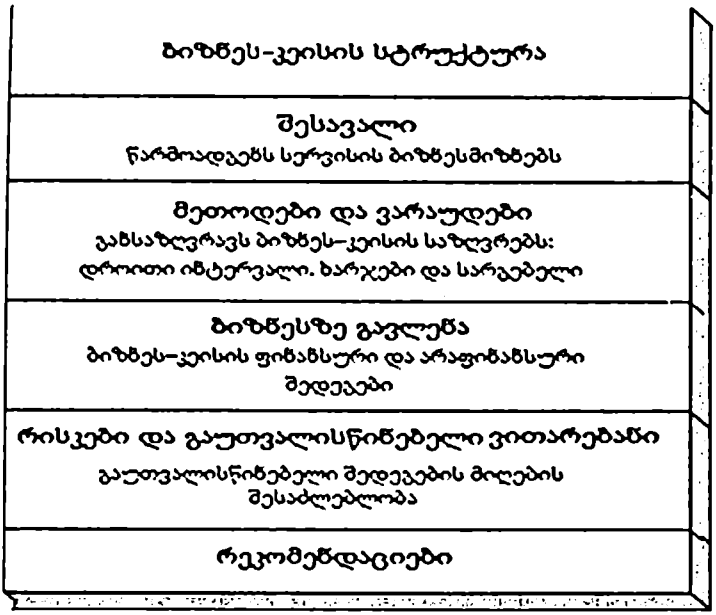
• პოსტსაპროგრამო ROI – ესაა ტექნიკა ინვესტიციის ანალიზისთვის სერვის-მენეჯმენტში, ფაქტი.

12.4.1. ბიზნეს-კეისი

ბიზნეს-კეისი – ესაა რომელიმე მნიშვნელოვანი ხარჯების მუხლების დასაბუთება. შეიცავს ინფორმაციას ხარჯების, სარგებლის, რეალიზაციის ვარიანტების, სირთულეების, რისკების და შესაძლო პრობლემების შესახებ [11].

ფაქტობრივად, ბიზნეს–კეისი არის გადაწყვეტილების მიღების და დაგეგმვის ინსტრუმენტი, რომელიც აპროგნოზირებს ბიზნესის მოქმედების ყველაზე ალბათურ შედეგებს. შედეგები

შეიძლება აისახოს რაოდენობრივად და ხარისხობრივად. ნახაზზე მოცემულია ბიზნეს-კეისის სტრუქტურა "Service Strategy" პუბლიკაციიდან:



ნახ.12.10. ბიზნეს-კეისის სტრუქტურა

ბიზნესის მიზნები, როგორც წესი, განისაზღვრება საკმაოდ ზოგადად. გამოყოფენ შემდეგი ტიპის მიზნებს:

1. ოპერაციული: მინიმიზირდეს რისკები, ამაღლდეს ეფექტიანობა, ამაღლდეს მწარმოებლურობა და ა.შ.

2. ფინანსური: ხარჯების თავიდან აცილება, შემოსავლების გაზრდა აქტივებიდან, გამომუშავების გაზრდა და ა.შ.

3. სტრატეგიული: კონკურენტუნარიანი პროდუქციის წარმოდგენა, დამკვეთთა დაკმაყოფილების გაუმჯობესება, ხარისხის ამაღლება და ა.შ.

4. დარგობრივი: პოზიციის გაუმჯობესება ბაზარზე, ლიდერის პოზიციის დაკავება ბაზარზე და ა.შ.

თუ კომპანია ყიდულობს სერვისს, იგი იმედოვნებს მიიღოს მისგან მხარდაჭერა დასმული მიზნების მისაღწევად. დანერგილი სერვისი ახდენს ბიზნესზე განსაზღვრულ გავლენას, რომელსაც არა აქვს მნიშვნელობა გარკვეულ ბიზნეს-მიზნებთან მიბმის გარეშე.

12.4.2. წინაპროგრამული ROI

სერვის-მენეჯმენტი ზოგჯერ ითხოვს გრძელვადიან ფინანსურ დაგეგმვას. გრძელვადიანი ხარჯების ბიუჯეტის შედგენა იყოფა ორ დიდ კატეგორიად:

- შერჩევითი გადაწყვეტილებები;
- გადაწყვეტილებები პრივილეგიების განაწილებით.

პირველი მათგანი გულისხმობს გადაწყვეტილების მიღებას იმის შესახებ, გავა თუ არა სერვის–მენეჯმენტის მიერ შემოთავაზებული ინიციატივა დადგენილ საზღვარზე, მაგალითად, მინიმალური ამონაგების მიღება. ამ ეტაპზე განისაზღვრება სრულად, გამოსადეგია თუ არა საინვესტიციო პროექტი შემდგომი განხილვისათვის. გადაწყვეტილებები შერჩევით ითვალისწინებს საინვესტიციო პროექტების რანჟირებას და პრივილეგიების განაწილებას.

არსებობს ორი მიდგომა გადაწყვეტილების მისაღებად გრძელვადიანი კაპიტალდაბანდების შესახებ:

- წმინდა დისკონტირებული შემოსავალი (Net Present Value – NPV) – ესაა ჯამი გადასახდების ნაკადის დისკონტირებული მნიშვნელობებისა, დაყვანილი დღევანდელ დღემდე. გამოსადეგია

გადაწყვეტილების მისაღებად საინვესტიციო პროექტების შერჩევისას;

- შემოსავლიანობის შიგა ნორმა (Internal Rate of Return – IRR) – ესაა საპროცენტო განაკვეთი, რომლის დროსაც წმინდა დისკონტირებული შემოსავალი (NPV) 0-ის ტოლია. გამოიყენება გადაწყვეტილების მისაღებად პრივილეგიების განაწილებისას.

NPV მაჩვენებელი არის სხვაობა ყველა ფულადი შემოსავლების და გასავლების, დაყვანილი დროის მოცემულ მომენტამდე (საინვესტიციო პროექტის განხილვის მომენტისთვის). იგი უჩვენებს ფულადი სახსრების ოდენობას, რომლის მიღებასაც ინვესტორი ელოდება პროექტიდან, მას შემდეგ, რაც ფულადი შემოსავლები ამოისყიდიან მის პირველსაწყის საინვესტიციო ხარჯებს და პერიოდულ ფულად გასავლებს, დაკავშირებულს პროექტის შესრულებასთან. ორი ნაკადის სხვაობის მნიშვნელობა – კაპიტალდაბანდება და მოგება – განსაზღვრავს, შესაფერისია თუ არა მოცემული საინვესტიციო პროექტი:

- თუ NPV–ს აქვს დადებითი მნიშვნელობა, მაშინ მოცემული საინვესტიციო პროექტი მისაღებია. იგი ეკონომიურად ეფექტურია, რადგან გვპირდება უფრო მეტის მოტანას, ვიდრე ინვესტიციების ამოგების მოთხოვნილი პროცენტია.
- თუ NPV ნულის ტოლია, მოცემული საინვესტიციო პროექტი ასევე მისაღებია. იგი გვპირდება ინვესტიციების ამოგების მოთხოვნილი პროცენტის მიღებას.
- თუ NPV უარყოფითია, მაშინ ინვესტიციის პროგრამა უადგილოა. იგი ვერ მოიტანს ამოგების მოთხოვნილი %–ის სასურველ მნიშვნელობას.

მსხვილი კომპანიები, ჩვეულებისამებრ, აფიქსირებენ ინვესტიციის ამოგების სავალდებულო პროცენტს. ესაა გასაშუალებული მნიშვნელობა (პროცენტებში ან წილებში),

რომელიც კომპანიამ უნდა გადაუხადოს მეპაიეებს ან კრედიტორებს მათი კაპიტალის გამოყენების გამო. ინვესტიციების ამოგების მოთხოვნილი პროცენტის მნიშვნელობა ფაქტობრივად არის ზღვარი გადაწყვეტილების მიღებას, ინვესტიციების რენტაბელობის შესახებ.

NPV ცუდად ერგება საინვესტიციო პროექტების რანჟირებას, ანუ გადაწყვეტილების მიღების პრივილეგიებით. მისი გამოყენება შეიძლება მხოლოდ ერთნაირი ინვესტიციების პირობებში, რაც პრაქტიკაში იშვიათად ხდება. გადაწყვეტილების მისაღებად რანჟირების მიხედვით შემოთავაზებული ალტერნატივებისათვის უკეთესია IRR-ის გამოყენება.

გავიმეორებთ, რომ IRR – ესაა საპროცენტო განაკვეთი, რომლის დროსაც წმინდა დისკონტირებული შემოსავალი (NPV) ტოლია 0-ის. ყველაზე მარტივი ხერხი IRR-ის გასათვლელად:

IRR = საჭირო ინვესტიციები/წმინდა ყოველწლიური ინვესტიციები

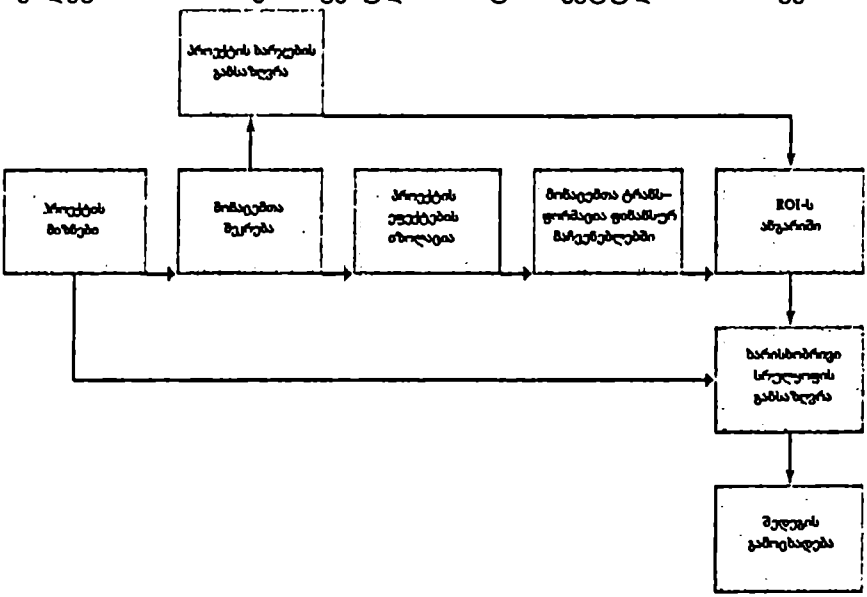
მიღებული IRR მნიშვნელობით გამოითვლება უკუგების პროცენტი (მითითებული პერიოდით, ჩვეულებრივად, 5 წელი), რომელიც შეუდარდება მოთხოვნილ ამოგების პროცენტს ამ კომპანიისთვის. თუ ის ნაკლებია, მაშინ საინვესტიციო პროექტი უსარგებლოა.

ამგვარად, საინვესტიციო გადაწყვეტილებების მისაღებად IRR გამოიყენება ალტერნატიული ინვესტიციების ამოგების პროცენტების გასაანგარიშებლად. საბოლოოდ უნდა ამოირჩეს საინვესტიციო პროექტი, რომელსაც IRR–ის მაქსიმალური მნიშვნელობა აქვს.

12.4.3. პოსტპროექტული ROI

მრავალი კომპანია ნერგავს სერვის-მენეჯმენტის მიერ წარმოდგენილ გადაწყვეტილებებს, ინვესტიციების სარგებლია-

წარის წინასწარი გაანგარიშების გარეშე. მიუხედავად ამისა, სასურველი მიზნებისა და მიღწეული შედეგების გასაგები ფინანსური განსაზღვრის გარეშე, მათ არ შეუძლიათ ფასეულობის გაზომვა, რომელიც მიიღეს ინვესტირების შედეგად. უფრო მეტიც, სერვისის გამოყენების განსაზღვრულ ეტაპზე შეიძლება საჭირო გახდეს დამატებითი საშუალებების ჩადება და ინვესტორებს მოუნდებათ ფინანსური დასაბუთების მიღება ამ დაბანდებების აუცილებლობაზე. პოსტპროექტული ROI-ს დანიშნულებაა ინვესტიციების ეფექტურობის განსაზღვრა მათი დაბანდების შემდეგ. 3.11 ნახაზზე მოცემულია პოსტპროექტული ROI-ს სქემა.



ნახ.12.11. პოსტპროექტული ROI–ს სქემა

დასაწყისში უნდა განისაზღვროს საინვესტიციო პროექტის მიზნები. ისინი შეიძლება იყოს სხვადასხვა, მაგალითად, „გაუმჯობესდეს სერვისის ხარისხი“, „დაინერგის საუკეთესო

საწარმოო პრაქტიკა", „შემცირდეს საკუთრების საერთო ღირებულება" და ა.შ.

მონაცემთა შეკრება ROI–ს ანგარიშის მნიშვნელოვანი ეტაპია, რადგან მასზეა დამოკიდებული მიღებული შედეგის კორექტულობა და სიზუსტე. ინვესტირების მიზნები გვეხმარება აუცილებელ მონაცემთა წყაროების და მათი ბუნების განსაზღვრაში. მაგალითად, სერვისის ხარისხის შეფასების პარამეტრები ან კლიენტების გამოკითხვის ანკეტები მათი დაკმაყოფილების დონის შესახებ.

შემდეგ უნდა მოხდეს საინვესტიციო პროექტის შედეგების იზოლირება. გამოიყენება რამდენიმე მეთოდი:

1. **პროგნოზირება.** ამ მეთოდში ყველაზე ხშირად აგებენ ტრენდულ ხაზს, რათა პროგნოზირებულ იქნას, თუ რა მოხდებოდა, რომ საანალიზო საინვესტიციო პროექტი არ დანერგილიყო. ეს მეთოდი გვაძლევს მაჩვენებლების რაოდენობრივი მნიშვნელობების მიღების საშუალებას;

2. **გავლენის შეფასება.** არსებობს შემთხვევები, როცა პროგნოზირების გამოყენება შეუძლებელია, შესავალი მონაცემების არარსებობის გამო, ან მათი გაზომვის სირთულის გამო. ამ დროს იყენებენ გავლენის შეფასების მეთოდს. მარტივ შემთხვევაში, დამკვეთების და ინვესტორები განსაზღვრავენ სრულყოფის დონეს, რომელიც უნდა მოიტანოს საინვესტიციო პროექტის დანერგვამ.

3. **საკონტროლო ჯგუფი.** ტექნიკა გულისხმობს საინვესტიციო პროექტის რეალიზაციას ორგანიზაციის რომელიმე ნაწილში. მიღებული მწარმოებლურობა შეუდარდება ორგანიზაციის სხვა ნაწილებს, რომლებიც არ მონაწილეობდნენ ექსპერიმენტში.

შემდეგ, იმისთვის, რომ გაითვალონ ROI, მიღებული მონაცემები უნდა მიიყვანონ ფინანსურ მაჩვენებლებამდე. ასეთი მიყვანის ტექნიკა დამოკიდებულ იქნება კონკრეტულ მონაცემებზე.

შედეგების რაოდენობრივი შეფასების მიღების შემდეგ აუცილებელია, შეფასდეს პროექტში მთლიანი ინვესტიციები. ისინი მოიცავს: დაგეგმვის, პროექტირების და რეალიზაციის ხარჯებს, მოწყობილობის ხარჯებს, სწავლების ხარჯებს. შემდეგ ROI გაითვლება ზემოთ აღწერილი ერთ-ერთი მეთოდით: NPV ან IRR სიტუაციის მიხედვით.

ამგვარად, სტრატეგიის განსაზღვრის ეტაპზე IT–ორგანიზაცია გამოავლენს ფასეულობას, რომელიც შეუძლია მოუტანოს ბიზნესს, და მოიფიქრებს, თუ როგორ მოახდინოს ამ ფასეულობის რეალიზაცია კონკრეტული სერვისების სახით. ინსტრუმენტად სერვისების გამოვლენისთვის, რომელთაც შეუძლია ფასეულობის მოტანა, მოიაზრება სერვისების პორტფელის მართვის პროცესი. კატალოგი სერვისებისა, რომლებიც მიმწოდებელს შეუძლია შესთავაზოს ახლავე – ახალი სერვისების დამუშავება, არსებული სერვისების სრულყოფა, შესაძლებლობა სერვისების გადაცემისა აუტსორსინგზე და ა.შ. ეს ყველაფერი მოთავსებულია სერვისების პორტფელში, რომელიც ასახავს IT–ორგანიზაციის სტრატეგიას და პოტენციალს.

სტრატეგიის ფორმირებისას სერვისების მიმწოდებელი ყურადღებას უნდა უთმობდეს ფინანსურ მხარეს: სწორად განსაზღვროს სერვისის ფასეულობა, გაითავისოს (გაიგოს) და გაზომოს სერვისის უზრუნველყოფის სრული ფასი, გაიგოს, თუ რა მოგების მიღება შეუძლია თვითონ მას, ინვესტორებს და დამკვეთებს.

13. სერვისების დაპროექტება, როგორც სერვისების სასიცოცხლო ციკლის ეტაპი

13.1. სერვისების დაპროექტება, როგორც სასიცოცხლო ციკლის ეტაპი

სერვისების სასიცოცხლო ციკლში სტრატეგიის აგების ეტაპის შემდეგ ხორციელდება სერვისების დაპროექტება. ამ ეტაპის ძირითადი მიზანია ახალი სერვისების დაპროექტება ან ცვლილებების შეტანა არსებულ სერვისებში. ძირითადი ამოცანები სერვისების დაპროექტების ეტაპზე შემდეგია:

1. სერვისების დაპროექტება, რომელთაც ძალუძს ბიზნესის დახმარება დაგეგმილი შედეგების მისაღწევად;

2. პროცესების დაპროექტება, რომლებიც მხარს უჭერს სერვისების სასიცოცხლო ციკლს;

3. რისკების იდენტიფიკაცია და მათი მართვა;

4. უსაფრთხოების და მდგრადობის დაპროექტება IT -ინფრასტრუქტურის, მოწყობილობის, აპლიკაციის, ინფორმაციული რესურსების;

5. მეთოდების და მეტრიკების დაპროექტება აზომვებისთვის;

6. გეგმების, პროცესების, პოლიტიკის, სტანდარტების, არქიტექტურის და დოკუმენტების შექმნა, რომლებიც ხელს შეუწყობს ხარისხიანი IT–გადაწყვეტის დაპროექტებას და მათ მართვას;

7. სხვადასხვა შესაძლებლობების და ჩვევების განვითარება IT–სფეროში;

8. სერვისების ხარისხის სრულყოფის ხელშეწყობა.

ახალი სერვისებისათვის მოთხოვნები ფორმირდება წესისამებრ, სერვისების პორტფელის მონაცემების საფუძველზე და ბიზნესის მოთხოვნილებებით. სერვისების დაპროექტება იწყება

ბიზნესის მოთხოვნების ერთობლიობის აგებით და სრულდება გადაწყვეტილების შემუშავებით, რომელიც შეძლებს ამ მოთხოვნების დაკმაყოფილებას და დაეხმარება ბიზნესს დაგეგმილი შედეგების მიღწევაში. ნაპოვნი გადაწყვეტა საპროექტო დოკუმენტაციასთან ერთად გადადის დანერგვის ეტაპზე, ახალი/შეცვლილი სერვისის გაშვების, ტესტირების ან განვითარებისთვის.

სერვისის საპროექტო დოკუმენტაცია (Service Design Package ან SDP) – ესაა დოკუმენტები, რომლებიც განსაზღვრავს სერვისის ყველა ასპექტს და მოთხოვნებს მასთან სასიცოცხლო ციკლის ყველა ეტაპზე. მოთხოვნის რეალიზაციამდე საპროექტო დოკუმენტაციაში, იგი უნდა იქნას გაანალიზებული, ფორმალიზებული და მხარდაჭერილი ხელმძღვანელობის მიერ.

ყველა ცვლილება არ ითხოვს სერვისების სასიცოცხლო ციკლში დაპროექტების ეტაპის ქმედებათა ჩართვას. დაპროექტება საჭიროა, როცა აუცილებელია „მნიშვნელოვანი“ ცვლილებები. ორგანიზაციამ უნდა განსაზღვროს თავისი „მნიშვნელოვანი ცვლილებების“ ერთობლიობა, რათა ორგანიზაციის ყოველმა თანამშრომელმა გაიგოს, თუ როდისაა საჭირო პროექტირება. ანუ, აბსოლუტურად ყველა ცვლილება უნდა იქნას შეფასებული „მნიშვნელობის“ მხრივ დაპროექტების კონტექსტში. ასეთი შეფასება არის ცვლილებების მართვის პროცესის ნაწილი.

დაპროექტების ეტაპზე დამუშავებული გადაწყვეტა უნდა შეესაბამებოდეს კორპორაციის და IT–ის პოლიტიკას. ამიტომაც დაპროექტებისას აუცილებელია სტრატეგიის და შეზღუდვების გათვალისწინება, რომლებიც სტრატეგიის აგების ეტაპზეა ფორმირებული.

საინტერესოა, რომ ITIL–ში გამოფილია ოთხი „P" სერვისების დაპროექტების ეტაპისთვის, ისევე როგორც სტრატეგიის აგების ეტაპისთვის:

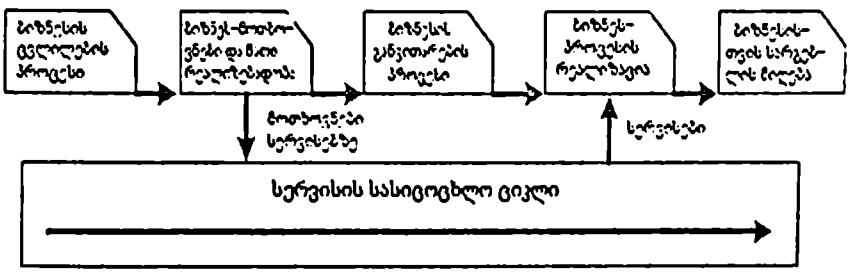
• პერსონალი – ადამიანები, ჩვევები და კვალიფიკაცია საჭირო სერვისების უზრუნველსაყოფად;

• პროდუქტები – ტექნოლოგიები და მართვის სისტემები გამოყენებული სერვისების უზრუნველსაყოფად;

• პროცესები – პროცესები, როლები და ქმედებები ჩართული სერვისების უზრუნველსაყოფად;

• პარტნიორები – ვენდორები, მიმწოდებლები და მწარმოებლები, რომლებიც მხარს უჭერენ და ეხმარებიან სერვისებით უზრუნველყოფას.

სერვისების დაპროექტება გლობალური გაგებით არის ბიზნესის ცვლილების საერთო პროცესის ნაწილი. ბიზნესის ცვლილების პროცესი და IT–ის როლი მასში მოცემულია 13.1 ნახაზზე.



ნახ.13.1. ბიზნესის ცვლილების პროცესი

დაპროექტების ძირითადი როლი ბიზნესის ცვლილების პროცესის კონტექსტში მდგომარეობს ინოვაციური სერვისების დამუშავებაში (მათ შორის არქიტექტურა, პროცესი, პოლიტიკა და

დოკუმენტაცია), რომლებიც შეძლებენ დააკმაყოფილონ ბიზნესის დღევანდელი და სამომავლო მოთხოვნილებანი. ამ დროს ITSM-ის საკვანძო პროცესები უნდა იქნას გამოყენებული ახალი სერვისების დამუშავების ან არსებულში ცვლილებების შეტანის დასაწყისშივე. ქვემოთ მოყვანილია ქმედებათა ერთობლიობა, რომელთა განხორციელება აუცილებელია პროექტირების ეტაპზე იმისთვის, რომ დამუშავებულმა გადაწყვეტამ ეფექტურად დააკმაყოფილოს ბიზნესის მოთხოვნილებანი:

1. ახალი გადაწყვეტა უნდა იქნას დამატებული სერვისების პორტფელში უკვე კონცეფციის ფორმირების სტადიაზე. სერვისების პორტფელი რეგულარულად უნდა განახლდეს, რათა იგი ასახავდეს ნებისმიერი, თუნდაც უმნიშვნელო ცვლილების აქტუალურ სტატუსს ინკრემენტალური და იტერაციული განვითარების ჩარჩოებში.

2. სერვისის / სისტემის საწყისი ანალიზის ჩარჩოებში აუცილებელია მოთხოვნების გაგება სერვისების დონის მიმართ. მოთხოვნები სერვისების დონის მიმართ (**Service Level Requirements** ან SLR) – ესაა დამკვეთის მოთხოვნა IT-სერვისზე. SLR–ები გაზირდება ბიზნესმიზნებზე და გამოიყენება მოლაპარაკებებისას და სერვისების დონის მიზნობრივი მაჩვენებლების შეთანხმებისათვის.

3. იყენებს რა SLR–ს, სიმძლავრეების მართვის გუნდს შეუძლია ახალი სერვისის მოდელირება არსებული ინფრასტრუქტურის გამოყენებით და იმის გაგება, შეძლებს თუ არა იგი ამ სერვისის მხარდაჭერას მომავალში. თუ დრო საშუალებას იძლევა, მოდელირების შედეგები აისახება სიმძლავრეების უზრუნველყოფის გეგმაში. სიმძლავრეების უზრუნველყოფის გეგმა (**Capacity Plan**) გამოიყენება რესურსების მართვისთვის, რომლებიც აუცილებელია IT–სერვისის უზრუნველსაყოფად. ეს

გეგმა შეიცავს სცენარებს მოთხოვნილების პროგნოზირებისათვის ბიზნესის მხრიდან, და ხარჯების შეფასებას, რომლებიც აუცილებელია სერვისის დონის შეთანხმებული მიზნობრივი მაჩვენებლების უზრუნველსაყოფად.

4. თუ ახალი სერვისის უზრუნველსაყოფად ან არსებული სერვისის გაფართოების მხარდასაჭერად საჭიროა ახალი ინფრასტრუქტურები, მაშინ აუცილებელია ფინანსების მართვის პროცესის მონაწილეობა.

5. ბიზნესზე გავლენის ანალიზი და რისკების შეფასება სერვისთან მიმართებით უნდა ჩატარდეს ადრე, სიმძლავრეების დაგეგმვის, წვდომის, დაპროექტების და უწყვეტობის სტრატეგიის ფორმირების ეტაპების წინ.

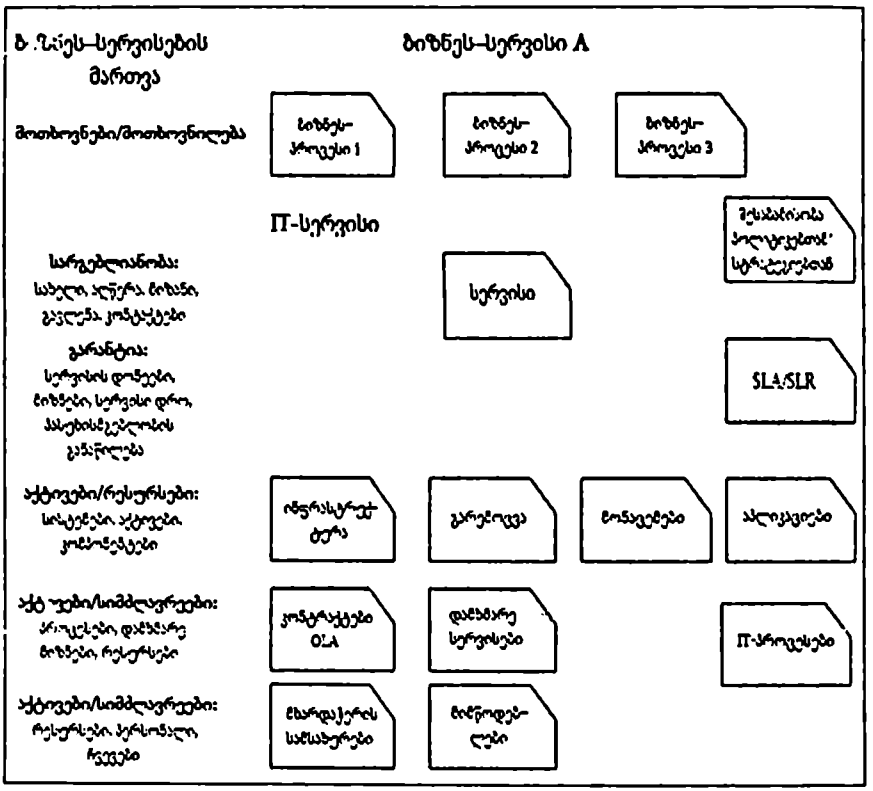
6. სამაგიდო-სერვისის მომსახურე პერსონალი წინასწარ უნდა ემზადებოდეს ახალი სერვისების დასანერგად, კერძოდ, შეასწავლოს თავის პერსონალს.

7. დანერგვის ეტაპი შეიძლება დაიწყოს რეალიზაციის დაგეგმვით და ცვლილებათა ცხრილის აგებით.

8. თუ ახალ სერვისს სჭირდება დამატებითი მომარაგება, საჭიროა მიმწოდებლების მართვის პროცესის ჩართვა.

მიმწოდებლების მართვა (Supplier Management) – ესაა პროცესი, რომელიც პასუხისმგებელია იმის უზრუნველყოფაზე, რომ ხელშეკრულებები მიმწოდებლებთან შეესაბამება ბიზნესის მოთხოვნებს, და ყველა მიმწოდებელი ასრულებს თავის საკონტაქტო ვალდებულებას.

სერვისი და მისი კომპონენტები მოცემულია 13.2 ნახაზზე.



ნახ.13.2. სერვისი და მისი კომპონენტები

გადაწყვეტების მოსაძებნად და შესაქმნელად, რომლებიც შეძლებენ ბიზნესის ახალი და არსებული მოთხოვნილებების დაკმაყოფილებას, სერვისის დაპროექტებამ უნდა გაითვალისწინოს შემდეგი ასპექტები:

1. ბიზნესპროცესი – ფუნქციური მოთხოვნილებების განსაზღვრა, რომლებისთვისაც წარედგინება სერვისი. მაგალითად, ტელეგაყიდვები ან ანგარიშფაქტურის შედგენა;

2. სერვისი – თვითონ სერვისი, რომელიც წარედგინება ბიზნესს დასანახავად;

3. SLA/SLR: დოკუმენტები, შეთანხმებული დამკვეთთან, რომლებიც განსაზღვრავს სერვისის დონეს, არეალს და ხარისხს;

4. ინფრასტრუქტურა – ყველა მოწყობილობა, რომლებიც აუცილებელია მომხმარებლის უზრუნველსაყოფად სერვისით, მათ შორის სერვერები, მარშრუტიზატორები, კონცენტრატორები, ტელეფონები, კომპიუტერები და სხვ.;

5. გარემო – გარემო, რომელიც აუცილებელია ინფრასტრუქტურის უსაფრთხო ექსპლუატაციისათვის: ჰაერის კონდიცირება, ელექტრობა და ა.შ.

6. მონაცემები – მონაცემები, რომლებიც საჭიროა სერვისის მხარდასაჭერად, აგრეთვე ბიზნესპროცესების უზრუნველსაყოფად აუცილებელი ინფორმაციით. მაგალითად, კლიენტთა სია, საბუღალტრო რეგისტრი;

7. აპლიკაცია – ყველა პროგრამული დანართი, რომლებიც აუცილებელია მონაცემთა მართვისათვის და ბიზნესპროცესების ფუნქციური მოთხოვნების დასაკმაყოფილებლად;

8. მხარდამჭერი სერვისები: ნებისმიერი დამხმარე სერვისები, რომლებიც აუცილებელია სერვისების უზრუნველსაყოფად;

9. ოპერაციული დონის შეთანხმება და კონტრაქტები – ნებისმიერი შეთანხმება, რომელიც აუცილებელია ხარისხიანი სერვისის უზრუნველსაყოფად, რომელიც შეთანხმებულია SLA-ზე;

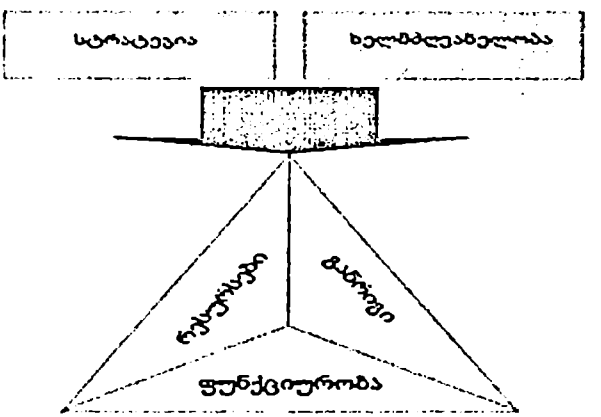
10. მხადაჭერის სამსახურები – ნებისმიერი შიგა გუნდი, რომელიც უზრუნველყოფს კომპონენტების მხარდაჭერის პირველ და მეორე ხაზებს, რაც აუცილებელია სერვისის უზრუნველსაყოფად, მაგალითად, Unix ან ქსელები;

11. მიმწოდებლები – პროცესის ნებისმიერი გარე მონაწილეები, რომლებიც უზრუნველყოფენ კომპონენტების

მხარდაჭერის მესამე და მეოთხე ხაზებს, რაც აუცილებელია სერვისის უზრუნველსაყოფად – ქსელი, აპარატული და პროგრამული უზრუნველყოფა.

დაპროექტებამ უნდა განიხილოს ზემოჩამოთვლილი თითოეული ასპექტი კომპლექსურად, და არა იზოლირებულად. იმისათვის, რომ შედეგად მიიღონ კონკურენტუნარიანი გადაწყვეტა, ბიზნესის მოთხოვნებისის დამაკმაყოფილებელი, აუცილებელია მითითებული კომპონენტების ურთიერთ-კავშირების და ურთიერთდამოკიდებულებების გათვალისწინება.

სერვისების დაპროექტებისას ბიზნესის ახალი მოთხოვნებით გათვალისწინებულ უნდა იქნას ამ მოთხოვნების არა მხოლოდ ფუნქციური მდგენელი. შემოთავაზებული გადაწყვეტა ამ ეტაპზე უნდა უზრუნველყოფდეს ბიზნესისთვის გეგმიურ მწარმოებლურობას. აუცილებელია ყველაფრის გაკეთება არსებული რესურსების გათვალისწინებით, ხარჯების და დროის დადგენილ საზღვრებში. ამგვარად, მენეჯერები მუშაობენ სამი მდგენელით (ნახ.13.3):



ნახ.13.3. დაპროექტების სამი მდგენელი

- ფუნქციურობა: სერვისი, მისი ფუნქციური შესაძლებლობები, უნარები და ხარისხი.
- რესურსები: ხელმისაწვდომი ადამიანები, ტექნოლოგიები და ფული.
- განრიგი: დროითი საზღვრები.

დაპროექტების დანიშნულებაა ბალანსის დაცვა ამ სამ მდგენელს შორის, ბიზნესის მოთხოვნილებათა მაქსიმალურად დაკმაყოფილების მიზნით, რომლებიც მუდმივად იცვლება. სამიდან ერთ–ერთის შეცვლა მოქმედებს დარჩენილიდან ერთ–ერთზე მაინც აუცილებლად, ან ორივეზე.

ეფექტური გადაწყვეტების დასამუშავებლად სერვისების მიმწოდებლებისთვის მეტად მნიშვნელოვანია ბიზნესის მამოძრავებელი ფაქტორების გაგება და მათი მოთხოვნილებანი. დაპროექტება ხშირად აღიქმება მხოლოდ როგორც სტადია, რომელიც წინ უსწრებს ექსპლუატაციას.

ITIL–ში მიდგომა სხვაგვარადაა, დაპროექტებამ არა მხოლოდ უნდა შემოგვთავაზოს ახალი გადაწყვეტები, არამედ უნდა უზრუნველყოს კიდევაც ამ გადაწყვეტების ეფექტური მართვის შესაძლებლობა მთელი სასიცოცხლო ციკლის განმავლობაში.

თუ გავაერთიანებთ ყველაფერ ზემოთქმულს, მაშინ დაპროექტებისადმი ერთიანი და სწორი მიდგომა უნდა ითვალისწინებდეს სერვისების დამუშავებას მართვის და სრულყოფის მექანიზმებითა და ფუნქციებით სასიცოცხლო ციკლის ყველა ეტაპზე.

ადამიანები, რომლებიც პასუხისმგებლები არიან დაპროექტების მართვაზე, უნდა იყვნენ დარწმუნებულნი იმაში, რომ უზრუნველყოფილია შემდეგი:

1. კარგი ურთიერთკავშირების არსებობა სხვადასხვა ქმედებებს შორის დაპროექტების ჩარჩოებში და სხვა ნაწილებთან, მაგ., შორის IT და ბიზნესის გეგმებთან და სტრატეგიებთან;

2. ბიზნესის ბოლო გეგმების და სტრატეგიების ვერსიათა წვდომა მათთვის, ვინც მონაწილეობს დაპროექტებაში;

3. საპროექტო დოკუმენტაციის შესაბამისობა ბიზნესის და IT-ის გეგმებთან და სტრატეგიებთან;

4. არქიტექტურა და დიზაინი არის:

o მოქნილი, ამგვარად, შეუძლიათ სწრაფი რეაგირება ბიზნესის ახალ მოთხოვნილებებზე;

o ინტეგრირებულია ბიზნესის და IT-ის ყველა სტრატეგიასა და პოლიტიკასთან;

o მხარს უჭერს სერვისის სასიცოცხლო ციკლის სხვა სტადიების მოთხოვნილებებს;

o თანამოქმედებენ ახალი სერვისების წინსვლისთვის ან არსებულის ცვლილებებისთვის, ბიზნესის მოთხოვნილების შესაბამისად.

დაპროექტების ერთ–ერთი ქვეეტაპია ბიზნესისა და მისი დრაივერების მოთხოვნილებათა განსაზღვრა და შემდგომი დოკუმენტირება. დრაივერებში აქ იგულისხმება რომელიღაც მოძრავი ბიზნესფაქტორები: ადამიანები, ინფორმაცია და ამოცანები, რომლებიც უზრუნველყოფენ დასმული მიზნების მიღწევას. დაპროექტების პროცესების რეგულირებისთვის ინფორმაცია იყოფა ორ კატეგორიად:

1. ინფორმაცია მოთხოვნების შესახებ არსებული სერვისებისთვის – არსებულ სერვისებში საჭირო ცვლილებების გათვალისწინებით:

o ახალი ფუნქციური შესაძლებლობები და მოთხოვნები;

- ცვლილებები ბიზნესპროცესებში, დამოკიდებულებებში, პრიორიტეტებში, გავლენასა და კრიტიკულობაში;
- ცვლილებები სერვისის ტრანზაქციების მოცულობაში. ტრანზაქცია (Transaction) – ესაა დისკრეტული ფუნქცია, შესრულებადი IT-სერვისის მიერ. მაგალითად, ფულის გადარიცხვა ერთი საბანკო ანგარიშიდან მეორეზე. ერთი ტრანზაქცია შეიძლება შეიცავდეს მონაცემთა მრავალ დამატებას, წაშლას და ცვლილებას. ამ დროს ყველა უნდა დასრულდეს წარმატებით, წინააღმდეგ შემთხვევაში მათგან არც ერთი არ იქნება შესრულებული (ანუ მთლიანი ტრანზაქცია იქნება გაუქმებული);
- სერვისის დონეების და მისი მიზნობრივი მაჩვენებლების ამაღლებისას ბიზნესის ახალ დრაივერთან დაკავშირებით, ან შემცირება ძველი სერვისებისთვის, რომლებიც მალე იქნებიან ჩანაცვლებული;
- მოთხოვნილებების – სერვისების მართვის პროცესების დამატებითი ინფორმაციის შესახებ.

2. ინფორმაცია მოთხოვნების შესახებ ახალი სერვისებისთვის:

- მოთხოვნილი ფუნქციურობა;
- მენეჯმენტის ინფორმაცია და სხვა მოთხოვნილებანი;
- მხარდაჭერილი ბიზნესპროცესი, დამოკიდებულებები, პრიორიტეტები, გავლენა და კრიტიკულობა;
- სერვისების დონის მოთხოვნები და მიზნობრივი მაჩვენებლები;
- ბიზნესის ტრანზაქციის დონეები, სერვისების ტრანზაქციის დონეები, მომხმარებელთა რაოდენობა და მისი სავარაუდო ზრდა, მომხმარებელთა ტიპები;
- ფინანსური და სტრატეგიული დასაბუთება ბიზნესისთვის;

o ვარაუდი სამომავალო ცვლილებების, ანუ ბიზნესის მომავალი ცნობილი მოთხოვნების შესახებ, ან ზრდის ტემპის ამაღლების შესახებ;

o სიმძლავრის დონე ბიზნესისთვის, რომელიც უნდა იყოს უზრუნველყოფილი.

ესაა ინფორმაციის მინიმალური ნაკრები დაპროექტების ეტაპის დაწყებისთვის. მისი სიზუსტე და აკურატულობა პირველხარისხოვანია. თუ არაკორექტული ან არასწორი ინფორმაცია იქნება გამოყენებული პროექტირების ეტაპზე, მაშინ დამუშავებული სერვისი ვერ დააკმაყოფილებს ბიზნესის მოთხოვნილებებს საბოლოო ჯამში.

მოთხოვნები სერვისებთან უნდა იყოს დოკუმენტირებული. ამისთვის დახარჯული დრო იქნება კომპენსირებული მომავალში კამათის, დისკუსიების და უთანხმოების არარსებობით სერვისის მიმწოდებელსა და დამკვეთს შორის. ბიზნესის მოთხოვნების განსაზღვრის სტადია მდგომარეობს შემდეგში:

1. პროექტის მენეჯერის დანიშვნა, საპროექტო გუნდის შექმნა და ხელმძღვანელობის დამტკიცება ფორმალური და სტრუქტურირებული მეთოდოლოგიის გამოყენებით;
2. ყველა დაინტერესებული პირის იდენტიფიკაცია, შესაბამისი დოკუმენტაციის შედგენა მათი მოთხოვნით და სარგებლიანობით, რომლებსაც ისინი მიიღებენ პროექტის რეალიზაციით;
3. ანალიზი, დოკუმენტირება, პრიორიტეტების განლაგება და მოთხოვნების შეთანხმება;
4. ბიზნესის ბიუჯეტის/სარგებლის გათვლა და დამტკიცება;

5. პოტენციური კონფლიქტების გადაწყვეტა ბიზნეს–ერთეულებს შორის და კორპორატიული მოთხოვნების შეთანხმება;

6. პროცესების განსაზღვრა მოთხოვნების დასამტკიცებლად და დამტკიცებულის შესაცვლელად;

7. ურთიერთმოქმედების გეგმის განვითარება დამკვეთთან, ძირითად დამოკიდებულებათა ხაზგასმა, ხარჯები მიმდინარე მომსახურებაზე და IT-ს შორის, და ის, თუ როგორ მოხდება ამ დამოკიდებულების და აუცილებელი კავშირების დაინტერესებულ მხარეებს შორის მართვა.

მას შემდეგ, რაც მოთხოვნები შეთანხმებული და დამტკიცებულია, მათ გამოუჩნდებათ „შემფასებლები“, ანუ შესაძლებელია კონკრეტული პროექტის ღირებულების გათვლა. საჭიროა ბალანსის დაცვა მათ შორის, რაც ორგანიზაციას შეუძლია თავის თავზე აიღოს, და იმას შორის, რაც მას უნდა. ზოგიერთი მოთხოვნის რეალიზაცია ძალზე ძვირია, ამიტომ ისინი უნდა ამოიშალოს უკვე პროექტირების ეტაპზე. ეს საკითხები უნდა დოკუმენტირდეს და შეუთანხმდეს ბიზნესის წარმომადგენელთან. ჩვეულებისამებრ, სირთულეები წარმოიშობა ბიზნესის სურვილსა და გამოყოფილ ბიუჯეტს შორის, რომელშიც არაა ასახული სერვისის სრული ღირებულება, მაგალითად:

პროექტირებისას გამოყენებული არქიტექტურა და დიზაინი უნდა იყოს ცხადი, ლაკონური, მარტივი და დასაბუთებული. სამწუხაროდ, ისინი ხშირად ძალზე რთულია და აქვთ თეორიული ხასიათი.

13.2. დაპროექტების ძირითადი ასპექტები

გამოიყოფა ხუთი ძირითადი ასპექტი სერვისების დასაპროექტებლად:

1. გადაწყვეტათა დაპროექტება, მათ შორის ყველა საჭირო და შეთანხმებული ფუნქციური მოთხოვნების, რესურსების და შესაძლებლობების;

2. მხარდამჭერი მმართველი სისტემების და ინსტრუმენტების დაპროექტება, კერძოდ, სერვისების პორტფელის სერვისების მართვის და კონტროლისთვის მათი სასიცოცხლო ციკლის ჩარჩოებში;

3. ტექნოლოგიების, მართვის სისტემებისა და ინსტრუმენტების დაპროექტება, რომლებიც აუცილებელია სერვისების უზრუნველსაყოფად;

4. პროცესების დაპროექტება, რომლებიც აუცილებელია სერვისების დიზაინის ასაგებად, დასანერგად, ექსპლუატაციისა და სრულყოფისთვის;

5. მეთოდების და მეტრიკების დაპროექტება სერვისების ხარისხის, ეფექტურობის და მწარმოებლურობის გასაზომად არქიტექტურასა და პროცესებში.

რა თქმა უნდა, დაპროექტების საკვანძო ასპექტია გადაწყვეტათა დამუშავება, რომელიც დააკმაყოფილებს ბიზნესის მოთხოვნილებებს. ყოველთვის, ახალი სერვისის ფორმირებისას, ის უნდა შემოწმდეს ყველა ზემოაღწერილ პუნქტებში. ესაა გარანტია იმისა, რომ იგი კარგად იმუშავებს სხვა სერვისებთან ერთად.

განვიხილოთ დეტალურად ეს ასპექტები.

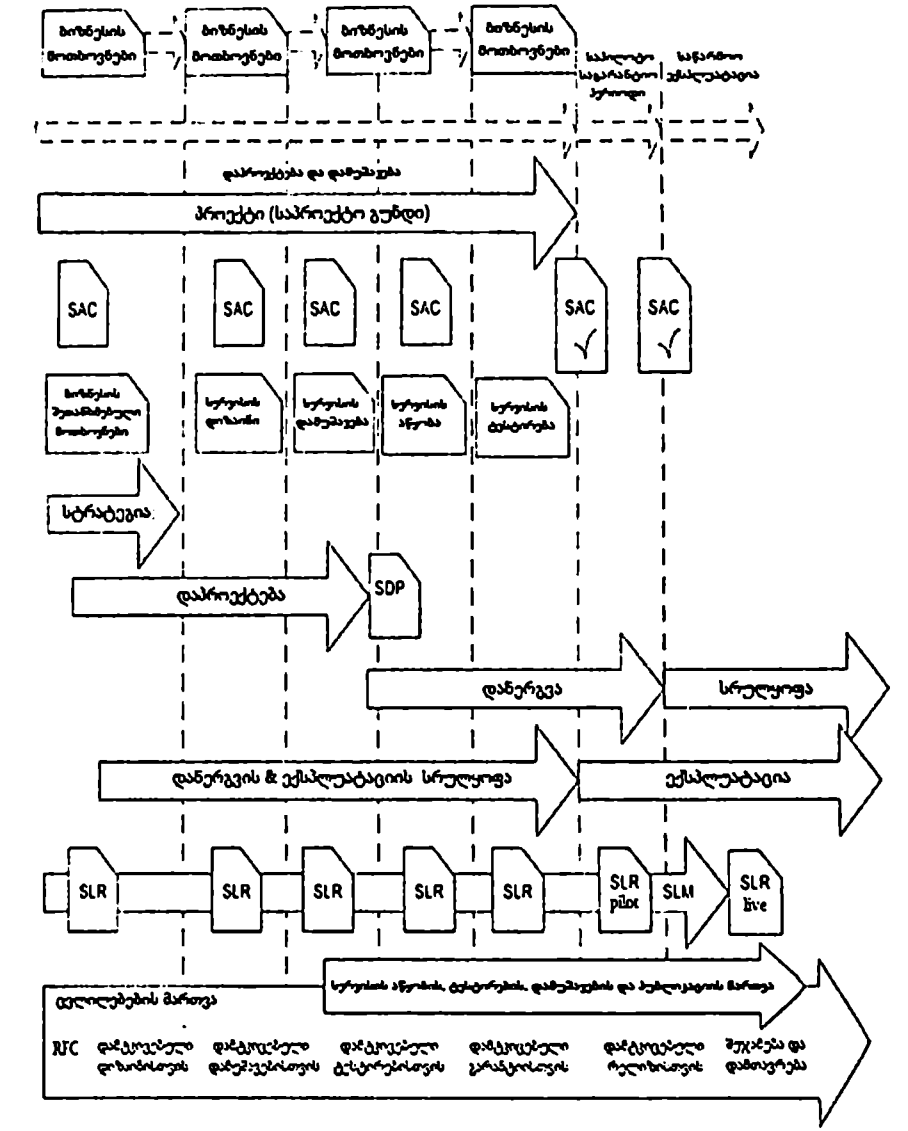
13.2.1. გადაწყვეტათა დაპროექტება

ახალი სერვისის დასაპროექტებლად ან ცვლილებების შესატანად არსებულში აუცილებელია მრავალი ქმედების ჩატარება. პირველ რიგში საჭიროა მკაცრი და სტრუქტურირებული მიდგომა, რომელიც მოგცემს საშუალებას შევქმნათ გადაწყვეტა ოპტიმალური ღირებულებით, ფუნქციონალობით, ხარისხით დროის მოცემულ ინტერვალში.

ეს პროცესი და მისი მდგენელები ნაჩვენებია 13.4 ნახაზზე. მოცემულია სერვისის სასიცოცხლო ციკლი, დაწყებული ბიზნესის ახალი ან შეცვლილი მოთხოვნებით და დამთავრებული მისი დაპროექტებით, დანერგვით და ექსპლუატაციით. მნიშვნელოვანი მომენტია აქ კავშირი ადამიანებს შორის, რომლებიც ექსპლუატაციას უწევენ სერვისს და მის დამპროექტებელს.

ქვემოთ მოყვანილია სფეროები, რომლებიც განხილულ უნდა იქნას გადაწყვეტის დაპროექტების მსვლელობისას:

1. ბიზნესის მოთხოვნების ანალიზი;
2. მიმოხილვა და ანალიზი არსებული სერვისებისა და ინფრასტრუქტურებისა მათი გამოყენების შესაძლებლობის გამოვლენის მიზნით ახალი გადაწყვეტის ჩარჩოებში;
3. ბიზნესციკლები და სეზონური რხევები, მათთან დაკავშირებული ბიზნესის და სერვისების ტრანზაქციათა დონეები, მომხმარებელთა რაოდენობა და მისი სავარაუდო ზრდა, მომხმარებელთა ტიპები;
4. სერვისთა დონის მოთხოვნები და მისი მიზნობრივი მაჩვენებლები, ასევე აუცილებელი ქმედებები სერვისების შეფასებისთვის, ანგარიშგებისა და მიმოხილვისთვის;
5. დროითი ჩარჩოები და საგეგმო შედეგები სერვისის გამოყენების გამო, ასევე მისი გავლენა სხვა სერვისებზე;



ნახ.13.4. სერვისების შექმნა ბიზნესის მოთხოვნების შესაბამისად

6. მოთხოვნების ტესტირებასთან, მათ შორის User Acceptance Testing, აგრეთვე პასუხისმგებლობა ტესტირების შედეგებზე.

- დარწმუნება, რომ Service Acceptance Criteria გათვალისწინებულია და მოთხოვნილი შედეგები ჩართულია საწყის დიზაინში;
- განხილულ და შეფასებულ იქნას არსებული ალტერნატივები, ხაზი გაესვას მათ უპირატესობებს და ნაკლოვანებებს;
- შეთანხმდეს ბიუჯეტი და ხარჯები;
- განხორციელდეს ხელმეორე შეფასება და დამტკიცება სარგებლიანობისა ბიზნესისათვის, მათ შორის ROI-ც;
- შეთანხმდეს არჩეული გადაწყვეტები და საგეგმო შედეგები მათი გამოყენებისას;
- შემოწმდეს, შეესაბამება თუ არა არჩეული გადაწყვეტები კორპორაციასა და IT-ში მიღებულ სტრატეგიებს, გეგმებს, პოლიტიკას და საპროექტო დოკუმენტებს. თუ არა, მაშინ კორექტირდეს ან გადაწყვეტა, ან სტრატეგია (ან სხვა დოკუმენტი). გათვალისწინებულ იქნას, რომ ნებისმიერი ცვლილება სტრატეგიისა გამოიწვევს კოლოსალური შრომის დანახარჯებს და უნდა შესრულდეს სტრატეგიის აგების ეტაპის ჩარჩოებში;
- დავრწმუნდეთ, რომ აუცილებელი და მისაწვდომი კორპორაციის ჩარჩოებში უსაფრთხოების კონტროლი ჩართულია არჩეულ გადაწყვეტაში;
- დასრულდეს IT–ს „ორგანიზაციული მზადყოფნის შეფასება", რათა დავრწმუნდეთ, რომ სერვისის ექსპლუატაციას შეძლებენ ეფექტურად, და ორგანიზაციას აქვს ყველაფერი, რაც აუცილებელია სერვისის შეთანხმებული დონის უზრუნველსაყოფად.

ეს მოიცავს შემდეგს:

1. ბიზნესის და IT–ს პერსპექტივების კომერციული გავლენა ორგანიზაციაზე მთლიანად, მათ შორის ყველა სარგებელი და თანმხლები ხარჯები დამუშავებაზე, დაპროექტებაზე, დანერგვაზე, ასევე ოპერაციული ხარჯები, დაკავშირებული სერვისის მხარდაჭერასთან;

2. რისკების შეფასება და შემცირება, რაც კავშირშია გადაწყვეტის დანერგვასთან;

3. ბიზნესის სტაბილურობა და სიმწიფე. ბიზნესი უნდა დარწმუნდეს, რომ მას აქვს ყველა აუცილებელი პროცესი, სტრუქტურა, როლი, ადამიანები, შესაძლებლობები და პასუხისმგებლობა, რათა მოხდეს ახალი სერვისის ექსპლუატაცია;

4. IT-ის სტაბილურობა და სიმწიფე. IT უნდა დარწმუნდეს, რომ მას აქვს აუცილებელი მოწყობილობა, პირობები, პერსონალი, ვალდებულებები, როლები, დოკუმენტაცია და ინსტრუმენტები სერვისის უზრუნველსაყოფად და მხარდასაჭერად;

5. მიმწოდებლებთან შეთანხმება, რაც აუცილებელია სერვისის უზრუნველსაყოფად;

6. საპროექტო დოკუმენტაციის კომპლექტი, სერვისის შემდგომი დანერგვის, ექსპლუატაციის და სრულყოფისთვის.

13.2.2. მხარდამჭერი სისტემის სერვისების პორტფელის დაპროექტება

ეფექტური ხერხი სერვისების სამართავად მთელი სასიცოცხლო ციკლის განმავლობაში არის სათანადო მართვის სისტემების და ინსტრუმენტების გამოყენება. ძირითადი მართვის სისტემაა სერვისების პორტფელი, რომელიც აღწერს მიმწოდებლის მიერ წარმოდგენილ სერვისს, ბიზნესისთვის ფასეულობის ტერმინებში. იგი ოპერირებს ბიზნესის მოთხოვნილებებით და იმით, თუ რას გვთავაზობს მიმწოდებელი მათზე საპასუხოდ. სერვისების პორტფელი შეიცავს დეტალურ ინფორმაციას ყველა სერვისზე და მათ სტატუსზე სასიცოცხლო ციკლის მიმდინარე ეტაპის ასახვით (ნახ.13.5). ITIL იძლევა რეკომენდაციას, დაუყენდეს სერვისებს შემდეგი სტატუსები:

1. „მოთხოვნები"– მიღებულია მოთხოვნათა ერთობლიობა ბიზნესიდან ან IT-დან ახალი სერვისისთვის ან არსებულის შეცვლისთვის;

2. „განსაზღვრულია" – მოხდა მიღებული მოთხოვნების შეფასება და დოკუმენტირება, შედგენილია SLR;

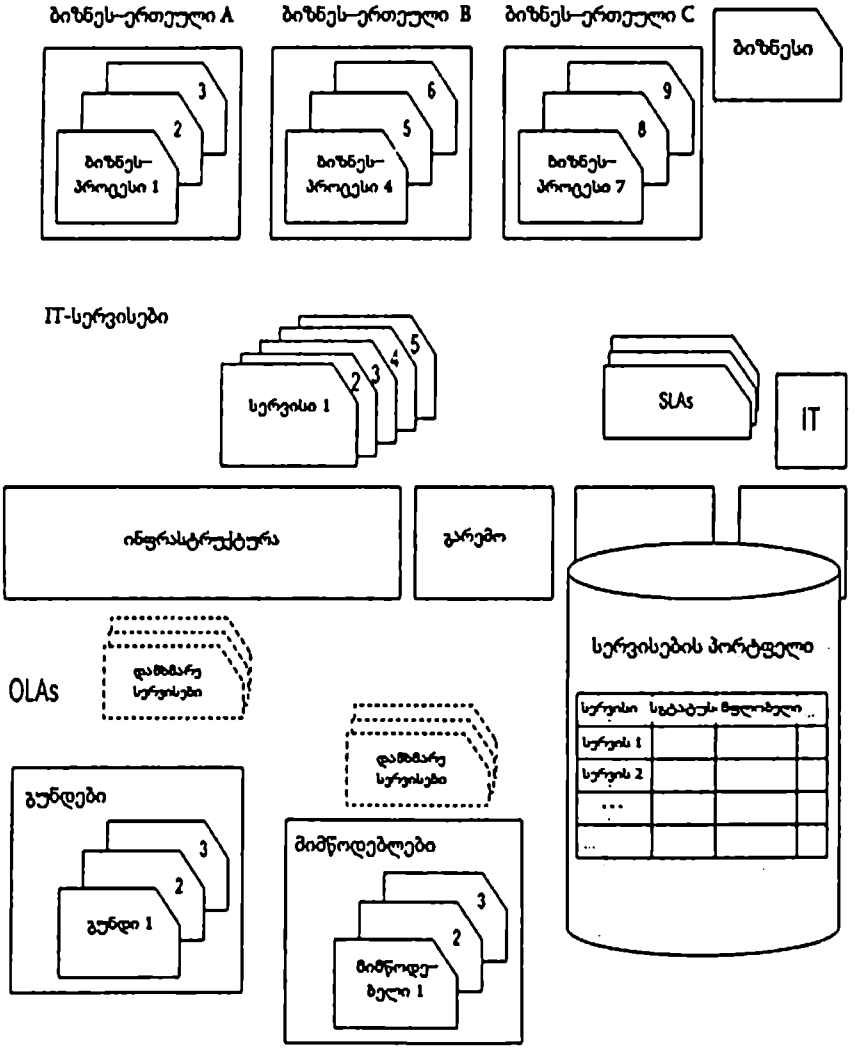
3. „გაანალიზებულია"– მოთხოვნათა ერთობლიობა განალიზებული და მოწესრიგებულია;

4. „დამტკიცებულია"– მოთხოვნათა ერთობლიობა საბოლოოდ ფორმალიზებული და დამტკიცებულია;

5. „შევსებულია"– გამოყოფილია რესურსები და თანხები ახალი სერვისისთვის;

6. „დაპროექტებულია"– ახალი სერვისი და მისი კომპონენტები დაპროექტებულია;

7. „დამუშავებულია"– ახალი სერვისი და მისი კომპონენტები მუშავდება;



ნახ.13.5. სერვისების პორტფელი – ინფორმაციის ცენტრალური საცავი

8. „აწყობილია" – სერვისის კომპონენტები აწყობილია ერთად;

9. „ტესტირება" – სერვისი და მისი კომპონენტები ტესტირდება;

10. „რელიზი" – სერვისის და მისი კომპონენტების რელიზი (გამოშვება);

11. „ექსპლუატაცია" – სერვისის და მისი კომპონენტების გამოყენება;

12. „მოხსნილია" – სერვისი და მისი კომპონენტები ამოღებულია ექსპლუატაციიდან.

ერთი სერვისის სხვადასხვა ელემენტს შეიძლება ჰქონდეს განსხვავებული სტატუსი დროის ერთ მომენტში. ყოველი ორგანიზაცია აკურატულად უნდა აპროექტებდეს სერვისების პორტფელს, მის შედგენილობას და მასთან წვდომას. სერვისების პორტფელის შედგენილობა უნდა შეიცავდეს შემდეგ ინფორმაციას:

1. სერვისის სახელი;
2. სერვისის აღწერა;
3. სერვისის სტატუსი;
4. სერვისის კლასიფიკაცია და მისი კრიტიკულობა;
5. გამოყენებული აპლიკაციები;
6. გამოყენებული მონაცემები ან/და მონაცემთა სქემები;
7. ბიზნეს–პროცესები, სერვისით მხარდაჭერილი;
8. ბიზნესის მფლობელები;
9. ბიზნესის მომხმარებლები;
10. IT მფლობელები;
11. სერვისის ხარისხის გარანტიის დონე, მიმართვა SLA და SLR –ზე;
12. მხარდამჭერი სერვისები;
13. მხარდამჭერი რესურსები;

14. სერვისები, რომლებიც დამოკიდებულია განხილვად სერვისზე;
15. OLA (Operational Level Agreement), კონტრაქტები და შეთანხმებები;
16. ხარჯები სერვისზე;
17. შემოსავალი სერვისიდან;
18. მეტრიკები სერვისისთვის.

დამკვეთებს და მომხმარებლებს შეუძლიათ წვდომის მიღება სერვისებზე მხოლოდ „შევსებულია" და „ექსპლუატაცია" სტადიებს შორის. სერვისები ამ სტატუსებით არის სერვისების პორტფელში. მიუხედავად იმისა, რომ სერვისების პორტფელის დაპროექტება ხდება დაპროექტების სტადიაზე, მას ფლობს და მართავს სერვისების პორტფელის მართვის პროცესი სტრატეგიის აგების ეტაპიდან.

სერვისების პორტფელი ინფორმაციის ძირითადი წყაროა მოთხოვნების და სერვისების შესახებ, ამგვარად მისი დაპროექტება უნდა მოხდეს ძალზე ფრთხილად და თანამიმდევრულად. ანალოგიურ მიდგომას დაპროექტებისადმი თხოულობს სხვა მართვის სისტემებიც, მაგალითად, Service Knowledge Management System და Service Desk System.

13.2.3. ტექნოლოგიების არქიტექტურის დაპროექტება

ტერმინს „არქიტექტურა“ აქვს განსხვავებული ინტერპრეტაცია კონტექსტისგან დამოკიდებულებით. აქ არქიტექტურა – სისტემის ფუნდამენტური სტრუქტურაა, რომელიც ასახავს მის კომპონენტებს, მათ ურთიერთქმედებას ერთმანეთთან და სისტემის ექსპლუატაციის პირობებს, აგრეთვე

პრინციპებს, რომლებიც საფუძველია სისტემის დაპროექტებისა და განვითარების.

„სისტემაში“ აქ იგულისხმება არა მხოლოდ სისტემა IT კონტექსტში. სისტემა – კომპონენეტების ერთობლიობაა, რომელიც ორგანიზებულია სპეციფიკური ფუნქციის ან ფუნქციათა ერთობლიობის უზრუნველსაყოფად.

სისტემის სახით მოცემულ კონტექსტში შეიძლება განხილულ იქნას ორგანიზაცია მთლიანად, ბიზნესფუნქცია, ინფორმაციული სისტემა და ა.შ. არქიტექტურის დაპროექტების არსი მდგომარეობს პოლიტიკის, სტრატეგიის, არქიტექტურის, დიზაინის, დოკუმენტების, გეგმების და IT-პროცესების განვითარებასა და მხარდაჭერაში, ორგანიზაციისთვის შესაფერისი სერვისების და გადაწყვეტების დანერგვისა და შემდგომი ექსპლუატაციის მიზნით.

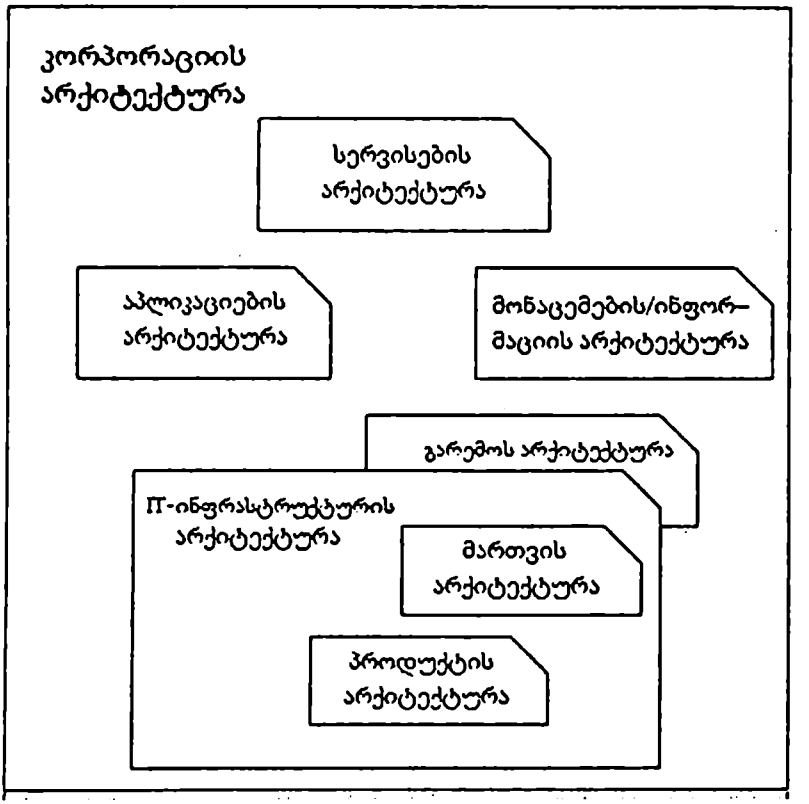
არქიტექტურის დაპროექტების შემავალი მონაცემებია ბიზნესის და სტრატეგიის აგების ეტაპის გეგმები, სტრატეგია და პოლიტიკა. დამპროექტებლების ამოცანაა დიზაინის, გეგმის, პოლიტიკის და არქიტექტურის სრულყოფა და განვითარება. ეს პროცესი განიხილავს აგრეთვე პასუხისმგებლობათა და როლების განაწილებას, სერვისს, ტექნოლოგიას, არქიტექტურას, პროცესს და პროცედურას, პარტნიორებს და მიმწოდებლებს, მართვის მეთოდებს.

არქიტექტურის დაპროექტება მოიცავს ასევე ყველა საკითხს ტექნოლოგიებთან დაკავშირებით, მათ შორის ინფრასტრუქტურას, გარემოს, აპლიკაციებს და მონაცემებს.

როგორც უკვე აღინიშნა, სისტემად შეიძლება მთლიანი ორანიზაციის განხილვა. იგი რთული სისტემაა კომპონენტების სიმრავლით: პერსონალი, ბიზნესფუნქციები, პროცესები,

ორგანიზაციული სტრუქტურა, ინფორმაციული და ფინანსური რესურსები, სტრატეგიები, მართვის სისტემები და ა.შ.

კორპორაციის არქიტექტურა უნდა უჩვენებდეს, თუ როგორ ურთიერთქმედებენ ერთმანეთთან ეს კომპონენტები საერთო კორპორაციული მიზნის მისაღწევად. ITIL განიხილავს კორპორაციის არქიტექტურას ბიზნესის, რომელსაც ის ეწევა, და გამოყენებული საინფორმაციო სისტემების კონტექსტში (ნახ.13.6).



ნახ.13.6. კორპორაციის არქიტექტურა

კორპორაციის არქიტექტურა უნდა შედგებოდეს შემდეგი ძირითადი არქიტექტურებისგან:

1. სერვისების არქიტექტურა – გადაყავს აპლიკაციები, ინფრასტრუქტურა, ქმედებათა ორგანიზაცია და მხარდაჭერა სერვისების ერთობლიობაში. სერვისების არქიტექტურა არის დამოუკიდებელი, ბიზნესში ინტეგრირებული მიდგომა ბიზნესისთვის სერვისების მისაწოდებლად. იგი იძლევა მოდელს დაყოფისთვის სერვისების არქიტექტურას, აპლიკაციების არქიტექტურას, ინფრასტრუქტურის არქიტექტურასა და მონაცემთა არქიტექტურას შორის. სერვისების არქიტექტურის ჩარჩოებში ასევე განიხილება საკითხები მტყუნებებისადმი სტაბილურობის უზრუნველყოფის, შემდგომი კორექტირების და უსაფრთხოების უზრუნველყოფის შესახებ.

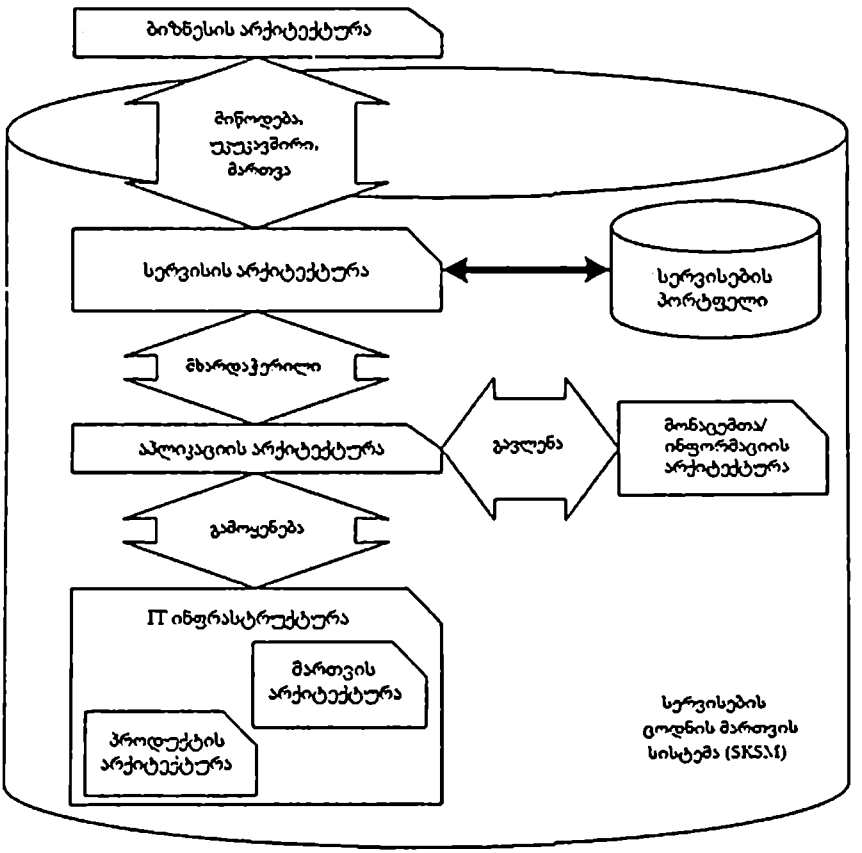
2. აპლიკაციების არქიტექტურა – იძლევა დეტალურ გეგმას ინდივიდუალური აპლიკაციების განვითარების და მიწოდების შესახებ, ასახავს ბიზნესის ფუნქციურ მოთხოვნებს აპლიკაციასთან და უჩვენებს ურთიერთდამოკიდებულებას აპლიკაციებს შორის. კომპონენტებზე დაფუძნებული მიდგომა მაქსიმალურს ხდის მათ ხელმეორედ გამოყენებას და ეხმარება აპლიკაციებს მოქნილობაში მომარაგების ცვლადი პოლიტიკის პირობებში.

3. მონაცემთა / ინფორმაციის არქიტექტურა – აღწერს ორგანიზაციის ლოგიკურ და ფიზიკურ ინფორმაციულ აქტივებს და მათი მართვის რესურსებს. იგი უჩვენებს, თუ როგორაა განაწილებული ინფორმაციული რესურსები და მათი მართვა კორპორაციული მიზნის მისაღწევად.

4. ინფრასტრუქტურის არქიტექტურა – აღწერს სტრუქტურას, ფუნქციურობას და პროგრამულ/აპარატურული უზრუნველყოფის გეოგრაფიულ განაწილებას, კომუნიკაციის კომპონენეტებს, ასევე მათთან დაკავშირებულ სტანდარტებს.

5. გარემოს არქიტექტურა – აღწერს გარემოს ასპექტებს, დონეებს და კონტროლის ტიპებს, აგრეთვე მათი მართვის საკითხებს.

აღწერილი არქიტექტურის ურთიერთკავშირი მოცემულია 13.7 ნახაზზე.



ნახ.13.7. არქიტექტურათა ურთიერთკავშირი

13.2.4. პროცესების დაპროექტება

პროცესი – ქმედებათა სტრუქტურირებული ერთობლიობაა, დაპროექტებული სპეციფიკური მიზნის მისაღწევად. პროცესი გარდაქმნის ერთ ან რამდენიმე შესასვლელს განსაზღვრულ გამოსასვლელებში. პროცესის განსაზღვრება მოიცავს ყველა როლს, პასუხისმგებლობის განაწილებას, ინსტრუმენტებს და კონტროლს, აუცილებელს მოლაპარაკებული შედეგების საიმედო მიწოდებაზე.

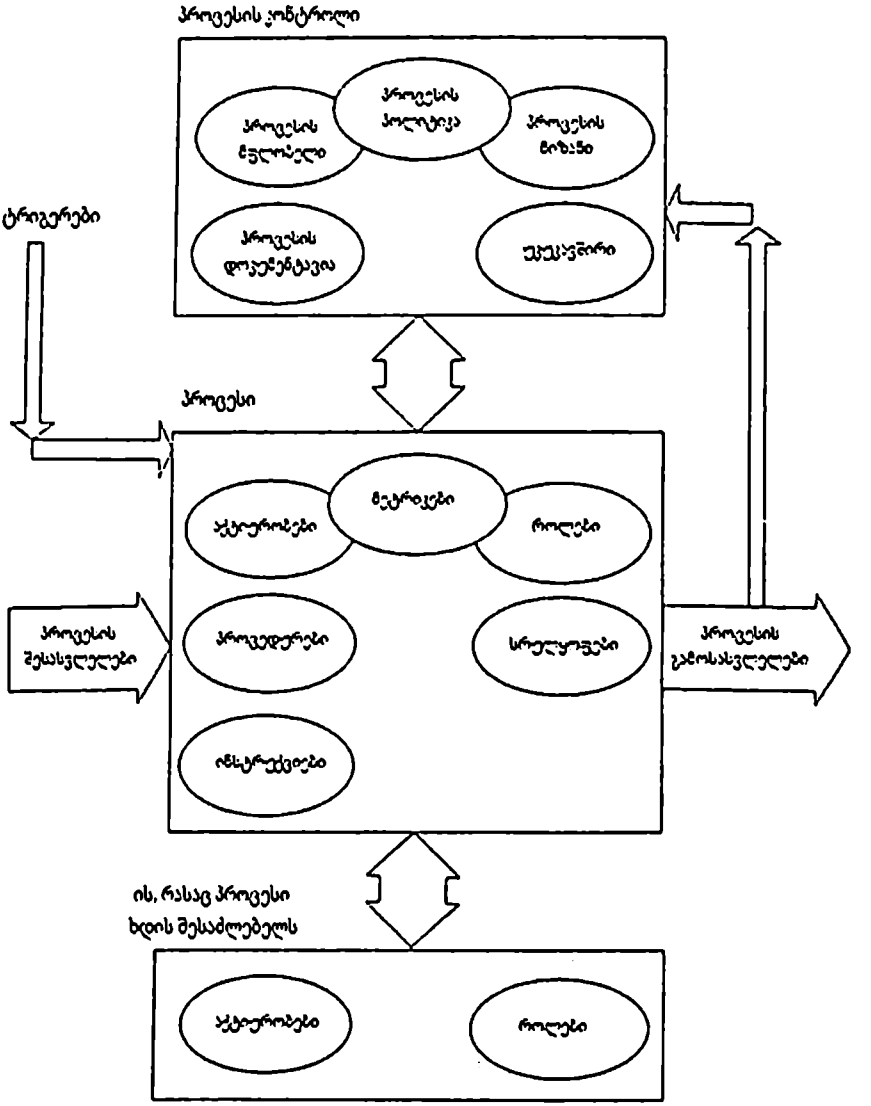
ერთხელ განსაზღვრული პროცესები უნდა კონტროლდებოდეს და იყოს მართვადი. პროცესების კონტროლი – ესაა ქმედება, დაკავშირებული პროცესის დაგეგმვასა და რეგულირებასთან, პროცესის წარმოდგენის მიზნით ეფექტური, რაციონალური და სტაბილური სახით. მხოლოდ კონტროლის დონეების განსაზღვრის შემდეგ შეიძლება განისაზღვროს კონტროლის ეფეტურობის გამზომი სისტემა შესაბამისი მეტრიკებით (ნახ.13.8).

პროცესი ყოველთვის იქმნება განსაზღვრული მიზნების მისაღწევად. პროცესის გამოსასვლელები უშუალოდ უნდა იყოს დამოკიდებული ამ მიზნებისგან.

დაპროექტებისას მნიშვნელოვანია შეფასების და მეტრიკის სისტემის დამუშავება პროცესის გამოსასვლელების, ანგარიშგების და სრულყოფისთვის.

ყველა პროცესს ჰყავს მფლობელი, პასუხისმგებელი მასზე და მის სრულყოფაზე, და რომ პროცესი უზრუნველყოფს თავის მიზნების მიღწევას.

მიზნები უნდა იყოს გაზომვადი და აღიწერებოდეს ბიზნესისთვის სასარგებლო ტერმინებით, მიღებული პოლიტიკის და სტრატეგიის გათვალისწინებით. დაპროექტების ეტაპზე ყველა პროცესს დაენიშნება მფლობელი.



ნახ.13.8. პროცესის ელემენტები

პროცესების გამოსასვლელები უნდა შეესაბამებოდეს რაღაც ოპერაციული ნორმების ერთობლიობას, რომლის წყარო იქნება ბიზნესის მიზნები. თუ პროცესის შედეგები შეესაბამება ნორმებს, მას შეიძლება ვუწოდოთ ეფექტური (იმიტომ რომ იგი შეიძლება გამეორდეს, გაზომვადი და მართვადია).

პროცესი ასევე ეფექტურად მოიხსენება, თუ იგი იყენებს რესურსების მინიმალურ ერთობლიობას. პროცესის გაზომვის და ანალიზის შედეგები შესაბამისი მეტრიკებით უნდა აისახოს მმართველ ანგარიშებში და უნდა მიეწოდოს უწყვეტი სრულყოფის პროცესის შესასვლელს.

პროცესი არის ITIL–ის საფუძველი. აუცილებელი შესასვლელების და გამოსასვლელების განსაზღვრა პროცესისაკენ ორგანიზაციის შიგნით იძლევა შესაძლებლობას, უფრო ეფექტურად და რაციონალურად იმართოს იგი.

ნორმების დადგენა პროცესებისთვის იძლევა მისი მუშაობის ხარისხის გაზომვის შესაძლებლობას. ნორმები განსაზღვრავს კონკრეტულ პირობებს, რომელთაც უნდა შეესაბამებოდეს პროცესის შედეგები. ნებისმიერი პროცესის დაპროექტების დაწყების წინ მნიშვნელოვანია წარმოდგენა, თუ მისი გამოსასვლელები როგორ გამოიყურება. ყოველი ორგანიზაცია უნდა იყენებდეს ფორმალიზებულ მიდგომას სერვის–მენეჯმენტის პროცესების დაპროექტებისა და რეალიზაციისთვის.

არაა საჭირო „იდეალური პროცესების“ შექმნისკენ სწრაფვა. მნიშვნელოვანია ორგანიზაციისთვის პრაქტიკული და გამოყენებადი პროცესების დაპროექტება, შემდგომი სრულყოფის შესაძლებლობებით. ერთ-ერთი მიმართულება პროცესორული განვითარების მიდგომისა არის ინსტრუმენტების და სტანდარტების შექმნა. იგი საშუალებას მოგვცემს პროცესების

ინტეგრაციისათვის, რომლებიც სხვადასხვა ორგანიზაციებს ეკუთვნის.

ამის მაგალითია ღია სტანდარტი DMTF, რომელიც ეფუძნება ITIL კონცეფციას. იგი აფორმალიზებს ინფორმაციის გაცვლას ინციდენტების, პრობლემების და ცვლილებების შესახებ პროცესებს შორის [41].

13.2.5. მეთოდების და მეტრიკების დაპროექტება გაზომვისთვის

დაპროექტრების ეტაპის ამ ნაწილს დიდი მნიშვნელობა აქვს, რადგან სწორედ გაზომვის სისტემა იძლევა ინფორმაციას სერვისის ეფექტურობის შესახებ. ეს ინფორმაცია გავლენას ახდენს ადამიანთა ქცევაზე, რომლებიც გასაზომ პროცესებთან მუშაობენ, მიზანზე, პერსონალის და გუნდის მწარმოებლურობაზე, ასევე შედეგის ანაზღაურებაზე.

გამოყენებული გაზომვის სისტემა და მისი შესაბამისი მეტრიკები უნდა ასახავდეს ხარისხს და დაპროექტების პროცესების ეფექტურობას ბიზნესის, დამკვეთების და მომხმარებლების თვალსაზრისით.

არსებობს ოთხი სახის მეტრიკა, რომლებიც შეიძლება გამოყენებულ იქნას პროცესების მწარმოებლურობის და შესაძლებლობების გასაზომად:

1. პროგრესი – საკონტროლო წერტილებში გაზომილი პროგრესის შედეგები;

2. შესაბამისობა – პროცესის შესაბამისობა ხელმძღვანელობის მოთხოვნებთან და რეგულატორებთან;

3. შედეგიანობა – პროცესის სიფრთხილე, კორექტულობა, ასევე მისი შესაძლებლობა დასმული მიზნის მისაღწევად;

4. ეფექტურობა – რესურსების გამოყენების მიზანშეწონილობის ზომა პროცესის რეალიზაციისთვის.

დასასრულებელ პროცესს უკეთესად მიესადაგება პირველი ორი მიდგომა, ხოლო დასრულებული პროცესისთვის რეკომენდებულია მესამე და მეოთხე.

13.3. შემდგომი ქმედებები სერვისების დაპროექტების ჩარჩოებში

სანამ დაპროექტებული გადაწყვეტა გადაცემული იქნება დანერგვის ეტაპზე, აუცილებელია შემდეგი დამატებითი ქმედებების შესრულება:

1. **ალტერნატიული გადაწყვეტების შეფასება.** ეს ქმედება აუცილებელია, თუ სერვისებით უზრუნველყოფა ხდება გარე მიმწოდებლებით და გადაწყვეტებით. იგი შედგება შემდეგი ქმედებებით:

   - მიმწოდებელთა ერთობლიობის ფორმირება და ტენდერის ორგანიზაცია;
   - მიმოხილვა და შეფასება ყველა გადაწყვეტის, რომლებსაც მიმწოდებლები სთავაზობენ. ყველაზე შესაფერისი მიმწოდებლის შერჩევა კონკრეტული ამოცანისათვის;
   - ალტერნატივების შეფასება და ღირებულების გაანგარიშება, შემდგომში საუკეთესოების ამორჩევით.

2. **არჩეული გადაწყვეტის მომარაგება.** მართალია არსებობს შესაძლებლობა, რომ დამუშავებული გადაწყვეტისათვის არ იქნება საჭირო მესამე მხარის მონაწილეობა (ანუ მიმწოდებლების), მიუხედავად ამისა, პრაქტიკაში ხშირია მათი მონაწილეობა, ამიტომ აუცილებელია შემდეგ ქმედებათა შესრულება:

- ამორჩეული მიმწოდებლისთვის ყველა აუცილებელი შემოწმების დასრულება;
- კონტრაქტების დადება მიმწოდებელთან;
- არჩეული გადაწყვეტის მომარაგება.

3. გადაწყვეტის დამუშავება.

აქ განიხილება ქმედება სერვისის პროექტის ტრანსლირებისათვის მისი დამუშავების გეგმაში. ყოველი გეგმა პასუხისმგებელი იქნება სერვისის ერთი ან მეტი კომპონენტის დასამუშავებლად და უნდა შეიცავდეს შემდეგს:

- ბიზნესის მოთხოვნილებები;
- სტრატეგია, გამოყენებული გადაწყვეტის დასამუშავებლად და/ან შესასყიდლად;
- დროითი ჩარჩოები;
- საჭირო რესურსები, მათ შორის IT შესაძლებლობები და ინფრასტრუქტურები, კვალიფიციური პერსონალი და ა.შ. ;
- სერვისის და მისი კომპონენტების დამუშავება, მათ შორის მართვის, ანგარიშგების ფორმირების, გაზომვის და სხვა მექანიზმების;
- სერვისის და მისი კომპონენტების ტესტირების გეგმა.

13.4. სერვისების დაპროექტების და უზრუნველყოფის მოდელები

სერვისების დაპროექტების მოდელი დამოკიდებულია მათი უზრუნველყოფის მოდელისგან. ანუ, სანამ არჩეულ იქნება ახალი სერვისის დაპროექტების მოდელი, მის უზრუნველსაყოფად აუცილებელია ჩატარდეს მიმდინარე შესაძლებლობების და რეზერვების მიმოხილვა. ასეთი მიმოხილვა უნდა შეიცავდეს შემდეგ საკითხებს:

- ბიზნესის მოთხოვნები და დრაივერები;
- სერვისების მიმწოდებლის არეალი და შესაძლებლობები;
- მოთხოვნა, მიზნები და ახალი სერვისისადმი მოთხოვნები;
- სერვისების გარე მიმწოდებლების არეალი და შესაძლებლობები;
- ორგანიზაციათა ძალები, რომლებიც უკვე ამოქმედებულია;
- პროცესში ჩართული ორგანიზაციების კულტურული თავისებურებანი;
- ამოქმედებული ინფრასტრუქტურები, აპლიკაციები, მონაცემები, სერვისები და IT –ს სხვა კომპონენტები;
- მოთხოვნილი კონტროლის ხარისხი ხელმძღვანელობის მხრიდან;
- მისაწვდომი რესურსები და ფინანსური საშუალებები;
- პერსონალის დონე და აუცილებელი ჩვევები.

ინფორმაცია ასეთი მიმოხილვიდან სერვისების მიმწოდებლის შესახებ გვეხმარება გავიგოთ, თუ როგორ უზრუნველყოფს იგი სერვისებს და როგორი შესაძლებლობების ამოქმედება შეუძლია ახალი დაპროექტებული სერვისისთვის. სერვისების უზრუნველყოფის მოდელი იძლევა საფუძველს სერვისების დაპროექტების მოდელის ასარჩევად.

არსებობს მრავალი მოდელი სერვისების უზრუნველსაყოფად, რომელთაგან თითოეულს აქვს თავისი უპირატესობა და ნაკლოვანება.

13.1 ცხრილში მოცემულია სერვისების უზრუნველყოფის ძირითადი მოდელები. პრაქტიკაში სერვისებით უზრუნველყოფა ხდება ერთ-ერთი ამ მოდელით ან მათი ვარიაციით.

სერვისების უზრუნველყოფის მოდელები

ცხრ.13.1

ინსორსინგი (Insourcing)	გამოიყენება სერვისების შიგა მიმწოდებელი IT-სერვისების სამართავად [11]. ორგანიზაცია იყენებს შიგა რესურსებს დაპროექტების, დამუშავების, დანერგვის, მართვის, ექსპლუატაციის მიზნით და/ან ახალი, შეცვლილი ან გადასინჯული სერვისების მხარდასაჭერად.
აუთსორსინგი (Outsourcing)	გამოიყენება სერვისების გარე მიმწოდებელი IT-სერვისების სამართავად. ორგანიზაცია იყენებს გარე ორგანიზაციის (ან ორგანიზაციების) რესურსებს მოქმედებათა ნაწილის შესასრულებლად, რაც დაკავშირებულია სერვისების დაპროექტების, დამუშავების, მართვის, ექსპლუატაციის ან მხარდაჭერის საკითხებთან.
კო-სორსინგი (Co-sourcing)	კომბინირებული ინსორსინგი და აუთსორსინგი. გამოიყენება რიგი გარე ორგანიზაციებისა, რომელიღაც ცალკეული ელემენტების უზრუნველსაყოფად, სერვისის სასიცოცხლო ციკლის ფარგლებში. ორგანიზაცია-დამკვეთის და მესამე მხარის თანამშრომლები მუშაობენ ერთად დაპროექტების, დამუშავების, დანერგვის, მართვის, ექსპლუატაციის მიზნით და/ან ახალი, შეცვლილი ან გადასინჯული სერვისების მხარდასაჭერად. მაგალითად, აუთსორსინგს შეიძლება მიეცეს პროგრამული უზრუნველყოფის დამუშავების ერთი ნაწილი, მაშინ, როცა ძირითადი კოდის მფლობელი იქნება თვით დამკვეთი.
პარტნიორობა ან მულტისორსინგი (Partnership or multisourcing)	მიდგომა ითვალისწინებს ფორმალურ შეთანხმებას ორ და მეტ ორგანიზაციას შორის ერთობლივი სამუშაოების ჩატარების შესახებ სერვისების დაპროექტების, დამუშავების, მართვის, ექსპლუატაციის და/ან მხარდაჭერის საკითხებზე.

ბიზნესპროცესების აუთსორსინგი (Business Process Outsourcing)	მიდგომა ითვალისწინებს ორგანიზაცია-დამკვეთის მთლიანი ბიზნესპროცესის გადაცემას სხვ ორგანიზაციის აუთსორსინგზე შეთანხმების დადებით. მაგალითად, საბუღალტრო აღრიცხვის გადაცემა.
აპლიკაციის დონის სერვისების უზრუნველყოფა (Applıcation Service Provision)	მიდგომა ითვალისწინებს შეთანხმებების დადებას აპლიკაციური პროგრამული სისტემების სერვისების მიმწოდებლებთან. ესაა გარე მიმწოდებელი (Application Service Provider-ASP), რომელიც უზრუნველყოფს სერვისებს აპლიკაციების გამოყენებით, რომლებიც პროვაიდერის სიმძლავრეებზეა განთავსებული. მომხმარებლები იღებენ წვდომას აპლიკაციებთან ქსელური ჩართვით პროვაიდერთან.
ცოდნის მართვის აუთსორსინგი (Knowledge Process Outsourcing ან KPO)	KPO არის აუთსორსინგის ახალი ფორმა. იგი სტადიაა და წინ უსწრებს მთლიანი ბიზნეს–პროცესების აუთსორსინგს. მოცემულ შემთხვევაში, ორგანიზაცია-დამკვეთი გადასცემს გარე ორგანიზაციას პროცესებს, რომლებიც ითხოვს სპეციფიკურ გამოცდილებას, კვალიფიკაციას და ჩვევებს. მაგალითად, თანამშრომელთა ტრეინინგი. KPO ითვალისწინებს პროცესების მართვას, რომლებიც ითხოვენ მონაცემთა ღრმა შესწავლას ან სერიოზულ ანალიზურ დამუშავებას, ცოდნის ბაზების ფორმირებას და მართვას, რომლებიც შემდგომ იქნება გამოყენებული, მათ შორის გადაწყვეტილების მხარდასაჭერად.

აუთსორსინგი საშუალებას აძლევს კომპანია-დამკვეთს შეკვეცოს ხარჯები და მნიშვნელოვნად შეამციროს შრომატევადობა და ხარჯები ინფორმაციული სისტემების და აპლიკაციების ექსპლუატაციაზე, კონცენტრირებული იყოს კომპანიის ძირითად ბიზნესპროცესებზე, და არ გადაერთოს დამხმარეებზე.

აუთსორსინგის ძირითად ფასეულობად შეიძლება ჩაითვალოს:

- ბიზნესპროცესის რეალიზაციის ღირებულების შემცირება მესამე მხარის ორგანიზაციის რესურსების გამოყენების ანგარიშზე;
- მიღებული პროდუქტების და სერვისების ხარისხის ამაღლება მესამე მხარის ორგანიზაციის სპეციფიკური რესურსების და ცოდნის გამოყენების ანგარიშზე ან იმის ხარჯზე, რომ დამკვეთი ორგანიზაცია შეძლებს არ გადაერთოს დამხმარე ბიზნესპროცესებზე.

ITIL გამოყოფს ორ მიდგომას პროგრამული უზრუნველყოფის და სერვისების დასამუშავებლად:

1. ტრადიციული დაპროექტება – ე.წ. კასკადური მოდელი (Waterfall). დაპროექტების მოდელი, რომელშიც დამუშავების პროცესი გამოიყურება როგორც ნაკადი მიმდევრობით შესასრულებელი ფაზებით: მოთხოვნების ანალიზი, დაპროექტება, რეალიზაცია, ტესტირება, ინტეგრაცია და მხარდაჭერა [24].

2. RAD (Rapid Application Development - აპლიკაციის სწრაფი დამუშავება) – პროგრამული პროდუქტების დამუშავების საშუალებების შექმნის კონცეფცია, რომელიც განსხვავებულია დაპროექტების ტრადიციული მიდგომებისგან [23].

კასკადურ მოდელში სტადიები სრულდება შემდეგი მიმდევრობით:

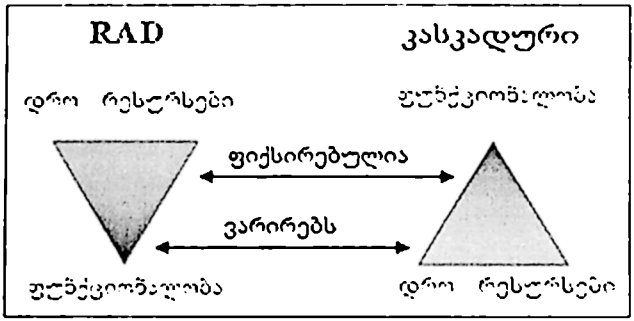
- მოთხოვნების განსაზღვრა;
- დაპროექტება;
- კონსტრუირება (ასევე „რეალიზაცია" ან „კოდირება");
- ინტეგრაცია;
- ტესტირება და გამართვა (ასევე „ვერიფიკაცია")
- ინსტალაცია;
- მხარდაჭერა.

ამ დროს დამმუშავებელს არ შეუძლია მომდევნო სტადიაზე გადასვლა, თუ არ დაასრულა წინა. ამგვარად, ჯერ სრულად მთავრდება ეტაპი „მოთხოვნების განსაზღვრა“, რის შედეგადაც მიიღება პროგრამული უზრუნველყოფის მოთხოვნების სია. მას შემდეგ რაც მოთხოვნები საბოლოოდ დადგინდება, ხდება გადასვლა დაპროექტებაზე, რომლის დროსაც იქმნება დოკუმენტაცია, რომელშიც აღიწერება პროგრამისტებისთვის მითითებული მოთხოვნების რეალიზაციის ხერხი და გეგმა.

დაპროექტების პროცესის მთლიანად დამთავრების შემდეგ იწყება პროგრამისტების მიერ პროექტის რეალიზაცია. შემდეგ სტადიაზე სრულდება პროგრამისტების სხვადასხვა გუნდის მიერ რეალიზებული კომპონენტების ინტეგრაცია. ამის შემდეგ იწყება პროდუქტის ტესტირება და გამართვა. ამ სტადიაზე გამოირიცხება ყველა უზუსტობა, რომლებიც წინა სტადიებზე არსებობდა. შემდეგ პროგრამული პროდუქტი ინერგება და ხორციელდება მისი შემდგომი მხარდაჭერა – ახალი ფუნქციონალობის დამატება და შეცდომების აღმოფხვრა.

კასკადური მოდელის დადებითი მხარეა ის, რომ შესაძლებელია წინასწარ იყოს გათვლილი გადაწყვეტის რეალიზაციის ღირებულება, ხოლო უარყოფითია – მოუქნელობა და სწრაფი რეაგირების შეუძლებლობა ბიზნესის მოთხოვნილებების ცვლილებებზე.

13.9 ნახაზზე ნაჩვენებია RAD და კასკადური მეთოდების შედარება.



ნახ.13.9. **RAD** და კასკადური მეთოდი

RAD არის დაპროექტების ბევრად თანამედროვე და მოქნილი მეთოდი. მისი ძირითადი უპირატესობაა გადაწყვეტის დამუშავებისას იტერაციული და ინკრემენტული მიდგომის გამოყენება. იტერაციული მიდგომა გულისხმობს სამუშაოთა შესრულებას მიღებული შედეგების უწყვეტი ანალიზის პარალელურად და სამუშაოს წინა ეტაპების კორექტირებას. ანუ ხორციელდება ერთგვარი უკუკავშირი. პროექტი ამ მიდგომის დროს პერიოდულად გაივლის განმეორებად ციკლს დაგეგმვა–რეალიზაცია–შეფასება. იტერაციული მიდგომის გამოყენებით RAD სწრაფად რეაგირებს ბიზნესის მოთხოვნათა ცვლილებებზე.

ინკრემენტული მიდგომა ითვალისწინებს სერვისის დამუშავებას „ნაწილ–ნაწილ“, ანუ მიმდევრობით. ამ დროს ყოველ „ნაწილს“ შეუძლია ერთი რომელიმე ბიზნეს–ფუნქციის მხარდაჭერა, რომლისთვისაც შექმნილია ეს სერვისი მთლიანად. ბიზნესისთვის ინკრემენტული მიდგომა იძლევა შესაძლებლობას, რომ სერვისის რომელიმე უკვე დამუშავებული ნაწილი იქნას გამოყენებული მანამ, სანამ იგი მთლიანად იქნება დამუშავებული.

სერვისების დაპროექტების დროს შესაძლებელია იტერაციული და ინკრემენტული მიდგომების კომბინირება. იწყებენ მოთხოვნების განსაზღვრით სერვისისთვის მთლიანად,

შემდეგ აგრძელებენ ინკრემენტალური მიდგომით ცალკეული ნაწილების დამუშავებას.

მთლიანად RAD-ს აქვს შემდეგი უპირატესობანი ტრადიციულთან შედარებით:

1. პროდუქტი უფრო სწრაფად შედის ბაზარზე;
2. უფრო ფართო შესაძლებლობებია მომხმარებელზე ორიენტირებული ინტერფეისების ასაგებად;
3. დიდი ადაპტაციის უნარი ბიზნესის მოთხოვნების ცვლილებებზე;
4. გადაწყვეტის მარტივი განვითარება და ფუნქციური ცვლილებები.

კიდევ ერთი მიდგომა – მზა გადაწყვეტების ყიდვა, ე.წ. „off-the-shelf“ (არსებული გაყიდვაში) ან COST. ასეთი პროგრამული უზრუნველყოფის ყიდვისას ორგანიზაციამ უნდა იცოდეს შემდეგი:

1. ამ მიდგომის დადებითი და უარყოფითი მხარეები;
2. განახორციელოს ამორჩევის პროცესი უკეთესი ეფექტური მზა გადაწყვეტისთვის;
3. განსაზღვროს პროცესი ეფექტური ინტეგრაციისთვის და მზა გადაწყვეტის მიერთებისთვის;
4. განსაზღვროს ფუნქციური მოთხოვნები მისაღებ დონეზე;
5. ფორმირებაში მოიყვანოს ჩამონათვალი მმართველი და ოპერაციული მოთხოვნებისთვის;
6. განსაზღვროს მოთხოვნები პროდუქტზე და მიმწოდებელზე.

მზა პროგრამული პაკეტების ყიდვა ბევრად ეკონომიურია, მაგრამ ნაკლებად მოქნილია, ვიდრე საკუთარი გადაწყვეტების დამუშავება. მიუხედავად ამისა, ზოგჯერ ორგანიზაციისთვის უფრო ხელსაყრელია მზა გადაწყვეტების ყიდვა.

14. პროცესები დაპროექტების ეტაპის ფარგლებში: სერვისების კატალოგის, სიმძლავრეების და წვდომის მართვა

დაპროექტების ეტაპის საბოლოო მიზანია სერვისების შექმნა, რომლებსაც შეუძლია ბიზნესის ცვლადი მოთხოვნილებების დაკმაყოფილება. დაპროექტების შესასვლელზე ინფორმაცია მიეწოდება სხვადასხვა წყაროდან. ეფექტური სერვისების შესაქმნელად იგი უნდა შეიკრიბოს, გაანალიზდეს, აგრეთვე ხელმეორედ უნდა შეფასდეს და გადაიხედოს დაპროექტების ტერმინებში.

დაპროექტების ასეთი ინტეგრაცია სერვისის სხვა სფეროებთან და სასიცოცხლო ციკლის ეტაპებთან იძლევა გარანტიას, რომ ახალი გადაწყვეტები იქნება თავსებადი და შედარებადი უკვე არსებულ სერვისებთან და შეძლებენ მომხმარებელთა და დამკვეთთა მოლოდინის გამართლებას.

ამ და შემდეგ თავებში განიხილება პასუხისმგებელი პროცესები ინფორმაციის უზრუნველსაყოფად, რომელიც საჭიროა ახალი ან შეცვლილი სერვისების დასაპროექტებლად.

14.1. სერვისების კატალოგის მართვა

სერვისების კატალოგი ინფორმაციის საკვანძო წყაროა სერვისების შესახებ, რომლითაც ხდება ბიზნესის უზრუნველყოფა სერვისების მიმწოდებლის მიერ. იგი აწვდის ბიზნესს აქტუალურ, საიმედო და სრულ სურათს ხელმისაწვდომი სერვისების, მათი დეტალების და სტატუსების შესახებ.

სერვისების კატალოგის მართვის მიზანია ინფორმაციის მართვა, რომელსაც შეიცავს კატალოგი, გარანტი იმისა, რომ ის კორექტულია და შეიცავს ყველა ექსპლუატაციაში მყოფი ან

გამზადებული სერვისის აქტუალურ სტატუსებს, დეტალებს და დამოკიდებულებას.

სერვისების კატალოგის მართვის ამოცანაა კატალოგის ფორმირება და მისი მართვა. ქმედება კატალოგის მართვის ფარგლებში უნდა შეიცავდეს შემდეგს:

1. სერვისების განსაზღვრა;
2. სერვისების კატალოგის ფორმირება და მხარდაჭერა;
3. კავშირის, დამოკიდებულების და შეთანხმების უზრუნველყოფა სერვისების პორტფელსა და სერვისების კატალოგს შორის;
4. კავშირების და დამოკიდებულებების უზრუნველყოფა ყველა სერვისს შორის, რომლებიც მხარდაჭერილია მისი კომპონენტებიით და კონფიგურაციული ერთეულებით სერვისების კატალოგის და კონფიგურაციების მართვის სისტემის კონტექსტში. კონფიგურაციული ერთეული (Configuration Item ან CI) – ესაა ნებისმიერი კომპონენტი, რომელიც ითხოვს მართვას იმისთვის, რომ უზრუნველყოს სერვისი [11]. ინფორმაცია ყოველ კონფიგურაციულ ერთეულზე რეგისტრირდება ჩანაწერის სახით კონფიგურაციების მართვის სისტემაში და მხარდაჭერილია მთელ სასიცოცხლო ციკლში აქტუალური კონფიგურაციების მართვის პროცესით.

სერვისების კატალოგს აქვს ბიზნესისთვის განსაკუთრებული ფასეულობა, რადგან იძლევა აქტუალურ ინფორმაციას მიმწოდებლის წვდომანებადართულ სერვისებზე, მათ შორის იმაზეც, თუ როგორ წარედგინება ისინი, რომელ ბიზნესპროცესებს უჭერს მხარს და როგორია ხარისხის გარანტია.

პოლიტიკა, რომელიც მიღბული და მხარდაჭერილია ორგანიზაციაში, უნდა განიხილავდეს სერვისების კატალოგის და სერვისების პორტფელის საკითხებს. კერძოდ, განსაზღვროს

სერვისების დეტალები, რომლებიც აუცილებელად უნდა აისახოს სერვისების პორტფელსა და კატალოგში, და სტატუსების სია, რომლებიც შეიძლება ჰქონდეთ სერვისებს. პოლიტიკის მნიშვნელოვან ასპექტად ითვლება პასუხისმგებლობის განაწილება სერვისების პორტფელის თითოეულ ნაწილზე.

თვით სერვისის არსი ვარირებს იმისდა მიხედვით, თუ ვინ იყენებს მას. მაშასადამე, მომხმარებლები შეიძლება ვერ ხედავდნენ და, ამგვარად, არ ითვალისწინებდნენ ზოგიერთ დამხმარე სერვისებს. დამხმარე სერვისი – ესაა ძირითადი სერვისის მუშაობის უზრუნველმყოფელი ან დასამატებელი სერვისი. მაგალითად, *კატალოგების სამსახური* – ძირითადი სერვისია და *სარეზერვო დუბლირების სერვისი* – კი დამხმარე.

IT–თვის დამხმარე სერვისს აქვს დიდი მნიშვნელობა, რადგან ის იძლევა საშუალებას წარმოადგინოს მომხმარებლისთვის „ხილვადი“ სერვისი და უზრუნველყოს მისი ხარისხი. ამიტომ დამხმარე სერვისი აუცილებლად უნდა იყოს ასახული სერვისების კატალოგში.

რეკომენდებული პრაქტიკაა სერვისების იერარქიული წარმოდგენა სერვისების კატალოგში მისი ტიპის დეტალიზაციით ბიზნესი–სერვისი, მხარდამჭერი სერვისი, განაწილებული სერვისი და ა.შ.

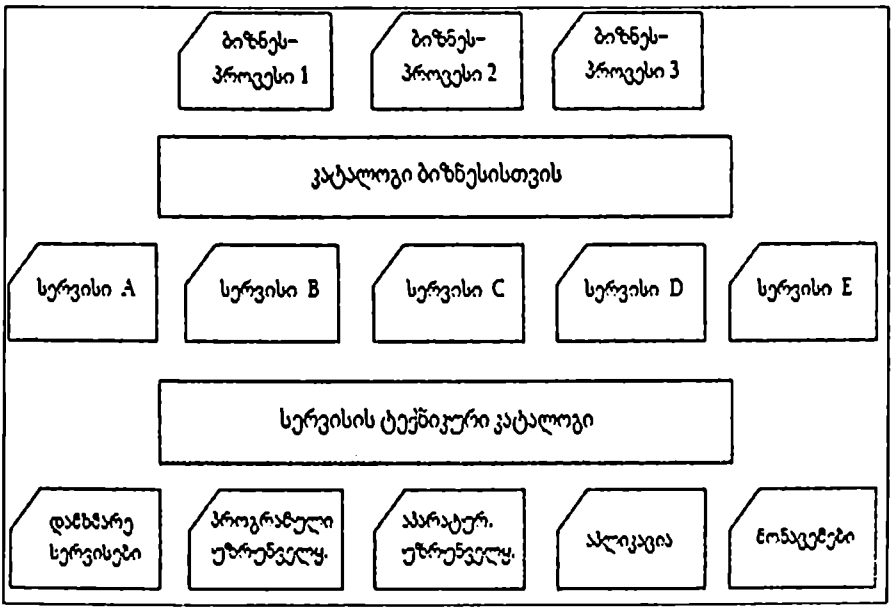
სერვისების კატალოგს აქვს ორი მდგენელი:

1. სერვისების კატალოგი ბიზნესისთვის – ესაა დამკვეთის თვალსაზრისი სერვისების კატალოგზე. იგი შეიცავს ინფორმაციას ყველა სერვისის შესახებ, რომელიც მიეწოდება დამკვეთს, მათ ურთიერთკავშირს ბიზნესერთეულებთან და ბიზნესპროცესებთან, რომელთა მხარდასაჭერადაცაა ისინი დანიშნული;

2. სერვისების ტექნიკური კატალოგი – ესაა სერვისების კატალოგის ის ნაწილი, რომელიც არ ჩანს მომხმარებლებისთვის.

შეიცავს ინფორმაციას ყველა სერვისის შესახებ, რომელიც მიეწოდება დამკვეთებს, აგრეთვე მათ კავშირებს მხარდამჭერ და განაწილებულ სერვისებთან, კომპონენტებთან და კონფიგურაციულ ერთეულებთან.

სერვისების კატალოგის ორი მდგენელის ურთიერთქმედება ნაჩვენებია 14.1 ნახაზზე.



ნახ.14.1. ბიზნესის სერვისების კატალოგის და სერვისების ტექნიკური კატალოგის ურთიერთკავშირი

როგორც ნახაზიდან ჩანს, სერვისების კატალოგი ბიზნესისთვის აკავშირებს სერვისებს და ბიზნესპროცესებს, ანუ იმას, რაც აღელვებს ბიზნესს, ხოლო სერვისების ტექნიკური კატალოგი აკავშირებს სერვისებს იმასთან, რაც უზრუნველყოფს მათ მუშაობას, ანუ იმას, რაც აღელვებს IT-ს.

ქმედებები, რომლებიც უნდა განხორციელდეს სერვისების კატალოგის მართვის ფარგლებში:

1. დამტკიცება და დოკუმენტირება ყველა სერვისის თავისი კომპონენტებით;
2. ურთიერთმოქმედება სერვისების პორტფელის მართვასთან ინფორმაციის შეთანხმების მიზნით, რომელიც არის სერვისების პორტფელში და სერვისების კატალოგში;
3. სერვისების კატალოგის ფორმირება და მხარდაჭერა სერვისების პორტფელთან მიბმით;
4. ურთიერთმოქმედება IT–თან და ბიზნესთან დამოკიდებულებათა დამყარების მიზნით ბიზნესერთეულებს, ბიზნესპროცესებსა და მხარდამჭერ სერვისებს შორის;
5. ურთიერთმოქმედება მხარდაჭერის სამსახურებთან, მიმწოდებლებთან და კონფიგურაციათა მართვასთან, დამოკიდებულებათა დამყარების მიზნით სერვისებსა და მხარდამჭერ კომპონენტებს შორის, რომლებიც არის სერვისების ტექნიკურ კატალოგში;
6. ურთიერთმოქმედება ბიზნესთან ურთიერთდამოკიდებულების მართვასა და სერვისების დონის მართვას შორის, იმის გარანტიის მიზნით, რომ ინფორმაცია სერვისების კატალოგში კორექტირდება ბიზნესის და მისი პროცესების შესაბამისად.

ინფორმაცია სერვისების კატალოგის მართვის ორგანიზაციისთვის შემოდის სხვადასხვა წყაროებიდან. ITIL –ში ინფორმაციის წყაროები პროცესისთვის იწოდება შესასვლელებად. სერვისების მართვის პროცესის ძირითადი შესასვლელებია:

1. ბიზნესის და IT–ს სტრატეგიები და გეგმები, მიმდინარე და სამომავლო მოთხოვნები სერვისების პორტფელის მიმართ;

2. გავლენა, პრიორიტეტები და რისკები, დაკავშირებული ყოველ სერვისთან ან მის მოთხოვნების ცვლილებასთან. ამ ინფორმაციას იძლევა ბიზნესზე გავლენის ანალიზის პროცესი;

3. ბიზნესის მოთხოვნა – დეტალური აღწერა ახალი ან შეცვლილი ბიზნესის მოთხოვნების სერვისების პორტფელთან;

4. სერვისების პორტფელი;

5. კონფიგურაციების მართვის სისტემა (CMS);

6. უკუკავშირი სხვა პროცესეთან სერვისის სასიცოცხლო ციკლის ფარგლებში.

სერვისების კატალოგის მართვის გამოსასვლელებია:

1. ხელმძღვანელობის მიერ დამტკიცებული დოკუმენტაცია სერვისების აღწერის შესახებ;

2. სერვისების პორტფელის განახლება, რომლის შედეგადაც მასში იქნება მოთავსებული აქტუალური ინფორმაცია სერვისების სტატუსების და დამოკიდებულებების შესახებ;

3. სერვისების კატალოგი, რომელიც შეიცავს სერვისების მიმდინარე სტატუსების დეტალურ აღწერას, ინტერფეისებისა და დამოკიდებულებების აღწერასთან ერთად.

მწარმოებლურობის საკვანძო მაჩვენებელი (Key Performance Indicator ან KPI) – ესაა მეტრიკა, რომელიც გამოიყენება პროცესის, სერვისის ან ქმედების სამართავად. გამოიყოფა მწარმოებლურობის ორი საკვანძო მაჩვენებელი სერვისების კატალოგის მართვის კონტექსტში:

- პროცენტული თანაფარდობა კატალოგში სერვისების რაოდენობასა და სერვისების რაოდენობასთან, რომლებიც მიეწოდება დამკვეთებს განსაზღვრული დროის მომენტში;
- შეუსაბამობის რაოდენობა ინფორმაციებს შორის, სერვისების კატალოგსა და „რეალურ სიტუაციას“ შორის.

ძირითად რისკებად სერვისების კატალოგის მართვისათვის განიხილება არაზუსტი ინფორმაცია, შემოსული ბიზნესიდან და IT–დან, აგრეთვე ცუდად ორგანიზებული წვდომა სერვისების კატალოგთან.

14.2. სერვისების დონის მართვა

სერვისების დონის მართვა (Service Level Management ან SLM) – ესაა პროცესი, პასუხისმგებელი სერვისების დონის შესახებ შეთანხმებათა განხილვისათვის, და მათი შესრულების უზრუნველმყოფელი. *SLM* პასუხისმგებელია იმაზე, რომ სერვისების მართვის პროცესები, ოპერაციული დონის შეთანხმებანი და გარე ხელშეკრულებები იქნება შესაბამისობაში სერვისის დონის შეთანხმებულ მიზნობრივ მაჩვენებლებთან. *SLM* აკვირდება და აბარებს ანგარიშს სერვისების დონეების მიხედვით, ასრულებს რეგულარულ მიმოხილვებს დამკვეთებისთვის [11].

სხვა სიტყვებით, პროცესი პასუხს აგებს დამკვეთთან მოლაპარაკებებზე, მოთხოვნათა შეთანხმებაზე და სხვადასხვა მაჩვენებლების მნიშვნელობათა შერჩევაზე, რომლისკენაც უნდა მიისწრაფოდეს სერვისი – სერვისის დონის მიზნობრივი მაჩვენებლებისკენ.

ხდება პროცესის *მონიტორინგი* და ანგარიშის ფორმირება, რომელშიც აისახება მიმწოდებლის შესაძლებლობა დამკვეთის მოთხოვნების შესრულების შესახებ. *SLM*–ის წარმატება ბევრადაა დამოკიდებული წარმოდგენილ ინფორმაციაზე, რომლის საფუძველზე ფორმირდება მიზნობრივი მაჩვენებლები. ინფორმაციის წყაროდ, უპირველეს ყოვლისა, განიხილება სერვისების კატალოგი და სერვისების პორტფელი. *SLM* არის ერთგვარად, ურთიერთქმედების წერტილი სერვისების მიმწოდებელსა და დამკვეთს შორის. მან უნდა წარუდგინოს სერვისების მიმწოდებელი ბიზნესს და ბიზნესი – მიმწოდებელს.

SLM უზრუნველყოფს მეთოდების კორექტულობას, პროფესიულობას და საიმედოობას, რომლებიც გამოიყენება სერვისების მწარმოებლურობის გასაზომად.

სერვისების მართვის პროცესის შუალედური მიზნები:

1. წარმოდგენილი სერვისების დონის დადგენა, შეთანხმება და დოკუმენტირება;
2. დამკვეთების და მიმწოდებლების ურთიერთობის უზრუნველყოფა და სრულყოფა;
3. უზრუნველყოფა იმისა, რომ სერვისის მიზნობრივი მნიშვნელობები მიღწევადია და შესაძლებელია მათი გაზომვა;
4. დამკვეთთა დაკმაყოფილების მონიტორინგი და სრულყოფა წარმოდგენილი სერვისების დონით;
5. იმის გარანტია, რომ დამკვეთებს აქვთ ცხადი და არაორაზროვანი მოლოდინი სერვისების დონის შესახებ;
6. იმის გარანტია, რომ გამოიყენება გაზომვის პროაქტიური მეთოდები იქ, სადაც იგი ეკონომიურად გამართლებულია.

SLM უნდა შეიცავდეს შემდეგს:

- ბიზნესთან ურთიერთობის განვითარება;
- მოლაპარაკებები და მოთხოვნების და მიზნობრივი მაჩვენებლების შეთანხმება, აგრეთვე დოკუმენტირება და მართვა SLA სამრეწველო ექსპლუატაციაში მყოფ ყველა სერვისისთვის;
- განვითარება და მართვა OLA, დარწმუნების მიზნით, რომ უზრუნველყოფილ იქნას შესაბამისობა და კორელაცია SLA-თან;
- მიმწოდებლებთან კონტრაქტების და სხვა შეთანხმებების გადასინჯვა და ანალიზი მიმწოდებლების მართვის ფარგლებში, რათა უზრუნველყოფილ იქნას კორელაცია SLA-თან;
- მტყუნებებზე გაფრთხილება, რისკების შემცირება, სერვისების ხარისხის სრულყოფა;

- მართვა და ანგარიშგება ყველა სერვისის მიხედვით, SLA-ს ყველა სისუსტის და „ხვრელის“ მიმოხილვა;
- სერვისების სრულყოფის გეგმის კოორდინაცია. სერვისების სრულყოფის გეგმა (Service Improvement plan) – ესაა ფორმალური გეგმა სრულყოფის დანერგვისათვის პროცესში ან სერვისში [11].

SLA არის საფუძველი დამოკიდებულების ფორმირებისთვის ბიზნესსა და მიმწოდებელს შორის, ხოლო *SLM* – ამ ურთიერთქმედების წერტილი. ძირითადი ქმედება *SLM*-ის ფარგლებში უნდა შეიცავდეს შემდეგს:

1. დოკუმენტირება, შეთანხმება, დამკვეთთა მოთხოვნების დამტკიცება *SLR* ფორმაში და მათი მართვა სერვისის სასიცოცხლო ციკლის ფარგლებში SLA-ს დახმარებით;
2. სერვისების მწარმოებლურობის მონიტორინგი და გაზომვა SLA-ს ფარგლებში;
3. სამომხმარებლო დაკმაყოფილების გაზომვა და მონიტორინგი;
4. რეპორტის ფორმირება;
5. რეპორტები და მიღებული ინფორმაციის შეკრება და ანალიზი;
6. გაუმჯობესებათა ინიცირება სერვისების სრულყოფის გეგმის ფარგლებში;
7. SLA, OLA კონტრაქტების და სხვა საბაზო შეთანხმებების მიმოხილვა და შემოწმება;
8. ინვესტორებთან, დამკვეთებთან და ბიზნესთან კონტაქტების და ურთიერთდამოკიდებულების განვითარება და დოკუმენტირება;
9. ყველა დადებითი და უარყოფითი გამოხმაურების რეგისტრაცია;

10. კორექტული ინფორმაციის წარდგენა სერვისების მწარმოებლურობის მართვის და მიღწევების დემონსტრირებისა და მხარდაჭერის ფარგლებში;

11. დოკუმენტების და *SLM* სტანდარტების წვდომის/ აქტუალობის უზრუნველყოფა და მათი მართვა.

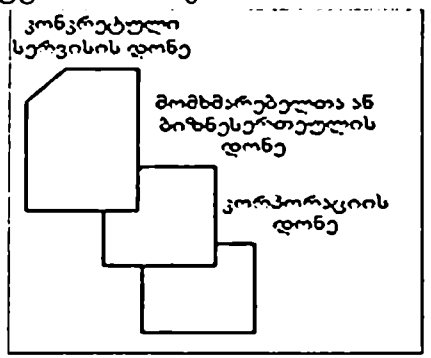
სერვისების კატალოგის გამოყენებისას *SLM*-მა უნდა მოახდინოს ფორმირება კონკრეტული ორგანიზაციისთვის ყველაზე მისაღები *SLA*. განიხილავენ *SLA*-ს რამდენიმე ტიპს:

1. **SLA,** სერვისებზე დაფუძნებული – ესაა SLA, რომელიც აღწერს სერვისების ერთ ტიპს ამ სერვისის ყველა მომხმარებლისთვის. მაგალითად, SLA-მ შეიძლება დაფაროს ელექტრონული ფოსტის სერვისი მისი ყველა მომხმარებლისთვის. ამ მიდგომის უპირატესობა მისი სიმარტივეა. ნაკლოვანებაა ის, რომ სხვადასხვა ტიპის მომხმარებელს შეიძლება დასჭირდეს სერვისის სხვადასხვა დონე ან მათ შეიძლება ჰქონდეთ განსხვავებული უპირატესობები ინფრასტრუქტურის თვალსაზრისით. მაგალითად, ტოპ-მენეჯერები შეიძლება ჩართული იყვნენ სწრაფ ქსელში, რიგითი თანამშრომლები კი – უფრო ნელში. სხვა სიტყვებით, აუცილებელია განსხვავებული მიზნობრივი მაჩვენებლების გაერთიანება ერთი შეთანხმების შიგნით;

2. **SLA,** მომხმარებლებზე დაფუძნებული – ესაა SLA, რომელიც აღწერს ყველა სერვისს, რომლებიც გამოიყენება გარკვეული ჯგუფის მომხმარებლების მიერ. მაგალითად, SLA-ს შეუძლია ყველა სერვისის აღწერა, რომლებიც მიეწოდება კორპორაციის ფინანსურ განყოფილებას. SLA-ს ეს სახე უფრო მოსახერხებელია დამკვეთისთვის, რადგან ფარავს ყველა იმ სერვისს, რომელიც მას სჭირდება;

3. მულტიდონური **SLA** (ნახ.14.2) შეიძლება სამ დონეს შეიცავდეს.

- კორპორაციის დონე – ფარავს *SLM-ის* საბაზო თავისებურებებს, რომლებიც მიესადაგება ორგანიზაციის ყველა თანამშრომელს. ეს თავისებურებები უნდა იყოს შესაძლოდ მუდმივები, რადგან SLA-ს განახლება ამ დონეზე ძალიან რთულია;
- მომხმარებელთა დონე – ფარავს *SLM-ის* ყველა თავისებურებას, რომლებიც ეხება მომხმარებელთა კონკრეტულ ჯგუფს ან ბიზნესერთეულს მათ მიერ გამოყენებული სერვისების მიხედვით;
- სერვისების დონე – ფარავს *SLM-ის* ყველა თავისებურებას, რომლებიც ეხება კონკრეტულ სერვისს მომხმარებელთა კონკრეტულ ჯგუფთან მიმართებით.



ნახ.14.2. მულტიდონური **SLA**

მრავალდონიანი სტრუქტურა საშუალებას იძლევა თავიდან ავიცილოთ ინფორმაციის დუბლირება და ზედმეტი განახლებები.

როგორი სტრუქტურაც არ უნდა აირჩიონ სერვისების მიმწოდებლებმა და ბიზნესმა, *SLA-ს* ფორმულირება უნდა იყოს ცხადი და არ ტოვებდეს არავითარ ეჭვს. მას შემდეგ, რაც *SLA* ფორმა დამტკიცდა, უნდა დაფორმირდეს *SLR*. ეს პროცესი საკმაოდ რთულია, ვინაიდან ბიზნესს ხშირად არ შეუძლია თავისი სურვილების და მოთხოვნების ცალსახად ფორმულირება

სერვისების მწარმოებლურობის, უსაფრთხოების, სიმძლავრის და უწყვეტობის ტერმინებში.

მსხვილ დამკვეთებთან მიმდინარეობს ხანგრძლივი მოლაპარაკებები *SLR* -ის აგების მიზნით და ბალანსის საპოვნელად, რა უნდათ და რისი მიღება შეუძლიათ რეალური ობიექტური ფაქტორებიდან გამომდინარე. *SLR* და *SLA* -ს დამტკიცების შემდეგ უნდა დამუშავდეს მექანიზმები სერვისების მწარმოებლურობის მონიტორინგისათვის. ცუდად დამუშავებული მექანიზმები იწვევს გაუგებრობას და კამათს დამკვეთსა და მიმწოდებელს შორის, რის შედეგადაც მთელი *SLM* პროცესი კარგავს აზრს. მნიშვნელოვანია სერვისის ყველა კომპონენტისთვის თვალყურის დევნება, რადგან დამკვეთისთვის მთავარია მისი მთლიანობა, სტაბილურობა და წვდომა ნებისმიერ დროს. მომხმარებლებმა, თავის მხრივ, მუდმივად უნდა აცნობონ მიმწოდებელს ყველა ინციდენტის და პრობლემის შესახებ, რათა მან შეძლოს სათანადო კორექტირების ჩატარება სერვისსა და მის კომპონენტებში.

სამომხმარებლო დაკმაყოფილებს გაზომვა განსხვავებულია მწარმოებლურობის გაზომვისგან, რომელიც სასურველია იყოს მაქსიმალურად ავტომატიზებული. სამომხმარებლო დაკმაყოფილება არის სუბიექტური ფაქტორი. მაშინაც კი, როცა მომხმარებლები ხვდებიან მწყობრიდან გამოსულ სერვისს, მათ მაინც აქვთ მასზე დადებითი შეხედულება, ხდება პირიქითაც. თავდაპირველად საჭიროა მცდელობა დამკვეთთა მოლოდინის სამართავად. ეს ნიშნავს სათანადო მოლოდინების და შესაბამისი მიზნობრივი მაჩვენებლების დაყენებას პირველ ადგილზე, და შემდგომ სისტემატური პროცესების დამუშავებას და მათ მართვას.

მომხმარებელთა დაკმაყოფილება = აღქმა - მოლოდინი

თუ ეს მნიშვნელობა >= 0 , მაშინ დამკვეთი კმაყოფილია.

დამკვეთის აღქმის გასაზომად *ITIL* რეკომენდაციას უწევს შემდეგ მეთოდებს და საშუალებებს:

1. დამკვეთთა პერიოდული გამოკითხვა და ანკეტირება;
2. უკუკავშირი მომხმარებლებთან შეხვედრების საფუძველზე;
3. უკუკავშირი დანერგვის შედეგების მიმოხილვიდან. ესაა ცვლილებების მართვის პროცესის ნაწილი. დანერგვის შედეგების მიმოხილვა (Post Implementation Review ან *PIR*), რომელიც სრულდება პროექტის ცვლილების დანერგვის შემდეგ. იგი განსაზღვრავს პროექტის ცვლილების წარმატებას, გამოავლენს შესაძლებლობებს სრულყოფისათვის.
4. დამკვეთების სატელეფონო გამოკითხვა;
5. მომხმარებელთა ინიციატივით შესრულებული რეცენზიები;
6. ფორუმები;
7. უპირატესობების და ნაკლოვანებების ანალიზი.

სერვისების მიმწოდებლისთვის მნიშვნელოვანია აჩვენოს დამკვეთებს, რომ იგი ყურადღებით ექცევა მათ შეხედულებებს, შეაქვს შესაბამისი კორექტივები და სრულყოფს სერვისს.

სერვისების მიმწოდებელი ყოველთვის დამოკიდებულია რომელიღაც თავის ან გარე მხარდაჭერის სამსახურებზე, მიმწოდებლებზე ან გარე პარტნიორებზე. კონტრაქტები გარე მიმწოდებლებთან აუცილებელია, მაგრამ ბევრი მიმწოდებელი ადგენს ასევე შეთანხმებებს მხარდაჭერის შიგა ჯგუფებთან.

ოპერაციული დონის შეთანხმება (Operational Level Agreement ან OLA) – ესაა შეთანხმება სერვისების მიმწოდებელსა და იმავე ორგანიზაციის მეორე ნაწილს შორის. OLA მხარს უჭერს სერვისების მიმწოდებელს დამკვეთისთვის სერვისის უზრუნველსაყოფად. OLA განსაზღვრავს წარმოსადგენ სქონელს ან სერვისებს და ორმხრივ პასუხისმგებლობას. წინასწარ, სანამ მოხდება ახალი *SLA*-ს ფორმირება, ან მასში ცვლილებების შეტანა,

აუცილებელია *არსებული ოპერაციული დონის შეთანხმებების* გაცნობა და, საჭიროების შემთხვევაში, მისი განახლება.

როგორც კი *SLA* ფორმირებულია და დამუშავებულია მონიტორინგის მექანიზმები, აუცილებელია რეპორტების ფორმირების პროცესის გამართვა. ანგარიშების ფორმირება უნდა მოხდეს რეგულარულად, ყოველკვირა ან უფრო ხშირად. რეპორტების განრიგი და ფორმატი აუცილებლად უნდა შეთანხმდეს დამკვეთთან. ანგარიშები უნდა იყოს გასაგები და შეიცავდეს ინფორმაციას სერვისების მწარმოებლურობაზე მიზნობრივ მაჩვენებელთა კონტესტში *SLA*-ში მითითებულის, აგრეთვე ინფორმაციას ყველა ცვლილების და სრულყოფის შესახებ.

ITIL იძლევა რეკომენდაციას, მოეწყოს რეგულარულ;ი შეხვედრები დამკვეთთან წარმოსადგენი სერვისების მიმოხილვის მიზნით და მათი მიღწევების შესახებ ბოლო პერიოდში. ასეთი „მიმოხილვითი შეხვედრები“ აუცილებელია ჩატარდეს თვეში ერთხელ ან კვარტალში ერთხელ მაინც. დამკვეთის და სერვისების მიმწოდებლის წარმომადგენლები უნდა განიხილავდნენ ანგარიშებს სერვისის ფუნქციონირების შესახებ, გამოავლინონ ადგილები, სადაც მაჩვენებლები ვერ აღწევენ დადგენილ მიზნობრივ მნიშვნელობებს, და შეთანხმდნენ მათი შემდგომი სრულყოფის შესახებ.

ფაქტორთა სიმრავლემ შეიძლება შეასრულოს ტრიგერის როლი *SLM*–სთვის, კერძოდ:

1. ცვლილებები სერვისების პორტფელში, როგორიცაა ბიზნესის ახალი მოთხოვნები, ახალი ან შეცვლილი სერვისები;
2. ახალი ან შეცვლილი შეთანხმებები, *SLR*, SLA, OLA და ა.შ.
3. "მიმოხილვითი ღონისძიებები" (ანკეტირება, შეხვედრები, სატელეფონო გამოკითხვები და ა.შ.);
4. დარღვევები სერვისში;

5. დადებითი და უარყოფითი რეცენზიები;
6. ცვლილებები სტრატეგიაში ან პოლიტიკაში.

SLM-ის შესასვლელებია:

- ინფორმაცია ბიზნესიდან – სტრატეგიები, გეგმები, მიმდინარე და სამომავლო მოთხოვნები;
- ბიზნესზე გავლენის ანალიზი – ინფორმაცია გავლენების შესახებ, პრიორიტეტებზე, რისკებზე, მომხმარებელთა რაოდენობაზე თითოეული სერვისისთვის;
- ბიზნესის მოთხოვნები – დეტალები ბიზნესის ნებისმიერ შეთანხმებულ ახალ და შეცვლილ მოთხოვნებზე;
- სტრატეგიები, IT პოლიტიკა და შეზღუდვები სტრატეგიის აგების ეტაპიდან;
- სერვისების პორტფელი და სერვისების კატალოგი;
- ინფორმაცია ცვლილებების შესახებ – ინფორმაცია ცვლილებათა მართვის პროცესიდან;
- CMS – ინფორმაცია ურთიერთმოქმედების შესახებ ბიზნეს-სერვისს, დამხმარე სერვისს და ტექნოლოგიებს შორის;
- უკუკავშირი დამკვეთთან, დადებითი და უარყოფითი რეცენზიები.

SLM-ის გამოსასვლელებია:

- რეპორტები სერვისების შესახებ, რომლებიც იძლევა ინფორმაციას სერვისის მუშაობის შესახებ SLA-ს მიზნობრივი მაჩვენებლების კონტექსტში. ეს ანგარიშები უნდა შეიცავდეს დეტალურ ინფორმაციას სერვისის ყველა მხარის შესახებ და მის უზრუნველსაყოფად, მათ შორის მიმდინარე და წარსულ მწარმოებლურობებზე, სისუსტეებზე და „ხვრელებზე“, ძირითად მოვლენებზე, დაგეგმილ ცვლილებებზე, მიმდინარე და სამომავლო სამუშაოს მოცულობებზე, გეგმებზე და სრულყოფის ქმედებებზე;

- სერვისების სრულყოფის გეგმა (SIP);
- დოკუმენტთა შაბლონები SLA, *SLR*, OLA-ს და სხვა შეთანხმებების შესადგენად;
- SLA;
- *SLR*;
- OLA.

ITIL გამოყოფს მწარმოებლურობის სუბიექტურ და ობიექტურ ინდიკატორებს *SLM*. სუბიექტურს მიეკუთვნება დამკვეთთა დაკმაყოფილების სრულყოფა წარმოდგენილი სერვისებით. ობიექტურია:

- მიღწეული მიზნობრივი მაჩვენებლების რაოდენობა ან პროცენტი;
- „ხვრელების“ რაოდენობა სერვისებში;
- სერვისების რაოდენობა აქტუალიური SLA-თი;
- სერვისების რაოდენობა რეგულარულად ფორმირებული რეპორტებით და მიმოხილვებით.

თუ შევაჯამებთ ყველაფერს, შეიძლება ითქვას, რომ *SLM არის „ჯაშუში ორივე ბანაკში“*. იგი არეგულირებს ურთიერთქმედებას მიმწოდებლებსა და დამკვეთებს შორის, წარმოადგენს რა ხან ერთ, ხან მეორე მხარეს.

„ოპოზიციური“ თვალსაზრისის წარმოდგენისას შეხვედრებზე, მოლაპარაკებებზე და სხვ. ხშირად დგება დაძაბული გაუგებრობის მომენტი. ამიტომაც *SLM* უნდა იყოს მაქსიმალურად გახსნილი და სასარგებლო ორივე მხარისთვის – სერვისების მიმწოდებლებისთვის და დამკვეთებისთვის.

14.3. სიმძლავრეების მართვა

სიმძლვრეების მართვა (Capacity Management) – ესაა პროცესი, რომელიც პასუხისმგებელია სერვისების სიმძლავრის და ინფრასტრუქტურის დროულ და ხარჯებით ეფექტურ შესაბამისობაზე სერვისის დონის შეთანხმებული მიზნობრივი მაჩვენებლების მოთხოვნებთან. სიმძლავრეების მართვა ითვალისწინებს ყველა რესურსს, რომლებიც აუცილებელია სერვისების უზრუნველსაყოფად, აგრეთვე აწარმოებს ბიზნეს–მოთხოვნების მოკლევადიან, საშუალოვადიან და გრძელვადიან დაგეგმვას.

სიმძლავრე (Capacity) – ესაა მაქსიმალური გამტარუნარიანობა, რომელიც შეიძლება უზრუნველყოს კონფიგურაციულმა ერთეულმა ან სერვისმა სერვისების დონის შეთანხმებული მიზნობრივი მაჩვენებლების ფარგლებში. კონფიგურაციული ერთეულების ზოგიერთი ტიპისთვის, სიმძლავრე შეიძლება გამოისახოს ზომით ან მოცულობით, მაგალითად, ვინჩესტერით.

სიმძლავრეების მართვის შუალედური მიზნები:

- სიმძლავრეების უზრუნველყოფის გეგმის ფორმირება და მართვა. სიმძლავრეების უზრუნველყოფის გეგმა (Capacity Plan) გამოიყენება რესურსების სამართავად, რომელიც საჭიროა სერვისის უზრუნველსაყოფად. ეს გეგმა შეიცავს სცენარებს მოთხოვნის პროგნოზირებისთვის ბიზნესის მხრიდან, და ხარჯების შეფასებას, აუცილებელს სერვისების დონის შეთანხმებული მიზნობრივი მაჩვენებლების უზრუნველსაყოფად;
- რეკომენდაციების უზრუნველყოფა და ხელმძღვანელობა ბიზნესის და IT–ის ყველა სხვა სფეროსთვის ყველა საკითხზე, რომელიც დაკავშირებულია მწარმოებლურობასა და სიმძლავრესთან;

- კონტროლი, რათა სერვისებმა მიაღწიოს დადგენილ მიზნობრივ მაჩვენებლებს, მწარმოებლურობის და სიმძლავრის მართვის გზით – როგორც სერვისის, ისე რესურსების;
- დახმარება პრობლემების დიაგნოსტირებასა და გადაწყვეტაში, რომლებიც დაკავშირებულია მწარმოებლურობასა და სიმძლავრესთან;
- შეაფასოს ცვლილებათა გავლენა სიმძლავრეების, სერვისების და რესურსების უზრუნველყოფის გეგმაზე;
- გარანტია მისცეს, რომ მწარმოებლურობის სრულყოფის პროაქტიური საშუალებები დაინერგოს იქ, სადაც ეს ეკონომიკურად გამართლებულია.

სიმძლავრეების მართვა მოიცავს შემდეგ ქმედებებს:

1. მონიტორინგი ბიზნესაქტიურობათა მოდელების და გეგმების, სერვისების დონეზე IT–სერვისების გამტარუნარიანობის გამოყენების მწარმოებლურობის და მხარდამჭერი ინფრასტრუქტურის, გარემოს, მონაცემების, აპლიკაციების ტერმინებში. პროცესმა უნდა დააფორმიროს შემთხვევითი და რეგულარული ანგარიშები სერვისების და მათი კომპონენტების მწარმოებლურობის და სიმძლავრის შესახებ;
2. ქმედების განხორციელება რეგულირებისა და აწყობისთვის რესურსების მაქსიმალური ეფექტური გამოყენების მიზნით;
3. დამტკიცებული და დამკვეთთა მომავალი მოთხოვნების გაგება IT–რესურსებში, პროგნოზების ფორმირება სამომავლო მოთხოვნებისთვის;
4. გავლენა მოთხოვნის მართვის პროცესზე;
5. სიმძლავრეების უზრუნველყოფის გეგმის ფორმირება;
6. დახმარება პრობლემების და ინციდენტების პროგნოზირებაში;

7. სერვისების და მათი კომპონენტების პროაქტიური სრულყოფა იქ, სადაც ეს ეკონომიკურად გამართლებულია ან მოითხოვება ბიზნესით.

პროცესი აწვდის სერვისების მიმწოდებელს შემდეგ ინფორმაციას:

1. რომელი კომპონენტები უნდა განახლდეს (მაგალითად, მეტი მეხსერება ან უფრო სწრაფი პროცესორები);
2. როდის განახლდეს კოპმპონენტები;
3. რა ეღირება კომპონენტების განახლება.

მრავალი პროცესი დამოკიდებულია სიმძლავრეების მართვაზე და იქნება ნაკლებეფექტური, თუ არ გამოიყენებს ამ ინფორმაციას. მაგალითად, ცვლილებების მართვამ უნდა მიიღოს ინფორმაცია სიმძლავრეების მართვიდან რომელიმე ცვლილების განხორციელებამდე, რადგან მათ შეუძლია იმოქმედოს სიმძლავრეების წვდომაზე.

სწორად ორგანიზებული სიმძლავრეების მართვა საშუალებას იძლევა პროგნოზი გაკეთდეს ბიზნესის განსხვავებულ მოვლენებზე მანამ, სანამ ისინი ფაქტობრივად მოხდება. ეს ხელს უწყობს ავიცილოთ თავიდან არასასურველი სიურპრიზები სერვისების და მათი კომპონენტების მწარმოებლურობასთან მიმართებით.

სიმძლავრეების მართვა მჭიდროდ ურთიერთქმედებს სტრატეგიის აგების ეტაპთან და დაგეგმვის სხვა პროცესებთან. სიმძლავრეების მართვას უნდა ესმოდეს და აანალიზებდეს ბიზნესის და IT-ს მოკლევადიან, საშუალოვადიან და გრძელვადიან გეგმებს. აგრეთვე მან უნდა მიაყურადოს ტრენდებს, ახალ იდეებს და ტექნოლოგიებს, რომლებიც გამოიყენება ამ გეგმების შესასრულებლად.

სიმძლავრეების მართვა უნდა უზრუნველყოფდეს შემდეგს:

1. ხარჯების და საჭირო რესურსების ბალანსს – უზრუნველყოს ის, რომ პროცესების მწარმოებლურობა იყოს გამართლებული ხარჯების თვალსაზრისით და უზრუნველყოს რესურსების უფრო ეფექტური გამოყენება;

2. მოთხოვნის და წინადადებების ბალანსი – უთვალთვალოს IT-ის მიერ წარმოდგენილ წინადადებებს, რათა დააკმაყოფილოს მოთხოვნა დამკვეთების მხრიდან ამჟამადაც და მომავალშიც.

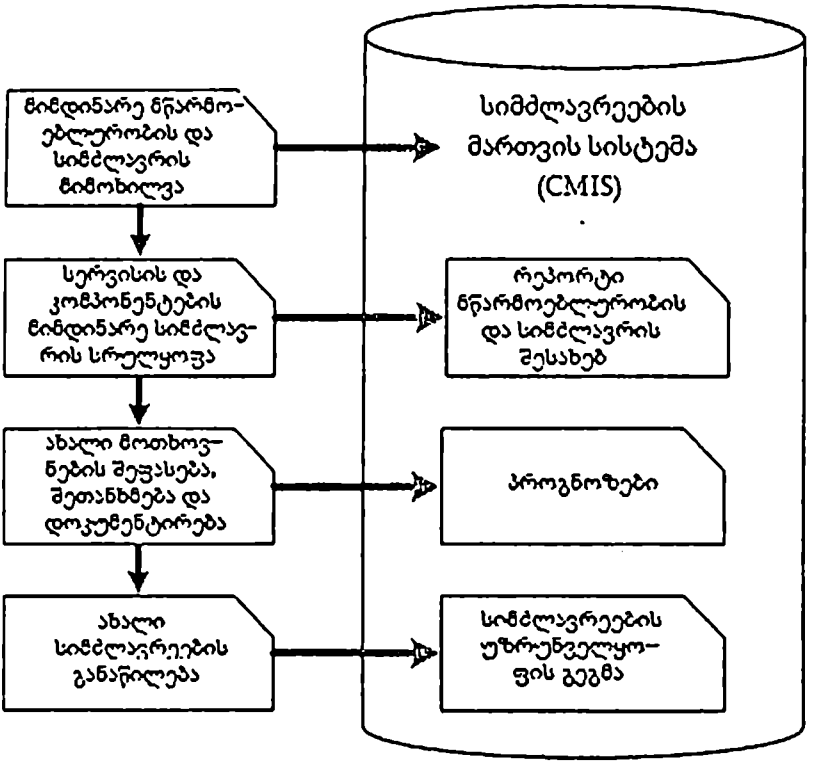
სიმძლავრეების მართვა არის უწყვეტი პროცესი, თანმხლები სერვისთან მთელი სასიცოცხლო ციკლის განმავლობაში. იგი ოპტიმიზაციას უკეთებს არსებული რესურსების გამოყენებას და გეგმავს მათ განაწილებას მომავალში (ნახ.14.3).

სიმძლავრეების მართვის ფარგლებში გამოყოფენ სამ ქვეპროცესს:

1. ბიზნესის სიმძლავრეების მართვა – გადაყავს ბიზნესის მოთხოვნილებანი და გეგმები სერვისების და ინფრასტრუქტურის მოთხოვნებში;

2. სერვისების სიმძლავრეების მართვა – მართავს, აკონტროლებს და აპროგნოზებს ექსპლუატაციაში არსებულ სერვისების მწარმოებლურობას და სიმძლავრეს.

3. კომპონენტების სიმძლავრეების მართვა – მართავს, აკონტროლებს და აპროგნოზებს ცალკეული კომპონენტების მწარმოებლურობას და სიმძლავრეს.



ნახ.**14.3.** სიმძლავრეების მართვის სისტემა

ამ პროცესებს ბევრი საერთო აქვთ, მაგრამ თითოეულ პროცესს თავისი ფოკუსი გააჩნია. ბიზნესის სიმძლავრეების მართვა ფოკუსირდება ბიზნესის მიმდინარე და სამომავლო მოთხოვნებზე. სერვისების სიმძლავრეების მართვა ფოკუსირდება არსებული სერვისების უზრუნველსაყოფად ბიზნესის მხარდასაჭერად. კომპონენტების სიმძლავრეების მართვა კი – ინფრასტრუქტურაზე, რომელიც უზრუნველყოფს სერვისების

გამოყენებას. 14.4 ნახაზზე ნაჩვენებია თითოეული ქვეპროცესის როლი.

გამოყოფენ რეაქტიურ და პროაქტიურ ღონისძიებებს სიმძლავრეების მართვის პროცესის ფარგლებში.

პროაქტიურ ღონისძიებებს მიეკუთვნება:

1. „წინაგამოცნობით" წარმოქმნილი საკითხები, დაკავშირებული რესურსების დეფიციტთან;

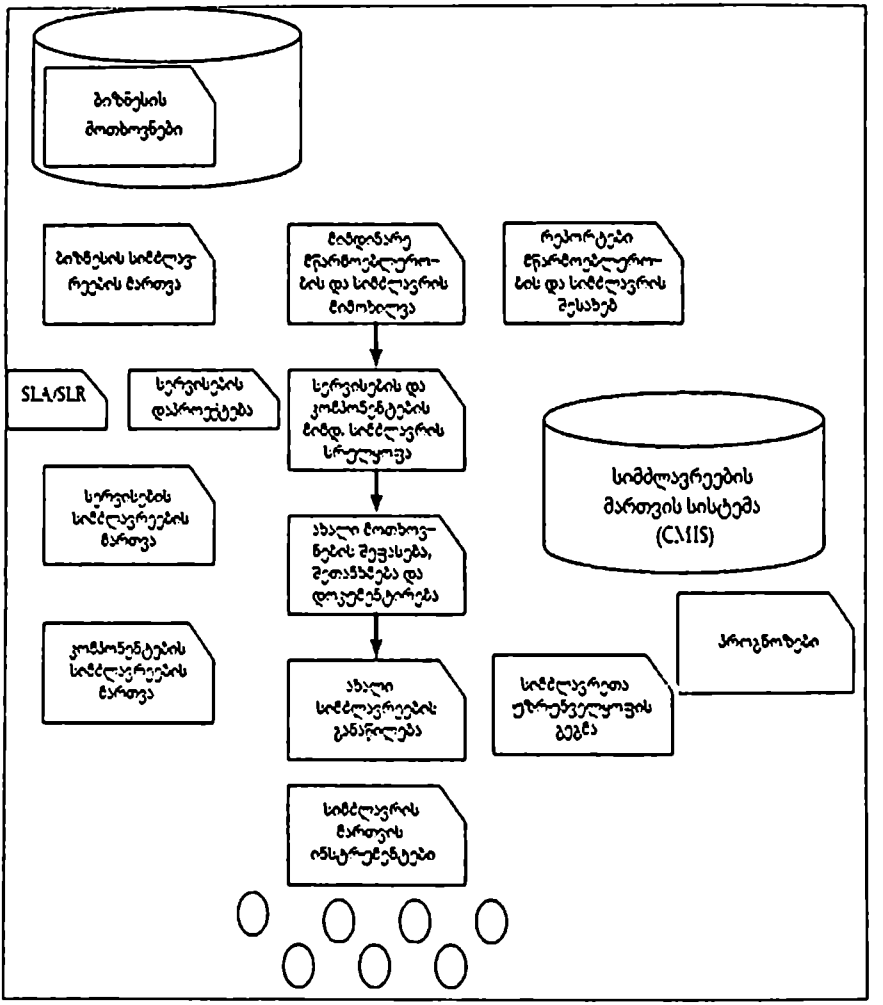
2. რესურსების გამოყენების დღევანდელი ტენდენციების გამოყოფა და რესურსებზე სამომავლო მოთხოვნების შეფასება. უკანასკნელი გამოისახება გეგმების განახლებასა და სრულყოფაში სასაზღვრო მნიშვნელობათა და რესურსების გამოყენების მიმართულებების ტერმინებში;

3. მოდელირება და ანალიზი ცვლილებათა ტენდენციების IT–სერვისებში, მათ შორის ცვლილებების განსაზღვრა რესურსებში, რომლებიც უნდა ჩატარდეს მომავალში;

4. უზრუნველყოფა იმის, რომ განახლებები იქნება დაფინანსებული, დაგეგმილი და გატარებული მანამ, სანამ იქნება დარღვეული SLA ან გაჩნდება რაღაც პრობლემები მწარმოებლურობასთან;

5. შესაძლებლობათა აქტიური ძებნა სერვისების მწარმოებლურობის სრულყოფისთვის იქ, სადაც იგი ეკონომიკურად გამართლებულია;

6. სერვისების მწარმოებლურობის და მათი კომპონენტების აწყობა და ოპტიმიზაცია.



ნახ.14.4. ქვეპროცესები სიმძლავრეების მართვის ფარგლებში

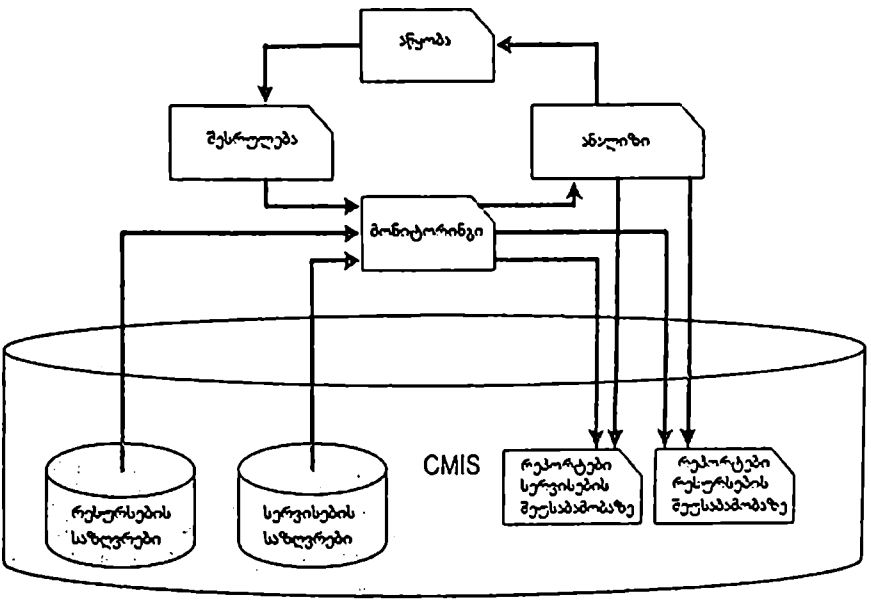
რეაქტიური ღონისძიებები შემდეგია:

1. მონიტორინგი, გაზომვა და აღრიცხვის წარმოება სერვისების და მათი კომპონენტების მიმდინარე მწარმოებლურობისთვის;

2. რეაგირება ყველა მოვლენაზე, რომლებიც დაკავშირებულია მწარმოებლურობის სასაზღვრო სიდიდეებთან, და შემდგომი ინიციალიზაცია კორექტული ზომების;

3. რეაგირება ყველა პრობლემაზე, რომლებიც დაკავშირებულია მწარმოებლურობასთან და დახმარება მათ გადაწყვეტაში.

აქტიურობა სიმძლავრეების მართვის პროცესის ფარგლებში ნაჩვენებია 14.5 ნახაზზე.



ნახ.14.5. ქმედება სიმძლავრეების მართვის პროცესის ფარგლებში

რაც უფრო ეფექტურად ტარდება პროაქტიური ღონისძიებანი, მით უფრო ნაკლები რეაქტიური ქმედებები იქნება საჭირო სიმძლავრეების მართვის მხრიდან. ქმედებები თითოეული განხილული ქვეპროცესისთვის განსხვავებულია. მთავარი განსხვავებაა ინფორმაცია, რომელიც მონიტორინგშია და იკრიბება. მაგალითად, ცალკეული კომპონენტების უტილიზაციის დონე – პროცესორების, დისკოების, ქსელური მოწყობილობის – კომპონენტების სიმძლავრეების მართვის საკითხებია.

ტრანზაქცია გამტარუნარიანობასა და პასუხის დროის მაჩვენებლებს შორის – სერვისების სიმძლავრეების მართვის საკითხებია. ბიზნესის სიმძლავრეების მართვის საკითხებს მიეკუთვნება ტრანზაქცია ონლაინ-სერვისის და ბიზნეს-მოცულობების მაჩვენებლებს შორის, მაგალითად, გაყიდვების გაზრდის ან მომსახურებული შეკვეთების ტერმინებში.

სიმძლავრეების მართვის პროცესის შესასვლელებია:

1. ინფორმაცია ბიზნესიდან – ორგანიზაციის სტრატეგიები და გეგმები, მათი ახლანდელი და მომავალი მოთხოვნები;

2. ინფორმაცია IT-დან – IT-სტრატეგიები, გეგმები და ბიუჯეტი (ეს ინფორმაცია ფარავს ყველა საკითხს, დაკავშირებულს ტექნოლოგიებთან, ინფრასტრუქტურასთან, გარემოსთან, მონაცემებთან და აპლიკაციებთან) და მათი კავშირები ბიზნესის სტრატეგიებთან და გეგმებთან;

3. ინფორმაცია კომპონენტების მწარმოებლურობასა და სიმძლავრეზე;

4. პრობლემები, დაკავშირებული სერვისის მწარმოებლურობასთან – ინციდენტები და პრობლემები, დაკავშირებული ცუდ მწარმოებლურობასთან;

5. ინფორმაცია სერვისებზე – ინფორმაცია *SLM-დან,* მათ შორის სერვისების კატალოგიდან და სერვისების პორტფელიდან, სერვისების მიზნობრივი მაჩვენებლები SLA და *SLR-ში* და ა.შ.

6. ფინანსური ინფორმაცია – ინფორმაცია ფინანსების მართვის პროცესიდან, მათ შორის სერვისების, რესურსების, კომპონენტების და განახლებების უზრუნველყოფის ღირებულება;

7. ინფორმაცია ცვლილებების შესახებ – ცვლილებების მართვის პროცესიდან, მათ შორის ცვლილებათა განრიგი, ცვლილებათა გავლენის შეფასება სიმძლავრეზე;

8. ინფორმაცია მწარმოებლურობაზე: ინფორმაცია სერვისების და მათი კომპონენტების მიმდინარე მწარმოებლურობაზე;

9. ინფორმაცია მიმდინარე კავშირების შესახებ ბიზნესსა და სერვისებს, დამხმარე სერვისებს და ტექნოლოგიებს შორის;

10. ინფორმაცია სამუშო დატვირთვაზე. სამუშაო დატვირთვა (*Workload*) – რესურსები, რომლებიც აუცილებელია სერვისის განსაზღვრული ნაწილის უზრუნველსაყოფად. სამუშაო დატვირთვა შეიძლება დაიყოს კატეგორიებად მომხმარებელთა მიხედვით, ჯგუფებად ან ფუნქციებად – ცალკე სერვისის ფარგლებში;

სიმძლავრეების მართვის გამოსასვლელებია:

1. სიმძლავრეების მართვის სისტემა (Capacity Management Information System ან CMIS) – ვირტუალური საცავი ყველა მონაცემის სიმძლავრეთა მართვის ფარგლებში, ჩვეულებრივ, აქვს განაწილებული არქიტექტურა.

2. სიმძლავრეთა უზრუნველყოფის გეგმა;

3. ინფორმაცია და რეპორტები სერვისის უზრუნველყოფაზე გამოიყენება სხვადასხვა პროცესების მიერ. მაგალითად, ფინანსების მართვის პროცესის დასახმარებლად იმის განსაზღვრისთვის, თუ რამდენი თანხა უნდა გამოიყოს ინფრასტრუქტურის განახლებისთვის;

4. სამუშაო დატვირთვის ანალიზი და რეპორტები მათ შესახებ. გამოიყენება ოპერაციული მართვის პერსონალის მიერ

ცვლილებათა შეფასების და შესრულებისათვის. ამავე დროს სიმძლავრეების მართვა იძლევა განრიგს იმის შესახებ, როდის გამოიყენება სერვისები, როგორია სამუშაო დატვირთვა, რა ახორციელებს რესურსების უფრო ეფექტურად გამოყენებას;

5. რეპორტები „შემთხვევათა მიხედვით" მწარმოებლურობის და სიმძლავრის შესახებ (ანუ არა განრიგით, არამედ კონკრეტული შემთხვევით). გამოიყენება სიმძლავრეების მართვის ყველა სფეროს მიერ, IT-ის და ბიზნესით პრობლემების ანალიზის და გადაწყვეტისთვის;.

6. პროგნოზები, რომლებიც გამოიყენება ყველა სფეროში ანალიზის და პროგნოზისთვის, განსაკუთრებით, ხელმძღვანელობის მიერ გადაწყვეტილების მისაღებად.

მაჩვენებლები, რომლებიც აფასებს სიმძლავრეების მართვის ეფექტურობას, უნდა შეიცავდეს:

- ზუსტ ბიზნესპროგნოზებს:
  - პროგნოზის დროული ფორმირება სამუშაოს დატვირთვის შესახებ;
  - პროგნოზების სიზუსტე პროცენტებში, ბიზნესისთვის;
  - ბიზნესგეგმების დროული გაერთიანება სიმძლავრეების უზრუნველყოფის გეგმასთან;
  - განსხვავების რაოდენობის შემცირება ბიზნესგეგმასა და სიმძლავრეების უზრუნველყოფის გეგმას შორის.
- ტექნოლოგიის ცოდნა, მათ შორის მომავლის:
  - სერვისების და მათი კომპონენტების მწარმოებლურობის და გამტარუნარიანობის მონიტორინგის სრულყოფა;
  - დანერგვის დროული დასაბუთება და ახალი ტექნოლოგიების დანერგვა ბიზნესის მოთხოვნების შესაბამისად;

- ძველი ტექნოლოგიების გამოყენების შემცირება, რომლებიც იწვევს მხარდაჭერის და მწარმოებლურობის პრობლემებს;

- ეკონომიკური ეფექტურობის დემონსტრირების უნარი:
  - შემცირება შემთხვევების „რაღაცის ყიდვა ბოლო მომენტში" სასწრაფო მწარმოებლურობის პრობლემების გადასაწყვეტად;
  - სერვისების და კომპონენტების ფუნქციონირების შემცირება მათი შესაძლებლობების ზღვარზე მწარმოებლურობის და სიმძლავრის მიხედვით;
  - ზუსტი პროგნოზები რესურსების გამოყენების შესახებ;
  - დარღვევების შემთხვევათა შემცირება ბიზნესპროცესებში, არასაკმარისი სიმძლავრის გამო IT-ის მხრიდან;
  - ხარჯების შემცირება სიმძლავრეთა უზრუნველყოფის გეგმის ფორმირებაზე.

- IT აუცილებელი სიმძლავრის უზრუნველყოფის შესაძლებლობა ბიზნესის მოთხოვნილებათა დასაკმაყოფილებლად:

1. ინციდენტების პრეცენტული რაოდენობის შემცირება, ცუდ მწარმოებლურობასთან დაკავშირებით;
2. ბიზნესის დანაკარგების პროცენტული შემცირება, სიმძლავრის უკმარობის გამო.
3. „ხვრელების" რაოდენობის შემცირება SLA-ში, სერვისების და მათი კომპონენტების ცუდი მწარმოებლურობის გამო.

ინფორმაციის რაოდენობა, ფორმირებული სიმძლავრეების მართვის განხილული სამი ქვეპროცესის ფარგლებში, ძალზე დიდია და ძნელად ემორჩილება ანალიზს. ამიტომაც აუცილებელია ძალების მობილიზება მათი გამოყენების უფრო მნიშვნელოვან რესურსებსა და საკითხებზე.

14.4. წვდომის მართვა

წვდომა (Availability) – ესაა შესაძლებლობა კონფიგურაციული ერთეულის ან სერვისისა, შეასრულოს შეთანხმებული ფუნქცია, როცა ეს მოითხოვება. წვდომა განისაზღვრება საიმედოობის, თანხლების, მომსახურების, მწარმოებლურობის და უსაფრთხოების საშუალებით.

წვდომის მართვა (Availability Management) – ესაა პროცესი, პასუხისმგებელი სერვისების განსაზღვრაზე, ანალიზზე, დაგეგმვაზე, გაზომვაზე და წვდომის ყველა ასპექტის სრულყოფაზე. წვდომის მართვა პასუხისმგებელია იმაზე, რომ მთელი ინფასტრუქტურა, პროცესები, საშუალებები, როლები და ა.შ. შესაბამისობაში იყოს სერვისების დონის შეთანხმებულ მიზნობრივ მაჩვენებლებთან წვდომის ნაწილში [11].

მთავარი მიზანი წვდომის მართვისა არის იმის გარანტია, რომ სერვისის წვდომის დონე იყოს ეფექტური ხარჯების მიხედვით და შეესაბამებოდეს ბიზნესის მიმდინარე და სამომავლო მოთხოვნილებებს. ამ პროცესის შუალედური მიზნები შემდეგია:

1. წვდომის მართვის გეგმის ფორმირება. წვდომის მართვის გეგმა (Availability Plan) – ესაა გეგმა, რომელიც უზრუნველყოფს სერვისისთვის წვდომის მიმდინარე და სამომავლო მოთხოვნილებების ეფექტურ შესრულებას ხარჯების მიხედვით [11];

2. რეკომენდაციების წარმოდგენა და ხელმძღვანელობა ბიზნესის და IT-ის სხვა სფეროებისთვის ყველა საკითხში, დაკავშირებულს წვდომასთან;

3. უზრუნველყოფა იმის, რომ სერვისებმა მიაღწიოს დადგენილ მიზნობრივ მაჩვენებლებს წვდომის კონტექსტში, სერვისების და რესურსების მართვის გზით;

4. დახმარება პრობლემების დიაგნოსტირებასა და გადაწყვეტაში, დაკავშირებული წვდომასთან;

5. ცვლილებების გავლენის შეფასება წვდომის მართვის გეგმაზე;

6. უზრუნველყოფა იმისა, რომ პროაქტიური საშუალებები წვდომის სრულყოფისათვის დანერგილი იყოს იქ, სადაც ეს იქნება ეფექტურად გამართლებული.

წვდომის მართვის პროცესი უნდა მოიცავდეს შემდეგ ქმედებებს:

1. მონიტორინგი ყველა ასპექტის, დაკავშირებული სერვისების და მხარდამჭერი კომპონენტების წვდომასა და საიმედოობასთან;

2. მეთოდების, ტექნიკის და გამოთვლების ერთობლიობის მართვა, რომელიც აუცილებელია ანგარიშგების და გაზომვების განსახორციელებლად;

3. დახმარება რისკების შესაფასებლად და მმართველ საქმიანობაში;

4. გაზომვების და ანალიზის შედეგების შეკრება, რეგულარული და სპეციალური (ერთეული შემთხვევებისთვის) რეპორტების ფორმირება სერვისების და მათი კომპონენტების წვდომის შესახებ;

5. ბიზნესის მიმდინარე და სამომავლო მოთხოვნილებათა გაგება სერვისების და მათი კომპონენტების წვდომის შესახებ;

6. გავლენა სერვისების დაპროექტებაზე მათი მაქსიმალური შესაბამისობისათვის ბიზნესის მოთხოვნილებებთან;

7. წვდომის მართვის გეგმის ფორმირება, რომელიც საშუალებას მისცემს მიმწოდებელს მხარი დაუჭიროს და სრულყოს სერვისების წვდომის დონე მიზნობრივ მაჩვენებლებთან შესაბამისობაში, შეთანხმებული SLA-ში. იგი ასევე დაეხმარება

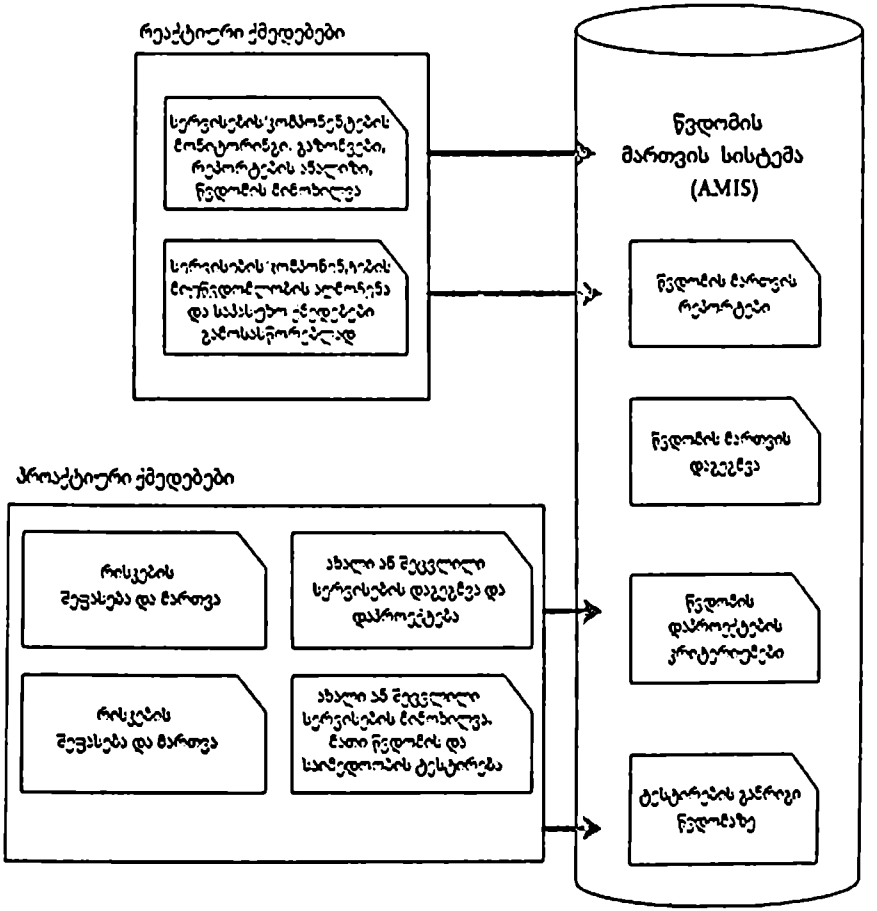
წვდომის დონეების დაგეგმვასა და პროგნოზირებაში, რომლებიც შეიძლება მომავალში გახდეს საჭირო.

8. ტესტების განრიგის მართვა ყველა კომპონენტისთვის წვდომის საკითხზე;

9. დახმარება პრობლემების და საკითხების იდენტიფიკაციასა და გადაწყვეტაში, დაკავშირებული სერვისების და მათი კომპონენტების მიუწვდომლობის შესახებ;

10. პროაქტიური სრულყოფა სერვისების წვდომისა იქ, სადაც ეს ეკონომიკურად ეფექტურია და შეესაბამება ბიზნესის მოთხოვნილებებს [10].

დამკვეთთა კმაყოფილება ბევრადაა დამოკიდებული სერვისების წვდომაზე, ამიტომაც წვდომის მართვის პროცესი ღებულობს განსაკუთრებულ მნიშვნელობას. ისევე, როგორც სიმძლავრეების მართვა, წვდომის მართვაც უნდა იმყოფებოდეს სერვისის სასიცოცხლო ციკლის ყველა ეტაპზე. წვდომის მართვა მოიცავს პროაქტიურ და რეაქტიურ ქმედებებს (ნახ.14.6).



ნახ.14.6. წვდომის მართვის პროცესი

14.4.1. რექატიური და პროაქტიური ქმედებები

რეაქტიური ქმედებებია მონიტორინგი, გაზომვა, ანალიზი, რეპორტების და მიმოხილვების ფორმირება სხვადასხვა ასპექტში, დაკავშირებული წვდომასთან. ისინი უზრუნველყოფენ, რომ წვდომის მიზნობრივი მაჩვენებლები მიღწეულია და გაზომილი.

პროაქტიური ქმედებებია რეკომენდაციების, გეგმების, დაპროექტებისთვის დოკუმენტების და ახალი და შეცვლილი სერვისების კრიტერიუმების ფორმირება. აქვე შედის ქმედებები სერვისების მუდმივი სრულყოფის და რისკების შემცირებისა იქ, სადაც ეს ეკონომიკურად გამართლებულია.

წვდომის მართვა შედგება ორი ურთიერთდაკავშირებული დონისგან:

1. სერვისების წვდომა – მოიცავს ყველა საკითხს, დაკავშირებულს სერვისების წვდომასთან და მიუწვდომლობასთან, აგრეთვე ცალკეული კომპონენტის წვდომის (ან მიუწვდომლობის) გავლენა მთლიანი სერვისის წვდომაზე;
2. კომპონენტების წვდომა – მოიცავს ყველა საკითხს, დაკავშირებულს კომპონენტების წვდომასთან და მიუწვდომლობასთან;

წვდომის მართვა ეფუძნება მონიტორინგს, ანალიზს, გაზომვებს და რეპორტების ფორმირებას შემდეგი კომპონენტების შესახებ:

1. წვდომა – შესაძლებლობა სერვისის, კომპონენტის ან კონფიგურაციული ერთეულის, შეასრულოს შეთანხმებული ფუნქცია მაშინ, როცა ეს მოითხოვება. იზომება პროცენტებში შემდეგი ფორმულით:

წვდომა (%) = (სერვისის წარმოდგენის შეთანხმებული დრო –
- მოცდენის დრო)/
/სერვისის წარმოდგენის შეთანხმებული დრო *100.

ბუნებრივია, რომ მოცდენის დრო ჩაერთვება ანგარიშში მოცდენის არსებობისას.

თუ ის არაა, მაშინ წვდომა იქნება 100 %-იანი.

2. საიმედოობა (Reliability) – ზომა იმისა, თუ რამდენად დიდხანს შეძლებს შეასრულოს შეთანხმებული ფუნქცია უწყვეტად სერვისმა, კომპონენტმა ან კონფიგურაციულმა ერთეულმა. სერვისის საიმედოობა შეიძლება ამაღლდეს ორი ხერხით. პირველი მდგომარეობს სერვისის მდგრადობის (სტაბილურობის) ამაღლებაში ცალკეული კომპონენტების მტყუნებაზე, მეორე – ცალკეული კომპონენტების საიმედოობის გაზრდით. საიმედოობა იზომება ორი მაჩვენებლით:

- საშუალო დრო ინციდენტებს შორის (Mean Time Between Service Incidents ან MTBSI) – ესაა საშუალო დრო სისტემის ან სერვისის ერთი მტყუნების მომენტიდან შემდეგ მტყუნებამდე [11].

საიმედოობა(MTBSI საათებში)=წვდომის დრო
საათებში/მტყუნებათა რაოდენობა.

- საშუალო დრო მტყუნებებს შორის (Mean Time Between Failures ან MTBF) – ესაა საშუალო დრო, რომელშიც სერვისი ან კონფიგურაციული ერთეული შეძლებს თავისი ფუნქციების შესრულებას შესვენების გარეშე. იზომება სამუშაოს დაწყებიდან მომდევნო მტყუნების მომენტამდე.

საიმედოობა(*MTBF* საათებში) = (წვდომის დრო საათებში –
– მოცდენის საერთო დრო საათებში)/მტყუნებათა რაოდენობა.

3. თანხლება – სერვისის ან კონფიგურაციული ერთეულის ნორმალური მუშაობის სწრაფად და ეფექტურად აღდგენის

საზომი, მტყუნების შემდეგ. იზომება სერვისის აღდგენის საშუალო დროის დახმარებით. სერვისის აღდგენის საშუალო დრო (Mean Time to Restore Service ან MTRS) – საჭიროა სერვისის ან კონფიგურაციული ერთეულის აღსადგენად მტყუნების შემდეგ. MTRS იზომება მტყუნების მომენტიდან ნორმალური მუშაობის სრულ აღდგენამდე.

თანხლება(**MTRS** საათებში) = მოცდენის სრული დრო საათებში /მტყუნებათა რაოდენობა.

მაგალითი. დავუშვათ, რომ სერვისს იყენებენ 7 დღის განმავლობაში 24 საათით დღე-ღამეში. მან იმუშავა 7010 საათი. ამ პერიოდში 2-ჯერ მოხდა მტყუნება. პირველის შემდეგ მოცდენის დრომ შეადგინა 10 საათი, მეორის შემდეგ – 5 საათი.

წვდომა = **(7010-(5+10))/7010*100=99,78 %** ,
საიმედოობა **(MTBSI)= 7010/2 = 3505** ,
საიმედოობა (MTBF) = **(7010-(5+10))/2 = 3497.5** საათი,
თანხლება **(MTRS) = (5+10)/2=7.5** საათი.

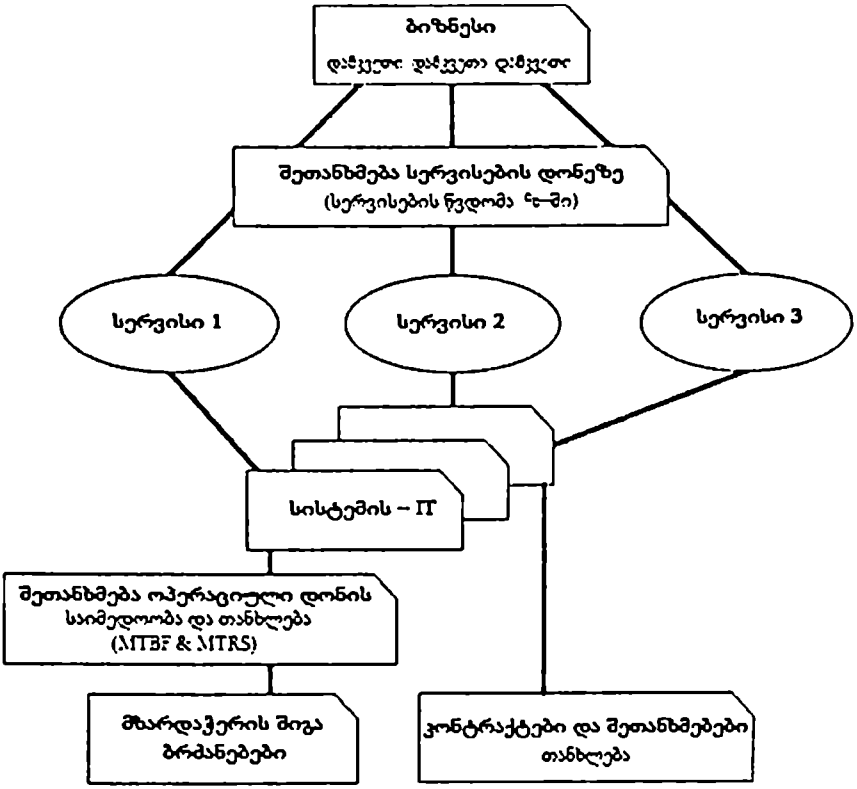
4. მომსახურება – მესამე მხარის მიმწოდებლის შესაძლებლობა, შეასრულოს სახელშეკრულებო პირობები. ეს ხელშეკრულება მოიცავს საიმედოოდბის, თანხლების ან წვდომის შეთანხმებულ დონეებს კონფიგურაციული ერთეულისათვის.

14.7 ნახაზზე მოცემულია წვდომის კომპონენტები და მათი ურთიერთკავშირი.

14.4.2. კრიტიკული ბიზნესფუნქცია

პროცესების დაპროექტების კონტექსტში შემოიტანება ტერმინი კრიტიკული ბიზნესფუნქცია (Vital Business Function ან VBF) – ესაა ფუნქცია ბიზნესპროცესში, კრიტიკული ბიზნესის წამატებისთვის.

რაც მაღალია ფუნქციის კრიტიკულობა ბიზნესისთვის, მით უფრო მაღალი საიმედოობა და წვდომა უნდა იყოს უზრუნველყოფილი.



ნახ.14.7. წვდომის ტერმინები და მათი ურთიერთკავშირი

ზოგიერთი VBF მოითხოვს განსაკუთრებულ მიდგომას მათი მომსახურების სერვისების დასაპროექტებლად:

• მაღალი წვდომა – სერვისი მახასიათებელია, რომელიც ასახავს, რომ სერვისის კომპონენტების მტყუნებათა შედეგები მინიმუმამდეა დაყვანილი და/ან შეუმჩნეველია მომხმარებლისთვის;

• მდგრადობა მტყუნებებისადმი – სერვისის, კომპონენტის ან კონფიგურაციული ერთეულის შესაძლებლობაა, გააგრძელოს მუშაობა რომელიმე კომპონენტის მტყუნების შემდეგაც;

• უწყვეტი ექსპლუატაცია – მიდგომა დაპროექტებისადმი, მიმართული სერვისების დაგეგმილი მოცდენების აღმოსაფხვრელად. ცალკეული კონფიგურაციული ერთეული შეიძლება გაითიშოს მაშინ, როცა სერვისი რჩება ხელმისაწვდომი.

• უწყვეტი წვდომა – მიდგომა დაპროექტებისადმი, მიმართული წვდომის 100%-იანი მიღწევისათვის. უწყვეტად მისაწვდომ სერვისს არ აქვს საგეგმო და არასაგეგმო მოცდენები.

წვდომის მართვის პროცესის შესასვლელებია:

1. ინფორმაცია ბიზნესიდან – ორგანიზაციის სტრატეგია, გეგმები და ბიუჯეტი, მისი მიმდინარე და სამომავლო მოთხოვნები, მათ შორის მოთხოვნები ახალ ან შეცვლილ სერვისთა წვდომაზე;

2. ინფორმაცია ბიზნესზე გავლენის ანალიზის შესახებ, მათ შორის VBF ჩამონათვლის განსაზღვრა;

3. ინფორმაცია ადრე ჩატარებული რისკების და შეფასებათა ანალიზის შესახებ;

4. ინფორმაცია სერვისების შესახებ, სერვისების პორტფელიდან და სერვისების კატალოგიდან, *SLM-დან*, მათ შორის სერვისთა მიზნობრივი მაჩვენებლები SLA და *SLR-დან*;

5. ფინანსური ინფორმაცია დაფინანსების მართვისგან – სერვისების უზრუნველყოფის ღირებულება და ხარჯები რესურსებზე;

6. ინფორმაცია რელიზების და ცვლილებების შესახებ, ცვლილებათა მართვის და რელიზების მართვის პროცესებიდან, კერძოდ, რელიზების და ცვლილებების განრიგები;

7. ინფორმაცია კონფიგურაციათა მართვიდან, ბიზნესის კავშირის შესახებ სერვისებთან, დამხმარე სერვისებთან და ტექნოლოგიებთან;

8. სერვისების მიზნობრივი მაჩვენებლები SLA, *SLR*, OLA - დან და სხვა კონტრაქტებიდან;

9. ინფორმაცია კომპონენტების შესახებ – წვდომა, საიმედოობა და თანხლება კომპონენტებისთვის, რომლებიც სერვისის საფუძველია;

10. ინფორმაცია ტექნოლოგიების შესახებ – ტოპოლოგია და კომპონენეტების კავშირი, ასევე ახალი ტექნოლოგიების შესაძლებლობანი;

11. ინფორმაცია მწარმოებლურობის შესახებ წარსულში;

12. ინფორმაცია მიუწვდომლობის შემთხვევების და მტყუნებების შესახებ.

წვდომის მართვის პროცესის გამოსასვლელებია:

1. წვდომის მართვის სისტემა (**Availability Management Information System** ან AMIS) – ყველა მონაცემის ვირტუალური საცავი, რომელსაც აკონტროლებს წვდომის მართვა. ჩვეულებრივ, ესაა ფიზიკურად განაწილებული საცავი;

2. წვდომის მართვის გეგმა;

3. კრიტერიუმები წვდომის დასაპროექტებლად, რომლებიც იძლევა მიზნობრივ მაჩვენებლებს;

4. რეპორტები სერვისთა წვდომის, საიმედოობის და თანხლების შესახებ, მიზნობრივი მაჩვენებლების მიღწევის კონტექსტში;

5. რეპორტები კომპონენტების წვდომის, საიმედოობის და თანხლების შესახებ, მიზნობრივი მაჩვენებლების მიღწევის კონტექსტში;

6. რისკების გადასინჯული მიმოხილვა, რისკების სიის განახლება;

7. მოთხოვნები მონიტორინგის, მართვის და ანგარიშგებისადმი იმ სერვისებთან მიმართებით, რომლებიც გარანტიას იძლევა, რომ ნებისმიერი გადახრები წვდომაში, საიმედოობასა და თანხლებაში იქნება აღმოჩენილი და აღმოფხვრილი;

8. წვდომის, საიმედოობის და თანხლების ტესტირების ჩატარების განრიგი;

9. სერვისების და მათი კომპონენტების გეგმიური და რეაქტიური მომსახურების განრიგი;

10. სერვისის მოსალოდნელი მოცდენის ფორმირება. სერვისის მოსალოდნელი მოცდენა (Projected Service Outage *или* PSO) – ესაა დოკუმენტი, რომელიც განსაზღვრავს დაგეგმილი ცვლილებების, მომსახურების ქმედების და ტესტირების გეგმის გავლენას სერვისების შეთანხმებულ დონეზე;

11. პროაქტიური ტექნოლოგიების დეტალური აღწერა, რომელიც გამოყენებულ იქნება საიმედოობის და წვდომის სრულყოფისთვის;

12. ქმედებები სერვისების სრულყოფისთვის SIP-ში ჩასართავად.

14.4.3. წვდომის მართვის პროცესის ეფექტურობის შეფასება

წვდომის მართვის პროცესის ეფექტურობის შესაფასებლად შეიძლება გამოყენებულ იქნას მწარმოებლურობის საკვანძო მაჩვენებელთა სიმრავლე, მაგალითად:

- სერვისების წვდომის და საიმედოობის მართვა:
  - პროცენტული შემცირება სერვისების და მათი კომპონენტების მიუწვდომლობისა;
  - პროცენტული გაზრდა სერვისების და მათი კომპონენტების საიმედოობისა;
  - ეფექტური გადახედვა SLA, OLA და სხვა ფუძემდებლური კონტრაქტების და ხელშეკრულებებისა;
  - პროცენტული შემცირება მტყუნებათა რაოდენობის და მათი გავლენისა;
  - *MTBF-ის გაზრდა;*
  - MTBSI-ის სრულყოფა;
  - MTRS-ის სრულყოფა.
- ბიზნესის მოთხოვნილებათა დაკმაყოფილება სერვისების წვდომაში:
  - პროცენტული შემცირება სერვისების მიუწვდომლობისა;
  - პროცენტული შემცირება მოცდენის ღირებულებისა ბიზნესისთვის;
  - პროცენტული შემცირება მტყუნებებისა დროში, რომელიც კრიტიკულია ბიზნესისთვის;
  - პროცენტული გაზრდა ბიზნესის დაკმაყოფილებისა.
- ოპტიმალური დანახარჯები სერვისების წვდომის უზრუნველყოფაზე:
  - პროცენტული შემცირება მიუწვდომლობის ღირებულებისა;

- დროული დამთავრება რისკების ანალიზის და სისტემის მიმოხილვისა;
- დროული დამთავრება რისკების ანალიზისა – „ხარჯები–სარგებელი“;
- პროცენტული შემცირება კომპონენტებისა და მესამე მხარის სერვისების მტყუნებებისა;
- სისტემის ანალიზის დროის შემცირება საიმედოობაზე;
- დროის შემცირება წვდომის მართვის გეგმის ფორმირებაზე;
- მმართველობითი ანგარიშების დროული ფორმირება.

წვდომის მართვამ უნდა დააფორმიროს და მართოს *AMIS*. ეს არის ცენტრალური საცავი მთელი ინფორმაციის, დოკუმენტების, მეტრიკების, და ა.შ. შესანახად, რომლებიც აუცილებელია წვდომის მართვის შესასრულებლად.

რეკომენდებულია, წვდომის მართვის გეგმის ფორმირება ერთი-ორი წლის ვადით, დეტალიზებულად – პირველი 6 თვით. გეგმა რეგულარულად უნდა გადაისინჯოს და განახლდეს.

ძირითად რისკად წვდომის მართვის პროცესისთვის, ისევე როგორც წინა პროცესებისთვის, განიხილება ინფორმაციის არასაკმარისობა ან უზუსტობა, რომელიც შემოდის ბიზნესიდან და IT-დან.

15. სერვისების უწყვეტობის და ინფორმაციული უსაფრთხოების მართვა დაპროექტების ეტაპის ჩარჩოებში. მიმწოდებლების მართვა

15.1. სერვისების უწყვეტობის მართვა

სერვისების უწყვეტობის მართვა (IT Service Continuity Management ან ITSCM) – ესაა პროცესი, პასუხისმგებელი *რისკების მართვაზე*, რომლებიც გავლენას ახდენს სერვისებზე. ITSCM უზრუნველყოფს შესაძლებლობას, რომ სერვისების მიმწოდებელს მუდმივად მიეცეს სერვისების მინიმალურად შეთანხმებული დონე, რისკების შემცირების გზით მისაღებ დონემდე, აგრეთვე სერვისების აღდგენის დაგეგმვის შესაძლებლობა [11].

სერვისების უწყვეტობის მართვის ძირითადი მიზანია ბიზნესის უწყვეტობის მართვის პროცესის მხარდაჭერა. ბიზნესის უწყვეტობის მართვა (Business Continuity Management ან BCM) – ესაა ბიზნესპროცესი, პასუხისმგებელი რისკების მართვაზე, რომელსაც შეუძლია სერიოზული გავლენა მოახდინოს ბიზნესზე.

BCM იცავს საკვანძო დაინტერესებულ მხარეებს, რეპუტაციას, ბრენდს და ქმედებას ფასეულობის შექმნის მიზნით. *BCM* პროცესი მოიცავს რისკების შემცირებას მისაღებ დონემდე და ბიზნეს-პროცესების აღდგენის ხერხების დაგეგმვას ბიზნესის დარღვევის შემთხვევაში. *BCM* ადგენს მიზნებს, საზღვრებს და მოთხოვნებს IT-სერვისის უწყვეტობის მართვასთან მიმართებით.

სინამდვილეში ტექნოლოგია არის მრავალი ბიზნესპროცესის ძირითადი კომპონენტი, ამიტომაც მათი უწყვეტობის და წვდომის უზრუნველყოფა აუცილებელია ბიზნესის არსებობისათვის მთლიანად. ITSCM მართავს სერვისების და მათი კომპონენტების აღდგენისათვის.

ITSCM-ის შუალედური მიზნებია:

1. მართვა – სერვისების უწყვეტობის უზრუნველყოფის და სერვისების აღდგენის გეგმების ერთობლიობისა, რომლებიც ბიზნესის უწყვეტობის უზრუნველყოფის გეგმების ნაწილია. სერვისების უწყვეტობის უზრუნველყოფის გეგმა (IT Service Continuity Plan) – განსაზღვრავს ბიჯებს ერთი ან რამდენიმე სერვისის აღსადგენად. გეგმამ ასევე უნდა განსაზღვროს მოვლენები, რომლებიც არის საფუძველი მისი ინიციაციისთვის, ადამიანებისთვის, რომლებიც უნდა ამოქმედდნენ, კომუნიკაციის საშუალებებისთვის და ა.შ.

ბიზნესის უწყვეტობის უზრუნველყოფის გეგმა (Business Continuity Plan ან BCP) - ესაა ბიჯების განმსაზღვრელი გეგმა, რომელიც აუცილებელია ბიზნესპროცესების აღსადგენად მათი ფუნქციონირების დარღვევის შემთხვევაში. გეგმა ასევე უნდა შეიცავდეს ინფორმაციას მოვლენების შესახებ, რომლებიც არის საფუძველი მისი ინიციაციისთვის, ადამიანებისთვის, რომლებიც უნდა ამოქმედდნენ, კომუნიკაციის საშუალებებისთვის და ა.შ.

2. ბიზნესზე გავლენის ანალიზის დამთავრება უწყვეტობის უზრუნველყოფის გეგმის მართვის გარანტიის ნაწილში ცვალებადი მოთხოვნებისა და ბიზნესის საჭიროების შესაბამისად;

3. რისკების ანალიზის და მენეჯმენტის თანხლება, კერძოდ, ბიზნესის ურთიერთქმედებისას წვდომის და უსაფრთხოების მართვის პროცესებთან, რომლებიც მართავენ სერვისებს შესაბამისად სერვისების შეთანხმებული დონისა;

4. რეკომენდაციების და სახელმძღვანელოების წარმოდგენა IT-ის სხვა სფეროებისთვის საკითხებში, რომლებიც დაკავშირებულია სერვისების უწყვეტობასა და აღდგენასთან;

5. უწყვეტობის და აღდგენის მექანიზმების უზრუნველყოფა, რომლებიც ეხმარებიან ბიზნესის მიერ დადგენილი მიზნობრივი მაჩვენებლების მიღწევაში;

6. ცვლილებების გავლენის შეფასება სერვისების უწყვეტობის უზრუნველყოფის გეგმებზე და სერვისების აღდგენის გეგმებზე;
7. პროაქტიური სრულყოფა სერვისების უწყვეტობისა იქ, სადაც ეს ეკონომიკურად ეფექტურია;
8. მოლაპარაკებების წარმართვა და კონტრაქტების დადება მიმწოდებლებთან აღდგენის აუცილებელი შესაძლებლობის უზრუნველყოფის შესახებ, უწყვეტობის მხარდაჭერის მიზნით (მიმწოდებლების მართვის პროცესის მონაწილეობით).

უწყვეტობის მართვა ფოკუსირდება მნიშვნელოვან ნეგატიურ მოვლენებზე, რომლებსაც *ITIL* მოიხსენიებს ბიზნესის „კატასტროფების" ტერმინით. უფრო ნაკლებმნიშვნელოვანი მოვლენები განიხილება ინციდენტების მართვის პროცესის ფარგლებში. არის თუ არა რომელიმე კონკრეტული მოვლენა კატასტროფა, დამოკიდებულია ორგანიზაციაზე, რომელშიც ის მოხდა.

ზომა და მნიშვნელობა მოვლენის ნეგატიური გავლენისა ბიზნესზე, მაგალითად, ფინანსური დანაკარგი ან რეპუტაციის დაკარგვა, იზომება ბიზნესზე გავლენის ანალიზის ფარგლებში. ბიზნესზე გავლენის ანალიზი განსაზღვრავს მინიმალურ მოთხოვნებს კრიტიკულობასთან, კონკრეტული მოთხოვნები ტექნოლოგიებთან და სერვისებთან განისაზღვრება უწყვეტობის მართვის ფარგლებში.

ITSCM უმთავრესად განიხილავს IT აქტივებს და კონფიგურაციებს, რომლებიც ბიზნესპროცესების მხარდამჭერია. კატასტროფის შემთხვევაში ბიზნესი უნდა გადაეწყოს ალტერნატიულ მუშა ლოკაციაზე. ამ დროს აუცილებელია ისეთი ელემენტების წარმოდგენა, როგორიცაა ოფისის კომფორტი თანამშრომელთათვის, კრიტიკული ქაღალდის ანგარიშების დუბლიკატები, კურიერების სერვისი და სატელეფონო კავშირები

კლიენტებთან და პარტნიორებთან. ამ მხრივ უწყვეტობის მართვამ უნდა გაითვალიწინოს ორგანიზაციის ოფისების რაოდენობა და ადგილმდებარეობა, ასევე სერვისები თითოეულში.

უწყვეტობის მართვის ფარგლებში უნდა შესრულდეს შემდეგი ქმედებები:

1. ITSCM-ის და გამოყენებული პოლიტიკის საზღვრების შეთანხმება;

2. ბიზნესზე გავლენის ანალიზი – სერვისის დანაკარგების ბიზნესზე გავლენის რაოდენობრივი შეფასებისთვის;

3. რისკების ანალიზი – იდენტიფიკაცია და შეფასება რისკებისა უწყვეტობის პოტენციური საფრთხეების განსაზღვრის და მათი განხორციელების ალბათობის შეფასების მიზნით. მასში მოიაზრება ასევე საფრთხეების მართვის მექანიზმების გამოყენება იქ, სადაც ეს ეკონომიკურად ეფექტური იქნება;

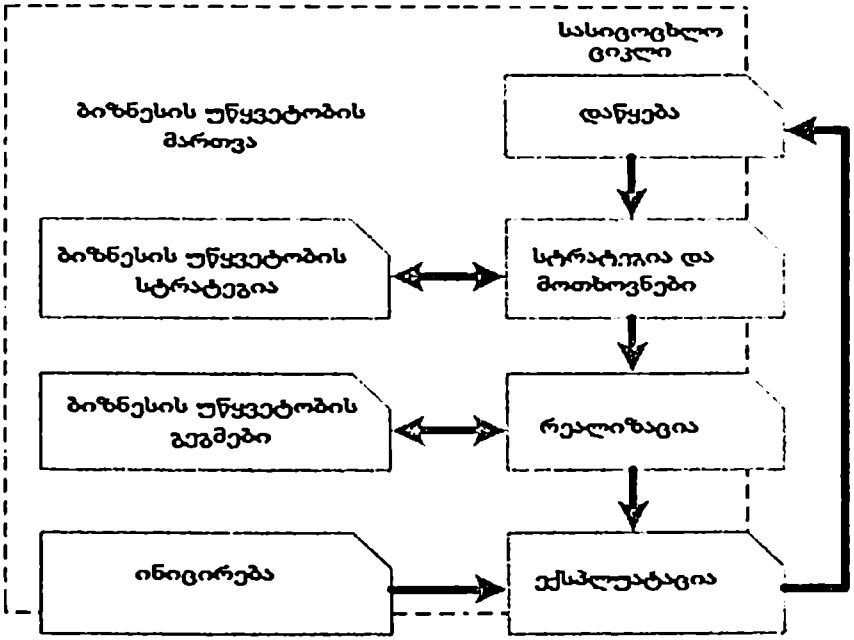
4. ITSCM სტრატეგიის ფორმირება, ინტეგრირებული *BCM* სტრატეგიაში.

5. უწყვეტობის უზრუნველყოფის გეგმების ფორმირება, ინტეგრირებული *BCM* გეგმებში.

6. უწყვეტობის უზრუნველყოფის გეგმების ტესტირება;

7. გეგმების უწყვეტი შესრულება და მათი მართვა.

15.1 ნახაზზე მოცემულია ITSCM-ის სასიცოცხლო ციკლი. ITSCM ციკლურად მეორდება სერვისის მთელ სასიცოცხლო ციკლზე და იძლევა გარანტიას, რომ ერთხელ შემუშავებული გეგმები სერვისების აღდგენისა და უწყვეტობის შესახებ შესაბამისობაში იყოს მომავალში ბიზნესის პრიორიტეტებთან და ბიზნესის უწყვეტობის უზრუნველყოფის გეგმებთან. 15.1 ნახაზზე ნაჩვენებია *BCM*-ის როლი ITSCM-ში.



ნახ.15.1. **ITSCM**-ის სასიცოცხლო ციკლი

ინიციალიზაციისა და მოთხოვნილებათა ფორმირების სტადიები ეკუთვნის *BCM*-ს. აქ ITSCM მხოლოდ უნდა მონაწილეობდეს ამ სტადიებში, რათა მხარი დაუჭიროს *BCM*-ს, გაიგოს კავშირები ბიზნესპროცესებს შორის და სერვისების დანაკარგების გავლენას მათზე. ამ საწყისი სტადიების შედეგად *BCM* აფორმირებს ბიზნესის უწყვეტობის უზრუნველყოფის სტრატეგიას. ITSCM-თვის პირველი რიგის სერიოზული ამოცანაა თავისი სტრატეგიის ფორმირება, რომელიც შესაძლებელს გახდის და მხარს დაუჭერს ბიზნესის უწყვეტობის სტრატეგიას. განვიხილოთ ITSCM-ის სასიცოცხლო ციკლის სტადიები.

სტადია 1 - დაწყება

ITSCM-ის ეს სტადია მოიცავს შემდეგ ქმედებებს:

- უწყვეტობის უზრუნველყოფის პოლიტიკის ფორმირება – უნდა განხორციელდეს რაც შეიძლება სწრაფად. პოლიტიკამ, მინიმუმ უნდა განსაზღვროს მიზნები, მომენტები და საკითხები, რომლებსაც მენეჯმენტმა უნდა მიაქციოს ყურადღება;
- საზღვრების და კომპეტენციების ტერმინების განსაზღვრა – TSCM-ის საზღვრების დადგენა და პასუხისმგებლობათა განაწილება მთელ პერსონალზე ორგანიზაციაში;
- რესურსების განაწილება – გარემოს ფორმირება ბიზნესის უწყვეტობის უზრუნველსაყოფად, რომელიც მოითხოვს მნიშვნელოვან ფინანსურ და ადამიანურ რესურსს;
- პროექტის განსაზღვრა ITSCM პროცესის ორგანიზების და მისი კონტროლის სტრუქტურისა – ITSCM და *BCM* რთული პროცესებია, რომლებიც თხოულობს ფრთხილ ორგანიზებას და კონტროლს;
- პროექტის და ხარისხის გეგმების შეთანხმება – გეგმები უზრუნველყოფს პროექტის კონტროლს და მის გამოყენებას განსხვავებულ სიტუაციებში.

სტადია 2 - მოთხოვნილებანი და სტრატეგია

ბიზნესის მოთხოვნების დადგენა სერვისების უწყვეტობაზე კრიტიკულად მნიშვნელოვანია, რადგან სწორედ ამ ეტაპზეა დამოკიდებული ორგანიზაციის მდგრადობა კატასტროფებისადმი და შესაბამისი დანახარჯები. თუ მოთხოვნები არაკორექტულია ან გაიპარა რამე მნიშვნელოვანი ინფორმაცია, მაშინ ITSCM-ის ყველა მექანიზმი იქნება არაეფექტური. ეს სტადია იყოფა ორ ქვესტადიად:

- მოთხოვნები – ბიზნესზე გავლენის ანალიზი და რისკების შეფასება;

• სტრატეგია – აყალიბებს რისკის შემცირების ზომებს და აღდგენის ოფციებს.

ბიზნესზე გავლენის ანალიზი (Business Impact Analysis ან BIA) – ესაა ქმედება ბიზნესის უწყვეტობის მართვის პროცესის ფარგლებში, რომელიც განსაზღვრავს კრიტიკულ ბიზნეს-ფუნქციებს და მათ დამოკიდებულებას გარემოს ფაქტორებზე. ეს ფაქტორები შეიძლება იყოს მიმწოდებლები, ადამიანები, სხვა ბიზნესპროცესები, სერვისები და ა.შ.

BIA განსაზღვრავს სერვისების დანაკარგების შედეგებს ბიზნესზე. დანაკარგები შეიძლება იყოს მნიშვნელოვანი, მაგალითად, დიდი ფინანსური დანაკარგები, „რბილი“ – მორალური, რეპუტაციის, კონკურენტული უპირატესობის დანაკარგები და ა.შ.

ბიზნესზე გავლენის ანალიზი განსაზღვრავს:

• ფორმას, რომელსაც მიიღებს განადგურება ან დანაკარგები, მაგალითად:

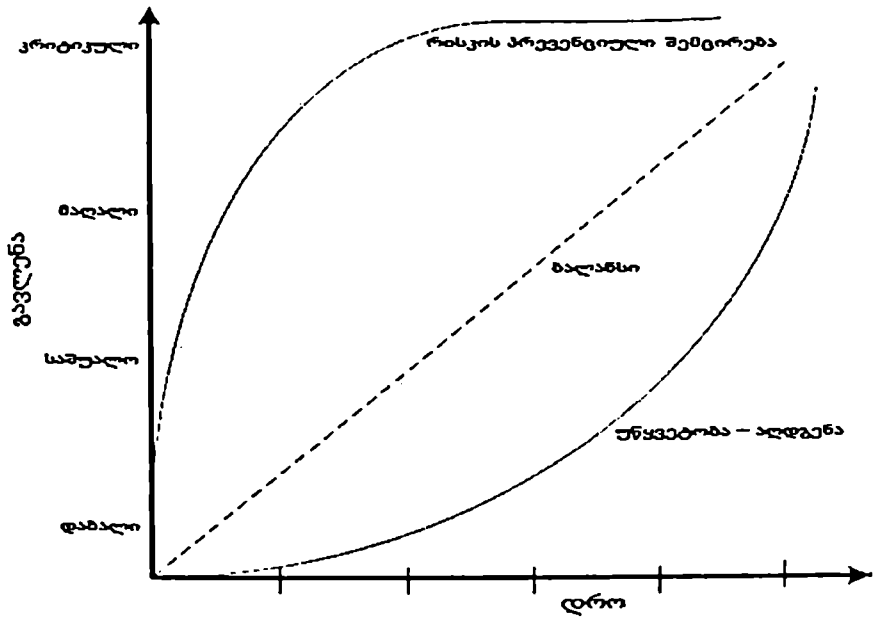
- დაკარგული შემოსავალი;
- დამატებითი ხარჯები;
- რეპუტაციის შელახვა;
- კეთილგანწყობილი კლიენტების დაკარგვა;
- კონკურენტული უპირატესობის დანაკარგი;
- ჯანმრთელობის შერყევა, კანონიერების და უსაფრთხოების დარღვევა;
- პერსონალის უსაფრთხოების რისკი;
- გასაღების ბაზრის დანაკარგი მოკლევადიან და გრძელვადიან პერიოდებში;
- ოპერაციული შესაძლებლობების დანაკარგი, მაგალითად, კონტროლის.

- როგორ გაიზრდება ნეგატიური შედეგები განადგურების ან დანაკარგების არასასურველი მოვლენის შემდეგ, ასევე დრო დღე-ღამის, კვირის, თვის, როდესაც ისინი იქნება ყველაზე მნიშვნელოვანი;
- საკადრო უზრუნველყოფა, უნარები, აპარატურა და სერვისები, რომლებიც აუცილებელია კრიტიკული ბიზნეს-პროცესების უწყვეტობის მინიმალური დონეების მხარდასაჭერად;
- დროის ჩარჩოები, რომლის საზღვრებში აუცილებელია საკადრო უზრუნველყოფის, აპარატურის, სერვისების და სხვა შესაძლებლობათა აღდგენის მინიმალური დონის უზრუნველყოფა;
- დროის ჩარჩოები, რომლის საზღვრებში აუცილებელია მთლიანად აღდგეს კრიტიკული ბიზნესპროცესები და მათი მხარდამჭერი საკადრო უზრუნველყოფა, აპარატურა, სერვისები და სხვა შესაძლებლობები;
- აღდგენის პრიორიტეტები სერვისებისთვის.

BIA-ს ერთ-ერთი ძირითადი გამოსასვლელია სერვისის ან ბიზნესპროცესის დანაკარგების გავლენის შეფასების დიაგრამის აგება მთლიანად ბიზნესზე (ნახ.15.2).

ბიზნესზე გავლენის *ანალიზი* არის ბაზა ITSCM-ის განსახორციელებლად. ანალიზის საფუძველზე ფორმირდება სერვისების, აპლიკაციების და სხვა კომპონენტების სია, რომლებიც ხდება ITSCM-ს განხილვის საგანი.

მეორე ეტაპი ITSCM-ის მოთხოვნების განსაზღვრისა მდგომარეობს არასასურველი მოვლენების აღმოცენების ალბათობის შეფასებაში.



ნახ.15.2. ბიზნესზე გავლენის გრაფიკული წარმოდგენა

რისკების შეფასება (Risk Assessment) – ესაა რისკების მართვის საწყისი ბიჯები. ანალიზდება აქტივების ფასეულობები ბიზნესისთვის, იდენტიფიცირდება საფრთხეები ამ აქტივებთან მიმართებით და ფასდება აქტივების დაუცველობა ამ საფრთხეებთან მიმართებით [11].

რისკების შესაფასებლად და მათ სამართავად გამოიყენება სტანდარტული მეთოდოლოგია M_o_R (*Management* of Risks), რომელიც შედგება შემდეგისგან:

- **M_o_R** პრინციპები – ბაზირებულია ორგანიზაციის მართვის პრინციპებზე და აუცილებელია რისკების ეფექტური მართვისათვის;

- **M_o_R** მიდგომა – ორგანიზაციის მიდგომა ზემოაღნიშნულ პრინციპებისადმი უნდა აისახოს რიგ დოკუმენტებში, კერძოდ, რისკების მართვის პოლიტიკაში;
- **M_o_R პროცესები.** გამოყოფენ ოთხ პროცესს M_o_R–ის ფარგლებში:
  - განსაზღვრება – საფრთხეთა დეფინიცია ქმედებისთვის, რომლებსაც შეუძლია გავლენა იქონიოს გამიზნული შედეგის მიღწევაზე;
  - შეფასება – ყველა განსაზღვრული საფრთხის ჯამური გავლენის შეფასება;
  - დაგეგმვა – მმართველი ქმედებების განსაზღვრა, რომლებიც ამცირებენ რისკებს;
  - რეალიზაცია – დაგეგმილი მმართველი ქმედებების განხორციელება, მათი კონტროლი, ეფექტურობის განსაზღვრა და კორექტირება აუცილებლობის შემთხვევაში.
- **M_o_R–ის** გადასინჯვა და დანერგვა – M_o_R-ის პროცესების, პოლიტიკის და მიდგომის დანერვა ისე, რომ ისინი უწყვეტად კონტროლდებოდეს და რჩებოდეს ეფექტური;
- ურთიერთმოქმედება – ყველა ქმედების ურთიერთ-მოქმედების უზრუნველყოფა M_o_R-ის ფარგლებში ინფორმაციის აქტუალურობის მხარდასაჭერად საფრთხეების, შესაძლებლობების და რისკების მართვის სხვა ასპექტების შესახებ.

ქმედებები ITSCM-ის ფარგლებში უნდა იყოს მიმართული რისკების გავლენისა და მათი წარმოქმნის ალბათობის შემცირებაზე.

ბიზნესზე გავლენის ანალიზის შედეგები და რისკების შეფასება არის სერვისების უწყვეტობის სტრატეგიის საფუძველი ბიზნესის მოთხოვნილებების შესაბამისად. უმეტესი ორგანიზაცია

უნდა იცავდეს ბალანსს რისკების შემცირებასა და აღდგენის მექანიზმების ფორმირებას შორის.

რაგინდ კარგად არ ტარდებოდეს ქმედებები რისკების შესამცირებლად, შეუძლებელია მათი მთლიანად აღმოფხვრა. ამიტომაც ყოველთვის აუცილებელია აღდგენის მექანიზმების დანერგვა ინტეგრაციაში წვდომის მართვის პროცესთან, რადგანაც სწორედ სერვისების წვდომა დაზარალდება, პირველ რიგში, ბიზნესისთვის არასასიამოვნო მოვლენების აღმოცენების შემთხვევაში.

ტიპური ღონისძიებები რისკების შესამცირებლად შემდეგია:

- UPS-ის და სარეზერვო კვების ინსტალაცია კომპიუტერისთვის;
- სისტემების მტყუნებამდგრადობის უზრუნველყოფა კრიტიკული აპლიკაციებით, რომლებისთვისაც მიუღებელია ნებისმიერი მოცდენა (მაგალითად, საბანკო სისტემაში);
- RAID-ის და სარკისებური დისკოების გამოყენება სერვერებისთვის, ინფორმაციის დაკარგვის თავიდან ასაცილებლად და მუშაობის უწყვეტობის უზრუნველსაყოფად;
- სათადარიგო კომპონენტების/მოწყობილობათა არსებობა, რომლებიც გამოყენებულ იქნება ძირითადის მტყუნების შემთხვევაში. მაგალითად, სათადარიგო სერვერი მინიმალური აუცილებელი კონფიგურაციით, რომელიც ამუშავდება ძირითადის გამორთვისას;
- SPOF-ების გამორიცხვა, მაგალითად, ქსელში წვდომის ერთიანი წერტილი ან ელექტროკვების ერთიანი წერტილი;.
- საიმედო IT-სისტემების და ქსელების გამოყენება;
- სერვისების აუთსორსინგი რამდენიმე მიმწოდებლისთვის;
- უსაფრთხოებაზე კონტროლის გაზრდა;

- სერვისების მუშაობისა დარღვევების აღმოჩენის კონტროლის გაზრდა;
- აღდგენის და სარეზერვო დუბლირების ყოვლისმომცველი სტრატეგია, რომელიც მოიცავს გარე შენახვასაც. გარე შენახვა გულისხმობს კრიტიკული ინფორმაციის რეგულარულ დუბლირებას (ყოველდღიური) გარე საცავში.

ზემოჩამოთვლილი ზომები ვერ წყვეტს ITSCM-ის ყველა საკითხს, მაგრამ მათი გამოყენება საშუალებას იძლევა მნიშვნელოვნად შემცირდეს დანაკარგების რისკი ბიზნესისთვის გაუთვალისწინებელ მდგომარეობათა აღმოცენების შემთხვევაში.

აღდგენის ოფციები ITSCM-ის ფარგლებში, რომლებიც უნდა იქნას გათვალისწინებული სტრატეგიის ფორმირებისას, შემდეგია [11]:

- გადასვლა ხელით მუშაობაზე სერვისთა ზოგიერთი ტიპისთვის შეიძლება გახდეს კარგი ალტერნატივა მოკლე პერიოდში სერვისის აღდგენამდე. მაგალითად, სერვის-დესკს (service desk) შეუძლია მუშაობა გარკვეული დროით ქაღალდის განაცხადებთან და ჟურნალებთან;
- ურთიერთშეთანხმება არის აღდგენის კიდევ ერთი ოფცია. უნდა მოხდეს შეთანხმებების დადება ორგანიზაციებს შორის, რომლებიც იყენებენ მსგავს ტექნოლოგიებს. დღეისათვის არაა მისაღები უმეტესი IT-სისტემებისთვის, მაგრამ შეიძლება მათი ცალკეულ შემთხვევებში გამოყენება, მაგალითად, გარე სარეზერვო დუბლირებისთვის ან პრინტერების გამოსაყენებლად.
- თანდათანობითი აღდგენა (Gradual Recovery) – აღდგენის ხერხი, ცნობილია ასევე როგორც „ცივი რეზერვირება“. გაითვალისწინება სერვისის აღდგენა 72 საათზე მეტ დროში. თანდათანობითი აღდგენის დროს ამოქმედებულია მობილური ან სტაციონარული სარეზერვო ცენტრი, აღჭურვილი

სიცოცხლისუზრუნველმყოფელი ელემენტებით და ქსელური გაყვანილობით, კომპიუტერული სისტემების გარეშე. აღდგენის ეს ოფცია რეკომენდებულია არაკრიტიკული სერვისებისთვის, რომელთა უზრუნველყოფა შეიძლება შეჩერდეს დღეებით და კვირებით, ბიზნესზე უმნიშვნელო გავლენით;

- შუალედური აღდგენა (Intermediate Recovery) – აღდგენის ხერხი, ცნობილი სახელით „თბილი რეზერვირება“. გაითვალისწინება სერვისის აღდგენა 24-72 საათის განმავლობაში. შუალედური აღდგენისას, ჩვეულებისამებრ, გამოიყენება საერთო მობილური ან სტაციონარული სარეზერვო ცენტრი, აღჭურვილი კომპიუტერული სისტემებით და ქსელური კომპონენტებით. აპარატურული და პროგრამული კონფიგურირება, ასევე მონაცემთა აღდგენა სრულდება სერვისების უწყვეტობის უზრუნველყოფის გეგმის ფარგლებში. აღდგენის ამ ოფციას ჩვეულებრივად სთავაზობენ მესამე მხარის ორგანიზაციები, რომლებსაც გააჩნიათ ამ მიზნით ყველა აუცილებელი მოწყობილობა და კვალიფიციური პერსონალი. ამ ოფციის ღირებულება დამოკიდებულია მესამე მხარის რესურსებზე, რომლებიც უნდა ამოქმედდეს აღსადგენად, ასევე დროზე, რომლის განმავლობაშიც უნდა აღდგეს სერვისი. ამ მეთოდის უპირატესობაა გამჭვირვალობა მომხმარებელთათვის. ნაკლოვანებაა ის, რომ ინფორმაცია (კონფიდენციალურიც) იქნება შენახული გარე ორგანიზაციაში. ეს უკანასკნელი კი აღდგენის ამ ხერხს არ იყენებს ბევრი ორგანიზაციისთვის;
- სწრაფი აღდგენა (Fast Recovery) – აღდგენის ხერხი. გაითვალისწინება სერვისის აღდგენა დროის მოკლე შუალედში, 24 საათზე ნაკლებ დროში. სწრაფი აღდგენისას იყენებენ გამოყოფილ სტაციონარულ სარეზერვო ცენტრს კომპიუტერული სისტემებით და პროგრამული უზრუნველყოფით,

კონფიგურირებულს სერვისების მუშაობისთვის. დაუყოვნებლივი აღდგენა იკავებს 24 საათს, თუ საჭიროა მონაცემთა აღდგენა სარეზერვო კოპირებით.

- დაუყოვნებლივი აღდგენა (Immediate recovery) – აღდგენის ხერხი, ცნობილია სახელით „ცხელი რეზერვირება“. გაითვალისწინება სერვისის აღდგენა სერვისის შეწყვეტის გარეშე. დაუყოვნებლივი აღდგენა, ჩეულებისამებრ, იყენებს ტექნოლოგიებს: სარკირება (რეზერვირება), დატვირთვის ბალანსირება და დანადგარების დაყენების ფართობის დაყოფა. ეს ხერხი ყველაზე ხშირად ითვალისწინებს სისტემის კომპონენტების „ორმაგ ლოკაციას“, ანუ სრულ დუბლირებას. ის ყველაზე ძვირადღირებულია და გამოიყენება მხოლოდ კრიტიკული ბიზნესპროცესებისთვის, რომელთა მოცდენამ შეიძლება დიდი ზარალი გამოიწვიოს. დუბლები უნდა ინახებოდეს რაც შეიძლება მოცილებით ორიგინალებისგან, რათა ისიც არ დააზიანოს დამანგრეველმა მოვლენამ.

უწყვეტობის უზრუნველყოფის სტრატეგია უნდა მოიცავდეს აღდგენის ყველა ზემოგანხილულ ხერხს. განსხვავებული სერვისები, ორგანიზაციის მიერ გამოყენებული, ითხოვს აღდგენის გასხვავებულ მიდგომებს და მტყუნებათა რისკების შემცირებას. რომელი ოფციაც არ უნდა იყოს არჩეული, ის უნდა იყოს ეკონომიკურად ეფექტური. მთავარი წესი – რაც უფრო დიდხანს გაძლებს ბიზნესი სერვისის გარეშე, მით უფრო იაფი უნდა იყოს გადაწყვეტა მისი უწყვეტობის უზრუნველსაყოფად.

სტადია **3** - რეალიზაცია

მას შემდეგ, რაც უწყვეტობის უზრუნველყოფის სტრატეგია განისაზღვრება, აუცილებელია შემუშავდეს სერვისების უწყვეტობის უზრუნველყოფის გეგმები ბიზნესის უწყვეტობის უზრუნველყოფის გეგმების შესაბამისად. ITSCM გეგმები იხილავს

ყველა ქმედებას, რომლებიც აუცილებელია საჭირო სერვისების, შესაძლებლობების და რესურსების უზრუნველსაყოფად, უწყვეტობის შესაბამისი დონეებით. - ეს ნიშნავს არა მხოლოდ საკითხების განხილვას, დაკავშირებულს სერვისების და შესაძლებლობების აღდგენასთან, არამედ ასევე მათ შორის დამოკიდებულებათა ცოდნასაც, ტესტირებას, მთლიანობის და მონაცემთა თანამიმდევრულობის შემოწმებას,

ITSCM გეგმები უნდა მოიცავდეს დოკუმენტაციას საიმედოობის უზრუნველყოფის საშუალებების აღდგენის ზომების შესახებ, დასაბუთებას კონკრეტული ზომების გამოყენების შესახებ კონკრეტული სიტუაციისგან დამოკიდებულებით. გეგმების ფორმირების დროს აუცილებელია იმაში დარწმუნება, რომ მათში დეტალურადაა განხილული და დოკუმენტირებული ყველა ქმედება აღდგენისათვის, მტყუნების შემთხვევაში. ITSCM გეგმები უნდა შეიცავდეს ასევე ისეთ ძირითად მომენტებს, როგორიცაა მონაცემთა აღდგენის წერტილი, დამოკიდებული სისტემების სია, ამ დამოკიდებულების ბუნება, მოთხოვნები პროგრამულ და აპარატულ უზრუნველყოფაზე, კონფიგურაციის დეტალები და სხვა მნიშვნელოვანი ინფორმაცია სისტემების და სერვისების შესახებ.

ინფორმაციის ერთ-ერთი ყველაზე მნიშვნელოვანი წყაროებიდან გეგმების ფორმირებისათვის არის ბიზნესზე გავლენის ანალიზი. სხვა სფეროებიც უნდა იყოს გაანალიზებული: *SLA*, უსაფრთხოების მოთხოვნები, ექსპლუატაციის ინსტრუქციები, პროცედურები, გარე კონტრაქტები.

გარდა უწყვეტობის უზრუნველყოფის გეგმების დამუშავებისა, იმისთვის, რომ დაცული იქნას მიღებული უწყვეტობის უზრუნველყოფის სტრატეგია, აუცილებელია შემდეგი ქმედებები:

1. ორგანიზაციული სტრუქტურის დაგეგმვა

კატასტროფის აღმოცენების შემთხვევაში, ორგანიზაციის სტრუქტურა ნაღდი ალბათობით განიცდის ცვლილებას და იქნება დაფუძნებული, უპირველეს ყოვლისა, შემდეგზე:

- ხელმძღვანელობა – ტოპ-მენეჯერი და ორგანიზაციის მმართველობა, რომლებიც ფლობენ ძალაუფლებას და კონტროლის საშუალებებს ორგანიზაციაზე. სწორედ ხელმძღვანელობაა პასუხისმგებელი მართვის შესახებ კრიზისულ სიტუაციაში;
- კოორდინაცია – დონე, პასუხისმგებელი კოორდინაციაზე აღდგენის პროცესის შიგნით;
- აღდგენა – ბიზნესის და IT ჯგუფების ერთობლიობა, რომლებიც წარმოადგენენ კრიტიკულ ბიზნესფუნქციებს და სერვისებს, მათ მხარდასაჭრად. თითოეული ჯგუფი პასუხისმგებელია თავისი სფეროს აღდგენის გეგმების შესრულებაზე პერსონალთან, მომხმარებლებთან და მესამე მხარესთან ურთიერთმოქმედებით.

2. ტესტირება

აღდგენის გეგმებმა უნდა გაიაროს ტესტირება. ტესტირება მნიშვნელოვანი ნაწილია. სწორედ ის იძლევა გარანტიას, რომ მიღებული სტრატეგია, შეთანხმებები, გეგმები და პროცედურები ნამდვილად იმუშავებს პრაქტიკაში.

სერვისების მიმწოდებელი პასუხისმგებელია იმაზე, რომ კატასტროფის შემთხვევაში სერვისები შეიძლება აღდგენილ იქნას მოცემულ დროით ინტერვალში მოთხოვნილი ფუნქციურობით და მწარმოებლურობით. ტესტები უნდა ჩატარდეს მაქსიმალურად რეალისტური სცენარებით. ამასთანავე, საჭიროა გაგება, რომ ყველაზე დეტალური ტესტირებაც კი ვერ გაითვალისწინებს ყველა ნიუანსს, რომლებიც შეიძლება აღმოცენდეს რეალურად.

სტადია 4 - უწყვეტი ექსპლუატაცია

ეს სტადია შედგება შემდეგიდან:

1. სწავლება, მზადყოფნა, ტრეინინგი – პერსონალი უნდა იყოს მზად გაუთვალისწინებელი მდგომარეობების აღმოცენებასთან და იცოდეს, თუ რა უნდა გააკეთოს ამ შემთხვევაში;

2. გადასინჯვა – ITSCM-ის პროცესის ყველა გამოსასვლელი რეგულარულად უნდა გადამოწმდეს აქტუალურობაზე და აუცილებლობის შემთხვევაში, კორექტირდეს;

3. ტესტირება – გარდა საწყისი ტესტირებისა, საჭიროა რეგულარული ტესტირების გათვალისწინება სტრატეგიის, გეგმების და ITSCM-ს სხვა გამოსასვლელების. სარეზერვო დუბლები და აღდგენის მექანიზმები აგრეთვე უნდა დატესტირდეს;

4. ცვლილებების მართვა – პროცესი, პასუხისმგებელი ცვლილების შეფასებაზე, მათი გავლენის თვალსაზრისით ITSCM-ს გეგმებზე.

ინიცირება არის დასკვნითი ტესტი ბიზნესის და სერვისების უწყვეტობის უზრუნველყოფის გეგმებისთვის. ამ პროცესმა უნდა განიხილოს აღდგენის გეგმების ამოქმედების პროცედურა გაუთვალისწინებელი მდგომარეობების შემთხვევაში.

აუცილებელია დახსომება, რომ გადაწყვეტა გეგმების ინიციალიზაციაზე კარგად უნდა იყოს აწონილი, განსაკუთრებით მესამე მხარის აღდგენის სერვისების გამოყენებაზე.

მტყუნება შეიძლება მოხდეს ნებისმიერ მომენტში, ამიტომ უნდა არსებობდეს აღდგენის გეგმების დაუყოვნებლივ ინიცირების შესაძლებლობა.

ITSCM-ის შესასვლელებია:

1. ინფორმაცია ბიზნესიდან – სტრატეგია, გეგმები და ორგანიზაციის ბიუჯეტი, მიმდინარე და სამომავლო მოთხოვნები;

2. ინფორმაცია IT–დან – სტრატეგია, გეგმები და IT–ს ბიუჯეტი;

3. ბიზნესის უწყვეტობის უზრუნველყოფის სტრატეგია და გეგმები;

4. ინფორმაცია სერვისების შესახებ – ინფორმაცია *SLM-დან*, კერძოდ, სერვისების პორტფელიდან, სერვისების კატალოგიდან, SLA/*SLR-დან*;

5. ფინანსური ინფორმაცია – ინფორმაცია ფინანსების მართვის პროცესიდან სერვისების, რესურსების და კომპონენტების უზრუნველყოფის ღირებულებათა შესახებ;

6. ინფორმაცია ცვლილებების შესახებ – ინფორმაცია ცვლილებების მართვის პროცესიდან, კერძოდ, ცვლილებების განრიგი და მათი გავლენა უწყვეტობის უზრუნველყოფის გეგმებზე;

7. ინფორმაცია ბიზნესისა და სერვისების, დამხმარე სერვისების და ტექნოლოგიების ურთიერთმიმართების შესახებ;

8. ბიზნესის უწყვეტობის უზრუნველყოფის მართვის და წვდომის მართვის განრიგები;

9. სერვისების უწყვეტობის უზრუნველყოფის გეგმები და პარტნიორთა, მიმწოდებელთა ტესტირების რეპორტები;

ITSCM-ის გამოსასვლელებია:

1. ITSCM-ის პოლიტიკა და სტრატეგია;

2. გეგმების ერთობლიობა, მათ შორის ანტიკრიზისული მართვის, სასწრაფო საპასუხო ქმედებების, აღდგენებისა კატასტროფების შემდეგ. აგრეთვე დამხმარე გეგმების ერთობლიობა და კონტრაქტები სერვისების აღდგენის მიმწოდებლებთან.

ანტიკრიზისული მართვა (Crisis Management) – პროცესი, პასუხისმგებელი ბიზნესის უწყვეტობის მართვის შესახებ ფართო გაგებით. ანტიკრიზისული მართვის გუნდი პასუხს აგებს სტრატეგიულ საკითხებზე, როგორიცაა მართვა ურთიერთ-დამოკიდებულებისა მასობრივ ინფორმაციის საშუალებებთან, იღებს გადაწყვეტილებას აქციონერთა ნდობის, ბიზნესის უწყვეტობის უზრუნველყოფის გეგმების ინიციალიზაციის შესახებ.

3. ბიზნესზე გავლენის ანალიზი და შესაბამისი რეპორტები;

4. რისკების ანალიზი, მმართველობითი მიმოხილვები და რეპორტები;

5. ITSCM-ის ტესტირების განრიგი;

6. სცენარები ტესტირების ჩასატარებლად;

7. მიმოხილვები და რეპორტები ITSCM-ის ტესტირების შესახებ.

საკვანძო მაჩვენებლი ITSCM-ის მწარმოებლურობის არის ის, რომ წარმოდგენილი სერვისები შეიძლება იქნას აღდგენილი ბიზნესის მხარდაჭერის მიზნით დასახული მიზნების მისაღწევად:

1. ტარდება რეგულარული აუდიტი ITSCM-ის გეგმების, იმის შემოწმების მიზნით, რომ ბიზნესის მოთხოვნები აღდგენისათვის შეიძლება იყოს დაკმაყოფილებული;

2. სერვისების აღდგენის ყველა მიზნობრივი მაჩვენებელი დოკუმენტირებულია, შეთანხმებულია SLA-ში, და შეიძლება იქნას მიღწეული ITSCM-ის გეგმების დახმარებით;

3. ტარდება რეგულარული და ყოვლისმომცველი ტესტირება ITSCM-ის გეგმების;

4. დადებულია ITSCM-ის ყველა აუცილებელი კონტრაქტი მესამე მხარესთან;

5. უზრუნველყოფილია რისკების შემცირება და სერვისების მტყუნების ნეგატიური გავლენა.

ეფექტურობის მაჩვენებლის სახით შეიძლება ასევე განხილულ იქნას ორგანიზაციის მზადყოფნა ქმედებებისადმი, ITSCM-ის გეგმების შესაბამისად.

ITSCM-ის ძირითადი რისკებია ინფორმაციის უკმარისობა და არაკორექტულობა, მოსული ბიზნესიდან, IT-დან და სხვა პროცესებიდან, აგრეთვე რესურსების დეფიციტი უწყვეტობის უზრუნველსაყოფად.

15.2. ინფორმაციული უსაფრთხოების მართვა

ინფორმაციული უსაფრთხოების მართვა (Information Security Management ან ISM) – არის პროცესი, რომელიც უზრუნველყოფს კონფიდენციალობას, მთლიანობას და წვდომას ორგანიზაციის აქტივების, ინფორმაციის, მონაცემების და სერვისებისას.

ინფორმაციული უსაფრთხოების მართვა არის ორგანიზაციული მიდგომის ნაწილი ინფორმაციული უსაფრთხოებისადმი, რომელსაც აქვს უფრო ფართო არეალი, ვიდრე სერვისების მიმწოდებელს, და მოიცავს საქაღალდო დოკუმენტების დამუშავებას, შენობაში წვდომას, სატელეფონო ზარებს და ა.შ. მთელი ორგანიზაციისთვის [11].

ISM-ის ძირითადი მიზანია ინფორმაციული უსაფრთხოების მართვის ეფექტური უზრუნველყოფა ყველა სერვისის და ქმედების სერვისების მართვის ფარგლებში. ინფორმაციული უსაფრთხოება დანიშნულია ინფორმაციის კონფიდენციალურობის, წვდომის და მთლიანობის დარღვევის დაცვისათვის, ასევე ინფორმაციული სისტემების და კომუნიკაციების დაცვისთვის.

1. კონფიდენციალურობა – ინფორმაციის მდგომარეობა, რომლის დროსაც მასზე წვდომას ახორციელებს მხოლოდ ამის უფლების მქონე სუბიექტი;

2. მთლიანობა – ინფორმაციის მდგომარეობა, რომლის დროსაც გამორიცხულია მისი ნებისმიერი ცვლილება, ან ცვლილებას ახორციელებს მხოლოდ ამის უფლების მქონე სუბიექტი;

3. წვდომა – ინფორმაციის მდგომარეობა, რომლის დროსაც წვდომის უფლების მქონე სუბიექტებს შეუძლიათ ამის რეალიზაცია შეუფერხებლად.

ინფორმაციული უსაფრთხოების მართვის მიზანი მიღწეულია, თუ:

1. ინფორმაცია მიღწევადია მაშინ, როცა ეს საჭიროა, ხოლო საინფორმაციო სისტემები მდგრადია შეტევებისგან, შეუძლიათ მათი თავიდან აცილება ან სწრაფი აღდგენა;

2. ინფორმაცია მისაწვდომია მხოლოდ მათთვის, ვისაც ამის უფლება აქვს;

3. ინფორმაცია კორექტული, სრული და დაცულია არაავტორიზებული ცვლილებებისგან;

4. ინფორმაციის გაცვლა პარტნიორებთან და სხვა ორგანიზაციებთან საიმედოდ დაცულია.

ბიზნესი განსაზღვრავს, რა და როგორ უნდა იქნეს დაცული. ამ დროს ინფორმაციული უსაფრთხოების უზრუნველყოფის ეფექტურობის და მთლიანობისთვის აუცილებელია ბიზნეს-პროცესების განხილვა თავიდან ბოლომდე, რადგან სუსტმა ადგილმა შეიძლება მთელი სისტემა დააზარალოს.

ISM პროცესი უნდა მოიცავდეს:

- ინფორმაციული უსაფრთხოების პოლიტიკის ფორმირებას, მართვას, გავრცელებასა და დაცვას, ასევე სხვა დამხმარე პოლიტიკისა, რომლებიც კავშირშია ინფორმაციულ უსაფრთხოებასთან. ინფორმაციული უსაფრთხოების პოლიტიკა (Security Policy) – განსაზღვრავს ორგანიზაციის მიდგომას ინფორმაციული უსაფრთხოების მართვასთან;
- უსაფრთხოებისადმი ბიზნესის შეთანხმებულ მიმდინარე და სამომავლო მოთხოვნების გაგებას;

- უსაფრთხოების კონტროლის გამოყენებას ინფორმაციული უსაფრთხოების და რისკების მართვის პოლიტიკის შესასრულებლად, რომლებიც დაკავშირებულია ინფორმაციის, სისტემების და სერვისების წვდომასთან. ტერმინი „უსაფრთხოების კონტროლი“ ნასესხებია ინგლისურიდან და მოცემულ კონტექსტში ნიშნავს კონტრზომების და გამაფრთხილებელი ზომების ერთობლიობას, რომლებიც გამოიყენება რისკების შემცირების, ანულირების და მათდამი წინააღმდეგობისთვის. ანუ უსაფრთხოების კონტროლი შედგება პროაქტიური და რეაქტიური ქმედებებისგან;
- უსაფრთხოების კონტროლის სიის დოკუმენტირება, ქმედებები მათი ექსპლუატაციის და მართვისთვის, ასევე მასთან დაკავშირებულ რისკებთან;
- მიმწოდებლების და კონტრაქტების მართვა, რომლებიც მოითხოვს წვდომას სისტემებზე და სერვისებზე. ხორციელდება მიმწოდებლების მართვის პროცესთან ურთიერთქმედებით;
- უსაფრთხოების და ინციდენტების ყველა ხვრელის კონტროლი, რომლებიც კავშირშია სისტემებთან და სერვისებთან;
- უსაფრთხოების კონტროლის პროაქტიური სრულყოფა და ინფორმაციული უსაფრთხოების დარღვევის რისკების შემცირება;
- ინფორმაციული უსაფრთხოების ასპექტების ინტეგრაცია სერვისების მართვის ყველა პროცესში.

ინფორმაციული უსაფრთხოების პოლიტიკა უნდა მოიცავდეს შემდეგს:

- ინფორმაციული უსაფრთხოების პოლიტიკის ასპექტების რეალიზაცია;
- ინფორმაციული უსაფრთხოების პოლიტიკის ასპექტების შესაძლო ბოროტად გამოყენება;
- წვდომის კონტროლის პოლიტიკა;
- პაროლების გამოყენების პოლიტიკა;

- ელექტრონული ფოსტის პოლიტიკა;
- ინტერნეტის პოლიტიკა;
- აქტიური დაცვის პოლიტიკა;
- ინფორმაციის კლასიფიკაციის პოლიტიკა;
- დოკუმენტების კლასიფიკაციის პოლიტიკა;
- დაშორებული წვდომის პოლიტიკა;
- მიმწოდებელთა წვდომის პოლიტიკა სერვისებთან, ინფორმაციასა და კომპონენტებთან;
- აქტივების განლაგების პოლიტიკა.

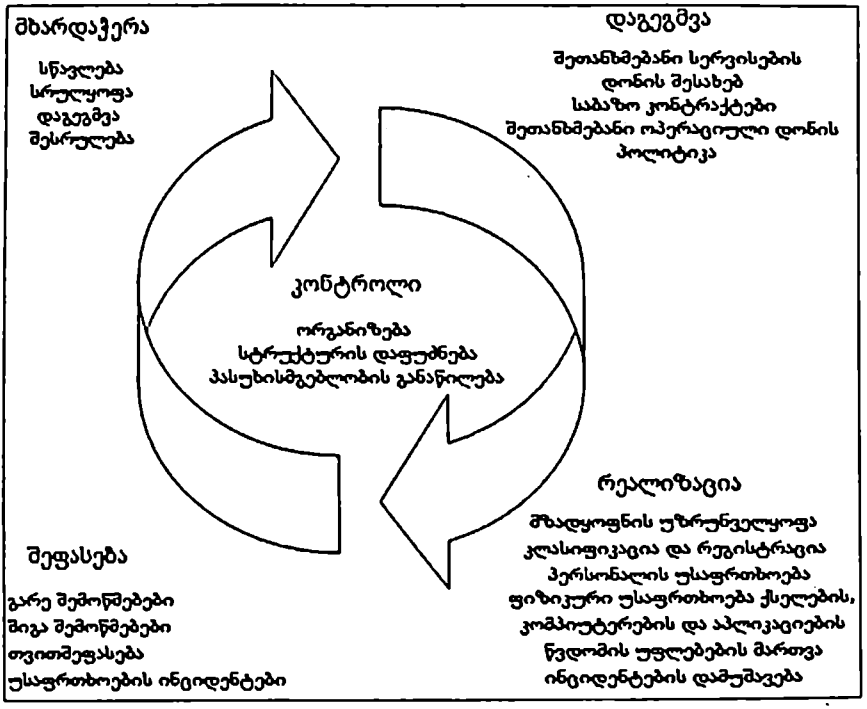
ჩამოთვლილი პოლიტიკის ასპექტები მისაწვდომი უნდა იყოს მომხმარებლებისა და დამკვეთებისთვის, რომლებიც, თავის მხრივ, ვალდებულნი არიან თანხმობა დაადასტურონ წერილობით.

პოლიტიკა მტკიცდება ბიზნესის და IT-ის ხელმძღვანელობის მიერ და გადაიხედება მდგომარეობათა მიხედვით.

ინფორმაციული უსაფრთხოების და მისი მართვის განსახორციელებლად აუცილებელია ინფორმაციული უსაფრთხოების მართვის სისტემის მხარდაჭერა.

ინფორმაციული უსაფრთხოების მართვის სისტემა (**Information Security Management System** ან ISMS) – ესაა სისტემა პოლიტიკის, პროცესების, სტანდარტების, სახელმძღვანელო დოკუმენტების და საშუალებების, რომლებიც უზრუნველყოფენ ორგანიზაციებს ინფორმაციული უსაფრთხოების მართვის მიზნების მისაღწევად.

15.3 ნახაზზე ნაჩვენებია ISMS-ის სტრუქტურა, რომლებიც უფრო ფართოდ გამოიყენება ორგანიზაციების მიერ.



ნახ.15.3. ISMS

განიხილება ISMS-ის სტრუქტურის ხუთი ელემენტი:

1. კონტროლი. მიზანია:

- ინფორმაციული უსაფრთხოების მართვის სისტემის ფორმირება ორგანიზაციის ფარგლებში;
- ორგანიზაციული სტრუქტურის ფორმირება ინფორმაციული უსაფრთხოების პოლიტიკის რეალიზაციის მომზადების, დამტკიცებისა და რეალიზაციისთვის;
- პასუხიმგებლობათა განაწილება;
- კონტროლის დოკუმენტაციის ფორმირება.

2. დაგეგმვა. მისი მიზანია – ინფორმაციული უსაფრთხოების შესაფერისი მეტრიკების და გაზომვის ხერხების დამუშავება და რეკომენდაცია. პირველ რიგში, დაგეგმვა უნდა ითვალისწინებდეს კონკრეტული ორგანიზაციის მოთხოვნებს და თავისებურებებს. ინფორმაციის წყაროებად ინფორმაციული უსაფრთხოების მოთხოვნების დასადგენად განიხილავენ ბიზნესს, რისკებს, გეგმებს, სტრატეგიას, შეთანხმებებს (პირველ რიგში – OLA და SLA). ამ დროს მნიშვნელოვანია გათვალისწინებულ იქნას მორალური, სამართლებრივი და ეთიკური ნორმები.

3. რეალიზაცია. მისი მიზანია – შესაბამისი პროცედურების, ინსტრუმენტების და უსაფრთხოების კონტროლების უზრუნველყოფა ინფორმაციული უსაფრთხოების პოლიტიკის მხარდასაჭერად.

რეალიზაციის ფარგლებში ხორციელდება შემდეგი ღონისძიებები:

- *აქტივების იდენტიფიკაცია* – კონფიგურაციების მართვასთან ერთად;
- ინფორმაციის კლასიფიკაცია – ინფორმაცია და ინფორმაციული საცავები უნდა იყოს კლასიფიცირებული, შესაბამისად მათი მგრძნობიაროზისა და მნიშვნელობისა, ინფორმაციული უსაფრთხოების სამ ასპექტთან მიმართებით (კონფიდენციალურობა, მთლიანობა, წვდომა).

4. შეფასება. მიზანი ISMS-ის ფარგლებში:

- ინფორმაციული უსაფრთხოების პოლიტიკის შესაბამისობის შემოწმება ინფორმაციული უსაფრთხოების მოთხოვნებთან SLA და OLA-დან;
- ინფორმაციული უსაფრთხოების ტექნიკური მდგენელის რეგულარული შემოწმებების ჩატარება IT-სისტემისთვის;

o ინფორმაციის მიწოდება რეგულატორებზე და გარე აუდიტებზე აუცილებლობის შემთხვევაში;

5. მხარდაჭერა. მიზნები ISMS-ის მხარდასაჭერად:

o შეთანხმებათა სრულყოფა ინფორმაციულ უსაფრთხოებასთან მიმართებით, მაგალითად, SLA და OLA;

o ინფორმაციული უსაფრთხოების საშუალებებისა და კონტროლის სრულყოფა.

საკვანძო ქმედებები *ISM-ის* ფარგლებში:

1. ინფორმაციული უსაფრთხოების პოლიტიკისა და მისი მხარდამჭერი დამხმარე პოლიტიკის ერთობლიობის ფორმირება, გადასინჯვა და კორექტირება;

2. ინფორმაციული უსაფრთხოების პოლიტიკის რეალიზაცია და დაცვა, ასევე მათ შორის ურთიერთქმედების უზრუნველყოფა;

3. ინფორმაციული აქტივების და დოკუმენტების შეფასება და კლასიფიკაცია;

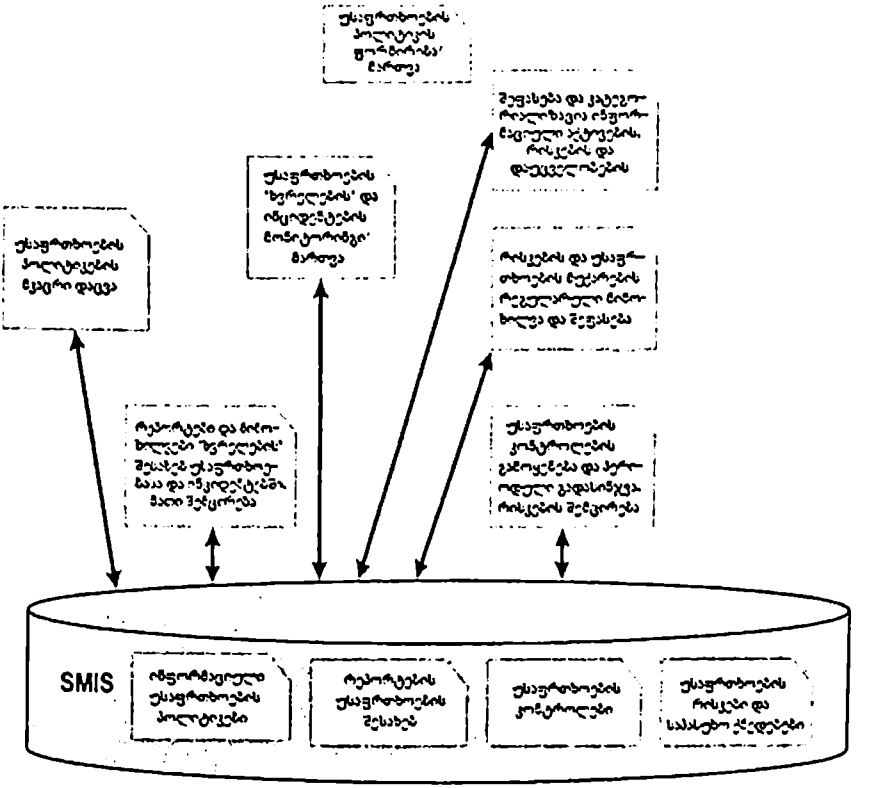
4. უსაფრთხოების კონტროლის ერთობლიობა, რისკების შეფასების ზომები, საპასუხო ქმედებები;

5. უსაფრთხოების „ხვრელების“ და ინციდენტების მონიტორინგი და მართვა;

6. ანალიზი, რეპორტების წარმოება და უსაფრთხოებაზე „ხვრელების“ გავლენის და ინციდენტების შემცირება;

7. განრიგის შედგენა და აუდიტების, ტესტირების და მიმოხილვების ჩატარება.

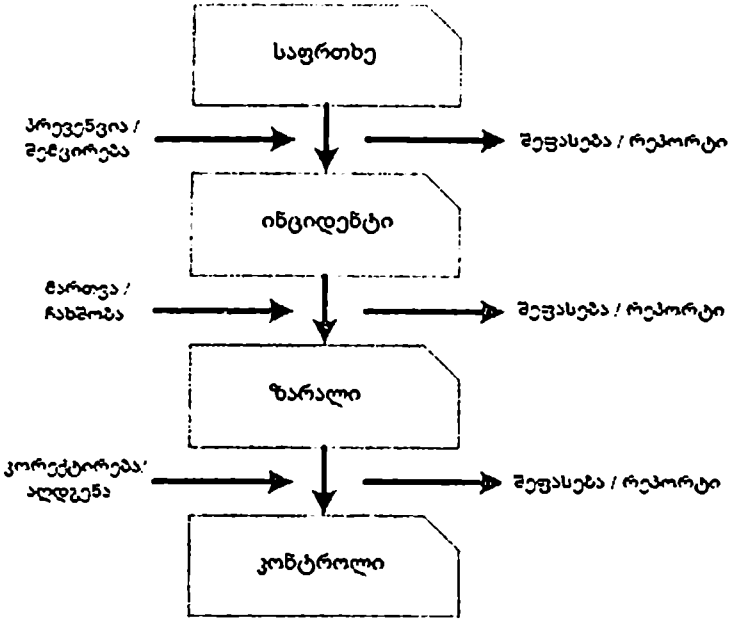
აღწერილ ქმედებათა ურთიერთმოქმედება მოცემულია 15.4 ნახაზზე.



ნახ.15.4. საკვანძო ქმედებები ISM-ის ფარგლებში

ინფორმაციული უსაფრთხოების პოლიტიკის უზრუნველსაყოფად და მხარდასაჭერად აუცილებელია უსაფრთხოების კონტროლების ერთობლიობის ფორმირება და გამოყენება.

ინციდენტების თავიდან ასაცილებლად და სწორი რეაგირებისთვის მათი აღმოცენების შემთხვევაში იყენებენ უსაფრთხოების ზომებს , რომლებიც 15.5 ნახაზზეა ასახული.



ნახ.15.5. უსაფრთხოების კონტროლი

ნახაზზე გამოყოფილია ოთხი სტადია.

პირველი – საფრთხის წარმოქმნა. საფრთხე არის ყველაფერი, რაც უარყოფითად აისახება ბიზნესპროცესზე ან შეუძლია მისი შეწყვეტა. ინციდენტი არის რეალიზებული საფრთხე.

ინციდენტი ამოსავალი წერტილია უსაფრთხოების კონტროლის გამოსაყენებლად. ინციდენტის შედეგად ჩნდება ზარალი. რისკების მართვის ან აღმოფხვრისათვის ასევე იყენებენ უსაფრთხოების კონტროლს. ყოველი სტადიისთვის საჭიროა ინფორმაციული უსაფრთხოების შესაფერისი ზომების შერჩევა:

1. პრევენციული – უსაფრთხოების ზომები, რომლებიც გამორიცხავს წინასწარ ინფორმაციული უსაფრთხოების ინციდენტის გამოვლენას. მაგალითად, წვდომის ნებართვების განაწილება;

2. აღდგენა – უსაფრთხოების ზომები, მიმართული პოტენციური ზარალის შესამცირებლად ინციდენტის შემთხვევაში. მაგალითად, სარეზერვო დუბლირება;

3. აღმომჩენი – უსაფრთხოების ზომები, მიმართული ინციდენტების აღმოსაჩენად. მაგალითად, ანტივირუსული დაცვა ან შემოჭრის აღმოჩენის სისტემა;

4. ჩამხშობი (აღმკვეთი) – უსაფრთხოების ზომები, რომლებიც ეწინააღმდეგება საფრთხის რეალიზაციის მცდელობას, ანუ ინციდენტებს. მაგალითად, ბანკომატი ართმევს კლიენტს ელექტრონულ ბარათს მის მიერ რამდენჯერმე PIN-კოდის არასწორად შეტანის შემთხვევაში;

5. მაკორექტირებელი – უსაფრთხოების ზომები, მიმართული აღდგენისათვის ინციდენტის შემდეგ. მაგალითად, სარეზერვო დუბლების აღდგენა, წინა სამუშაო მდგომარეობაში დაბრუნება და ა.შ.

ISM პროცესის შესასვლელებია:

1. ინფორმაცია ბიზნესიდან – სტრატეგიები, გეგმები, ბიზნესის ბიუჯეტი, ასევე მისი მიმდინარე და სამომავლო მოთხოვნები;

2. ბიზნესის უსაფრთხოების პოლიტიკა, უსაფრთხოების გეგმები, რისკების ანალიზი;

3. ინფორმაცია IT-დან – სტრატეგია, გეგმები და ბიუჯეტი IT-ის;

4. ინფორმაცია სერვისების შესახებ – *SLM-დან*, კერძოდ, სერვისების პორტფელიდან და კატალოგიდან, SLA/*SLR*;

5. რეპორტები: პროცესების და რისკების ანალიზი *ISM-დან*, სერვისების წვდომის მართვის და უწყვეტობის მართვის;

6. დეტალური ინფორმაცია ინფორმაციული უსაფრთხოების ყველა ინციდენტზე და „ხვრელებზე“;

7. ინფორმაცია ცვლილებების შესახებ – ინფორმაცია ცვლილებების მართვის პროცესიდან, კერძოდ, ცვლილებათა განრიგი და მათი გავლენა გეგმებზე, პოლიტიკაზე და ინფორმაციული უსაფრთხოების კონტროლზე;

8. ინფორმაცია ბიზნესის ურთიერთმიმართებაზე სერვისებთან, დამხმარე სერვისებთან და ტექნოლოგიებთან;

9. ინფორმაცია სერვისებთან და სისტემებთან პარტნიორების და მიმწოდებლების წვდომის შესახებ, წარმოდგენილი მიმწოდებელთა მართვის და წვდომის მართვის პროცესების მიერ.

ISM-ის გამოსასვლელებია:

1. ყოვლისმომცველი ინფორმაციული უსაფრთხოების პოლიტიკა და სხვა დამხმარე პოლიტიკა, რომელსაც აქვს კავშირი ინფორმაციულ უსაფრთხოებასთან;

2. ინფორმაციული უსაფრთხოების მართვის სისტემა (ISMS) შეიცავს მთელ ინფორმაციას, აუცილებელს *ISM-ის* უზრუნველსაყოფად;

3. რისკების გადაფასების შედეგები და რევიზიის რეპორტები;

4. უსაფრთხოების კონტროლის ერთობლიობა, მათი ექსპლუატაციის, ასევე მათთან დაკავშირებული ყველა რისკის მართვის აღწერა;

5. ინფორმაციული უსაფრთხოების აუდიტი და რეპორტები;

6. ინფორმაციული უსაფრთხოების გეგმების ტესტირების განრიგი;

7. ინფორმაციული აქტივების კლასიფიკაცია;

8. რეპორტები ინფორმაციულ უსაფრთხოებასა და ინციდენტებში არსებული „ხვრელების“ შესახებ;

9. პოლიტიკა, პროცესები და პროცედურები მიმწოდებელთა და პარტნიორთა წვდომის მართვისათვის სერვისებთან და სისტემებთან.

ინფორმაციული უსაფრთხოების მწარმოებლურობის პროცესის საკვანძო მაჩვენებლებად შეიძლება გამოყენებულ იქნას მეტრიკების სიმრავლე, მაგალითად:

1. ბიზნესის დაცულობა ინფორმაციული უსაფრთხოების დარღვევისგან:
   - შეტყობინებების პროცენტული შემცირება „ხვრელების“ შესახებ სერვის-დესკზე;
   - ბიზნესზე ნეგატიური გავლენის პროცენტული შემცირება „ხვრელების“ და ინციდენტების მხრიდან;
   - პროცენტული გაზრდა პუნქტების, რომელთაც ეხება ინფორმაციული უსაფრთხოება, SLA-ში.

2. ინფორმაციული უსაფრთხოების ცხადი და შეთანხმებული პოლიტიკის ფორმირება, ბიზნესის მოთხოვნილებათა გათავალისწინებით, ანუ არადამთხვევათა რაოდენობის შემცირება *ISM-ის* პროცესებსა და ბიზნესის ინფორმაციული უსაფრთხოების პროცესებსა და პოლიტიკას შორის;

3. უსაფრთხოების უზრუნველყოფის პროცედურები, რომლებიც გამართლებული, შეთანხმებული და დამტკიცებულია ორგანიზაციის ხელმძღვანელობის მიერ:
   - უსაფრთხოების უზრუნველყოფის პროცედურების შეთანხმებულობის და სარგებლიანობის გაზრდა;
   - მხარდაჭერის გაზრდა ხელმძღვანელობის მხრიდან;

4. სრულყოფის მექანიზმები:
   - შეთავაზებულ სრულყოფათა რაოდენობა კონტროლთან და პროცედურებთან მიმართებით;

- არადამთხვევათა რაოდენობის შემცირება ტესტირების და აუდიტის დროს აღმოჩენის პროცესში.

5. ინფორმაციული უსაფრთხოება არის განუყოფელი ნაწილი *ITSM-ის* სერვისებისა და პროცესების, ანუ შესაძლებელია სერვისების და პროცესების რაოდენობის ზრდა, რომლებშიც გათვალისწინებულია უსაფრთხოების ზომები.

ISM ეჯახება სიძნელეებს და რისკებს ინფორმაციული უსაფრთხოების უზრუნველყოფის გზაზე. სამწუხაროდ, პრაქტიკაში ძალზე ხშირად ბიზნესი თვლის, რომ ინფორმაციული უსაფრთხოების საკითხებზე უნდა იმუშაოს მხოლოდ IT-მ. კიდევ უარესია, როცა ბიზნესს არ ესმის, თუ საერთოდ რისთვისაა საჭირო ყურადღების მიქცევა ინფორმაციულ უსაფრთხოებაზე.

ინფორმაციის დაცვის ეფექტური სისტემის შექმნა მოიცავს დიდ ხარჯებს, რაც უნდა ესმოდეს ხელმძღვანელობას, რადგან ისინი წყვეტენ ფინანსირების საკითხებს. ამ დროს მნიშვნელოვანია ბალანსის დაცვა – ინფორმაციული უსაფრთხოების უზრუნველყოფა არ უნდა ღირდეს თვით დასაცავ ინფორმაციაზე ძვირი.

15.3. მიმწოდებლების მართვა

მიმწოდებელთა მართვა (Supplier Management) – ესაა პროცესი, პასუხისმგებელი იმის უზრუნველყოფაზე, რომ ხელშეკრულებები მიმწოდებლებთან შეესაბამება ბიზნესის მოთხოვნებს, და ყველა მიმწოდებელი ასრულებს თავის კონკრეტულ ვალდებულებებს [11].

<u>ტერმინები:</u>

Supplier = მიმწოდებელი

Provider = სერვისების მიმწოდებელი

მიმწოდებელი (Supplier) – მესამე მხარეა, რომელიც პასუხისმგებელია საქონლის და სერვისის მიწოდებაზე, რომლებიც აუცილებელია IT–სერვისების უზრუნველსაყოფად.

მიმწოდებელთა მაგალითებია: ვენდორები პროგრამული და აპარატურული უზრუნველყოფის, ქსელური ტელეკომუნიკაციური პროვაიდერები, ასევე აუთსორსინგული ორგანიზაციები.

განსაზღვრებიდან ნათელია, რომ მიმწოდებელს შეუძლია ასევე IT-სერვისების მიწოდება, მაგრამ საკვანძოა ის, რომ იგი მესამე მხარეა !

ძალზე მნიშვნელოვანია მიმწოდებელთა მართვის პროცესის ინტეგრირება სერვისების სასიცოცხლო ციკლის ყველა სტადიაზე, რადგან მიმწოდებლები ასრულებენ უდიდეს როლს სერვისების უზრუნველყოფაში.

მიმწოდებელთა მართვის პროცესის შუალედური მიზნები:

1. ფასეულობის მიღება ბიზნესის მიერ დახარჯული ფულის სანაცვლოდ;

2. უზრუნველყოფა იმის, რომ ყველა ძირითადი კონტრაქტი და შეთანხმება მიმწოდებლებთან შეესაბამება ბიზნესის მოთხოვნებს, SLA და *SLR*-ის მოთხოვნებს;

3. მიმწოდებლებთან ურთიერთმიმართებების მართვა;

4. მიმწოდებელთა მწარმოებლურობის მართვა;

5. მიმწოდებლებთან მოლაპარაკებების წარმართვა და კონტრაქტების დადება, ასევე მათი მართვა სერვისების სასიცოცხლო ციკლის შიგნით;

6. მიმწოდებელთა პოლიტიკის მართვა, მიმწოდებელთა და ხელშეკრულებათა მხარდამჭერი ბაზის მართვა.

ყოველ პროვაიდერს უნდა ჰქონდეს სტრუქტურირებული მიდგომა მიმწოდებელთა მართვისათვის, თავიანთი სერვისების ეფექტური უზრუნველყოფისათვის. მრავალი მიმწოდებელი

აწვდის დამხმარე სერვისებს და პროდუქტებს, რომლებსაც ნაკლები გავლენა აქვს სერვისების უზრუნველყოფაზე. ოღონდაც დამხმარე სერვისების და პროდუქტების გაერთიანებას შეაქვს დიდი წვლილი სერვისების საბოლოო ფასეულობაში, რომლებიც დამკვეთებს წარედგინება.

ამ დროს, რაც მეტი წვლილი შეაქვთ მიმწოდებლებს სერვისის საბოლოო ფასეულობაში, მით მეტი ყურადღება უნდა გამოიჩინოს პროვაიდერმა სერვისების მიმწოდებელთა მართვის პროცესისადმი.

მიმწოდებელთა მართვის პროცესი უნდა შეიცავდეს::

1. მიმწოდებელთან მუშაობის პოლიტიკის ფორმირება და დაცვა;
2. მიმწოდებლების და ხელშეკრულებების ბაზის ფორმირება, მისი მართვა;
3. მიმწოდებელთა და კონტრაქტთა კატეგორირება, რისკების შეფასება;
4. მიმწოდებელთა და კონტრაქტთა შეფასება და შერჩევა;
5. მოლაპარაკებების წარმართვა და კონტრაქტების და შეთანხმებების გაფორმება;
6. კონტრაქტების მიმოხილვა, გადახედვა და შეწყვეტა;
7. მიმწოდებელთა და მათი მწარმოებლურობის მართვა;
8. მიმწოდებელთა სერვისების, ასევე მათი სრულყოფის გეგმების შეთანხმება და რეალიზაცია;
9. სტანდარტული კონტრაქტების, ტერმინებისა და პირობების მართვა;
10. დავების მართვა, რომლებიც ჩნდება მოლაპარაკებების დროს და კონტრაქტების დადებისას.

კონკრეტულ მიმწოდებლებთან ურთიერთობისთვის პასუხს უნდა აგებდეს პროვაიდერის პერსონალიდან დანიშნული პირი. გამოყოფენ მიმწოდებელთა მართვის პროცესის მფლობელისა და

კონტრაქტების მენეჯერის როლს. მცირე ორგანიზაციებში ეს როლები შეთავსებულია.

მართვა თვალყურს ადევნებს იმას, რომ მიმწოდებლები ასრულებდნენ თავიანთ ვალდებულებებს კონტრაქტების შესაბამისად, მიაღწიონ მიზნობრივ მაჩვენებლებს დადგენილ დროში. ცენტრალურ საცავად ინფორმაციის შესანახად იყენებენ მიმწოდებელთა და ხელშეკრულებათა ბაზას.

მიმწოდებელთა და ხელშეკრულებათა ბაზა (Supplier and Contract Database ან SCD) – ესაა მონაცემთა ბაზა ან სტრუქტურირებული დოკუმენტი, რომელიც გამოიყენება მიმწოდებელთა ხელშეკრულებების მართვისათვის მათი მთელი სასიცოცხლო ციკლის განმავლობაში.

SCD შედგება მიმწოდებელთა ყველა ხელშეკრულების საკვანძო ატრიბუტებისგან. SCD უნდა შეიქმნას ცხადად განსაზღვრული როლებით და პასუხისმგებლობებით (ნახ.15.6).

SCD უნდა მოიცავდეს:

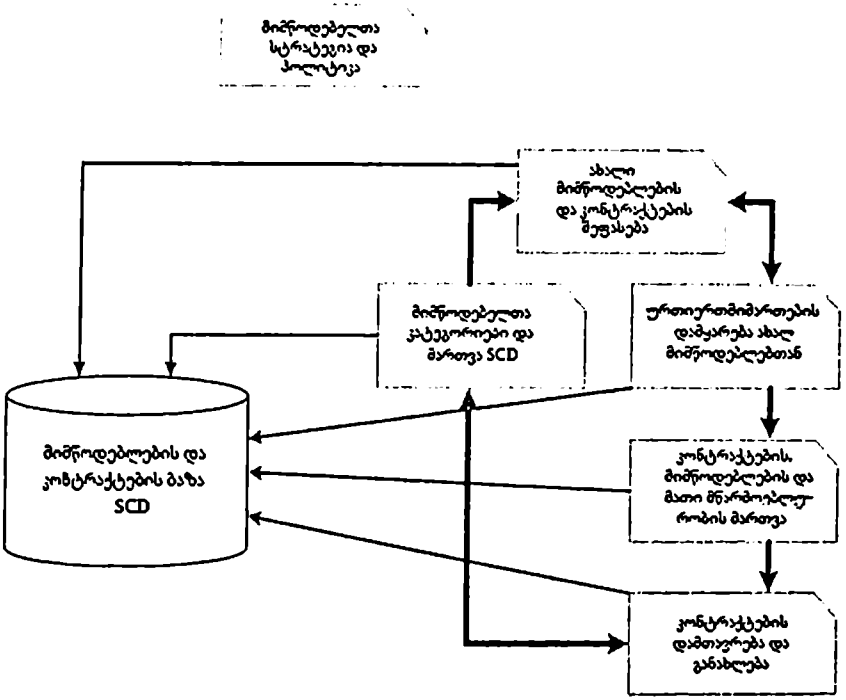
1. მიმწოდებელთა კატეგორირებას და SCD-ს მართვას (დაპროექტების ეტაპი);

2. ახალი მიმწოდებლის ძებნა და შეფასება (დაპროექტების ეტაპი);

3. ახალ მიმწოდებლებთან ურთიერთდამოკიდებულებათა დამყარება (დანერგვის ეტაპი);

4. კონტრაქტების, მიმწოდებლების და მათი მწარმოებლურობის მართვა (ექსპლუატაციის ეტაპი);

5. კონტრაქტების განახლება და დამთავრება (ექსპლუატაციის ეტაპი).



ნახ.15.6. მიმწოდებლების მართვის პროცესი

შემდგომში განვიხილავთ ძირითად ქმედებებს მიმწოდებლების მართვის ფარგლებში.

15.3.1. ახალი მიმწოდებლების და კონტრაქტების შეფასება

სერვისების მიმწოდებელთა არჩევისას საჭიროა ფაქტორების სიმრავლის გათვალისწინება, კერძოდ, მისი წინა წლების მიღწევები და ახლანდელი შესაძლებლობები, ასევე სხვა ორგანიზაციების რეკომენდაციები მათ შესახებ. მიმწოდებელთან ურთიერთობის ტიპისგან დამოკიდებულებით შეიძლება სხვა,

ახალი ფაქტორების გამოყენებაც. ამასთან დაკავშირებით ყოველ ორგანიზაციას უნდა ჰქონდეს ფორმალიზებული პროცესები და პროცედურები ახალი მიმწოდებლების და კონტრაქტების შესაფასებლად.

სერვისის მხარდაჭერა შეიძლება ხდებოდეს ერთი ან რამდენიმე მიმწოდებლისგან. ამ დროს ბევრი ურთიერთობა მიმწოდებლებთან შეიძლება დახასიათდეს როგორც პარტნიორული. ანუ, დღეისათვის ორგანიზაციები გვერდს უვლიან დამოკიდებულებათა ტრადიციულ იერარქიულ წყობას მიმწოდებლებთან, რომელშიც მიმწოდებლები ყოველთვის დამოკიდებული იყვნენ დამკვეთებისგან. დამოკიდებულებები მიმწოდებლებთან ხასიათდება შემდეგით:

1. ორიენტაცია სტრატეგიაზე – დამოკიდებულებები აიწყობა კულტურის, ბიზნესის ფასეულობების და მიზნების, ანუ მისი სტრატეგიის შესაბამისად;

2. ინტეგრაცია – ორი ორგანიზაციის პროცესების მჭიდრო ინტეგრაცია;

3. ინფორმაციული ნაკადი – კარგად აწყობილი ინფორმაციის გაცვლა ორი ორგანიზაციის პროცესებს შორის;

4. ურთიერთნდობა – ურთიერთნდობა ორგანიზაციებს შორის;

5. გახსნილობა – გახსნილობა სერვისების მწარმოებლურობასთან, ხარჯებთან და რისკების ანალიზთან მიმართებით;

6. კოლექტიური პასუხისმგებლობა – გუნდები, ორი ორგანიზაციის თანამშრომელთა გაერთიანება, აგებს პასუხს მიმდინარე მწარმოებლურობაზე და თანამშრომლობის განვითარებაზე მომავალში;

7. *საერთო რისკები და პრემიები* – შეთანხმება იმაზე, თუ როგორ იქნება განაწილებული სარგებელი და თანმხლები რისკები.

ამ პრინციპებზე დაფუძნებულ დამოკიდებულებებს მოაქვს სარგებლობა ორივე მხარისთვის. მჭიდრო ინტეგრაციის გამო მიმწოდებელს შეუძლია სწრაფი რეაგირება ორგანიზაციის მოთხოვნილებებზე, ხოლო ორგანიზაცია, შესაბამისად, იღებს უფრო მეტ ფასეულობას მიმწოდებელთან ურთიერთმიმართებით.

ორ მხარეს შეუძლია ააწყოს თავისი IT სტრუქტურები ერთმანეთის მიმართ, რაც უზრუნველყოფს სერვისების დამატებით ეფექტურობას და ხარჯების შემცირებას. ამ დროს ყოველ მონაწილეს კარგად უნდა ესმოდეს, თუ რას ელოდება მისგან მეორე მონაწილე.

პროვაიდერმა უნდა გაითვალისწინოს მიმწოდებლის არჩევის მიდგომა. იგი უნდა იყოს დაფუძნებული ისეთ ფაქტორებზე, როგორიცაა სერვისის მნიშვნელობა, უზრუნველყოფილი მიმწოდებლის მიერ, რისკები და ღირებულება. აუცილებლად ითვლება რისკების ანალიზის ჩატარება ნებისმიერი შეთანხმების დადებამდე. რისკების ანალიზმა უნდა განიხილოს ყველა შესაძლო რისკი: ფინანსური, რეპუტაციის დაკარგვის, ოპერაციული, სამართლებრივი და ა.შ.

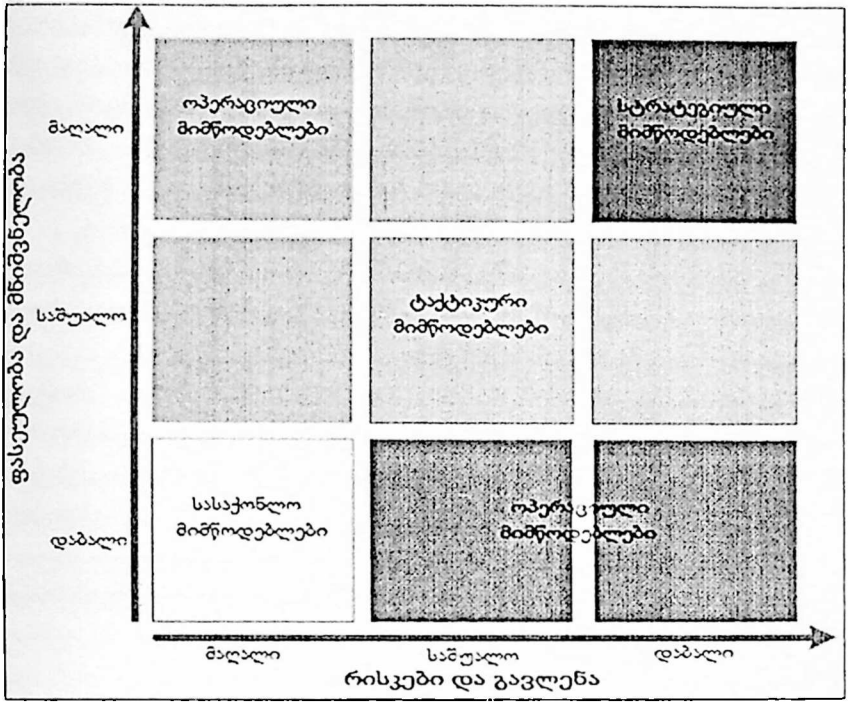
რაც უფრო სრული და დეტალური კონტრაქტი იქნება დადებული, მით ნაკლები დავა და უთანხმოება იქნება მომავალში. საბაზო კონტრაქტის ძირითადი ნაწილებია:

- ძირითადი პირობები და ვადები – ვადა, რომლისთვისაც იდება კონტრაქტი. მხარეები, რომლებიც მას დებენ. არეალი, განსაზღვრებანი და კომერციული ბაზისი;
- სერვისების აღწერა – სერვისებით უზრუნველყოფილი ფუნქციურობა, მათი მწარმოებლურობა, წვდომა, უსაფრთხოება და ა.შ., აგრეთვე შეზღუდვები, რომლებიც გავლენას ახდენს სერვისების მწარმოებლურობაზე და მათ უზრუნველყოფაზე;

- ნორმები სერვისებისთვის – მეტრიკები და ხერხები სერვისების გასაზომად, მწარმოებლურობის და ხარისხის მინიმალური დონეები. მონიშნული დონეები უნდა იყოს ცხადი, მიღწევადი და გაზომვადი, შეესაბამებოდეს ბიზნესის პრიორიტეტებს და მხარს უჭერდეს SLA და *SLR-ს* მიზნობრივ დონეებს;
- საწარმოო დატვირთვა – წარმოების მოცულობა, რომლებისთვისაც გამოიყენება სერვისების ნორმები და საფასო დიაპაზონის ცალკეული საზღვრები;
- მმართველობითი ინფორმაცია – ინფორმაცია, რომელიც უნდა წარმოადგინოს მიმწოდებელმა ოპერაციული მწარმოებლურობის შესახებ. აუცილებელია, რომ ურთიერთდამოკიდებულება აიგოს სერვისების მწარმოებლურობის რაც შეიძლება მნიშვნელოვანი მეტრიკებით;
- პასუხისმგებლობა და დამოკიდებულება - ორგანიზაციის და მიმწოდებლის ვალდებულებათა აღწერა.

15.3.2. მიმწოდებელთა კატეგორიები და **SCD**-ს მართვა

მიმწოდებელთა მართვის პროცესი უნდა იყოს ადაპტირებადი და დიდ დროს და ყურადღებას უთმობდეს ორგანიზაციისთვის განსაკუთრებით მნიშვნელოვან მიმწოდებლებს. ამისათვის აუცილებელია პრიორიტეტების განთავსება მიმწოდებლების მიხედვით, ანუ მოხდეს მათი კატეგორირება. ამ მიზნით უკეთესია მიმწოდებელთა წვლილის და რისკის შეფასება ბიზნესისთვის მათი ფასეულობის მიხედვით (ნახ.15.7).



ნახ.15.7. მიმწოდებელთა კატეგორირება

ამის შესაბამისად შეიძლება შემდეგი კატეგორიების შეთავაზება:

1. სტრატეგიული მიმწოდებლები – მათთან ურთიერთობა იმართება ორგანიზაციის ხელმძღვანელობის დონეზე. ფორმირდება გრძელვადიანი კონტრაქტები, და ხდება კონფიდენციალური ინფორმაციის გაცვლა მიმწოდებლებთან. ასეთი დამოკიდებულებები მოითხოვს დაპროექტების და სტრატეგიის აგების ეტაპების რესურსს, ასევე უწყვეტი სრულყოფის სტრატეგიის დამუშავებას;

2. ტაქტიკური მიმწოდებლები - მათთან ურთიერთობა იმართება საშუალო დონის მენეჯერების დონეზე. ტაქტიკურ მიმწოდებელს მიეკუთვნება ის, ვისაც შეაქვს მნიშვნელოვანი კომერციული წვლილი და აქვს მჭიდრო კავშირი ბიზნესთან. მაგალითად, მიმწოდებელი, რომელიც უზრუნველყოფს სერვერების აღდგენის სერვისებს აპარატურული მტყუნებების შემდეგ;

3. ოპერაციული მიმწოდებლები – ოპერაციული სერვისების და პროდუქტების მიმწოდებლები. ურთიერთობები ასეთ მიმწოდებლებთან იმართება ქვედა დონის მენეჯერების მიერ და მოიცავს იშვიათ, მაგრამ რეგულარულ კონტაქტებს და მწარმოებლურობის მიმოხილვებს, მაგალითად, ინტერნეტ–ჰოსტინგის მიმწოდებელი, ბიზნესისთვის ნაკლებგამოყენებადი და ნაკლებმნიშვნელოვანი საიტის;

4. სასაქონლო მიმწოდებლები – დაბალი ფასეულობის პროდუქტების მიმწოდებლები ან ვისი სერვისები და პროდუქტებიც შეიძლება ადვილად შეიცვალოს ალტერნატიულით. მაგალითად, ქაღალდის ან ორგტექნიკის მიმწოდებლები.

ასეთი კლასიფიკაციიდან გამომდინარე, რაც უფრო სპეციალიზებულ სერვისს ან პროდუქტს გვთავაზობს მიმწოდებელი, მით უფრო მეტი ყურადღება უნდა დაეთმოს მას, მიმწოდებელთა მართვის პროცესის ფარგლებში.

სტანდარტული სერვისების მიმწოდებლების ურთიერთობებისთვის არაა საჭირო დიდი დროის და რესურსების ხარჯვა, რადგან ისინი შეიძლება ადვილად შეიცვალოს სხვებით.

სერვისების მიმწოდებელთა არჩევისა და მათი კატეგორირების საფუძველში ძევს ზუსტი გაგება იმისა, თუ რისი მიღება უნდა ბიზნესს მათი სერვისების და პროდუქტებისგან. ამ დროს ძალზე მნიშვნელოვანია, აიგოს მიმწოდებელთა კორექტული

ჯაჭვი. არაა რეკომენდებული რომელიმე ბიზნესპროცესის გადაცემა აუთსორსინგზე ერთ მიმწოდებელზე, რადგან იგი აჩენს რისკების სიმრავლეს.

SCD იძლევა ინფორმაციას მიმწოდებლების შესახებ, მათ მიერ შეთავაზებული სერვისების და პროდუქტების შესახებ და მათთან დადებული კონტრაქტების დეტალების შესახებ.

15.3.3. ახალ მიმწოდებლებთან ურთიერთკავშირის დამყარება

ახალი მიმწოდებლების და კონტრაქტების დამატება SCD-ში უნდა კონტროლირდებოდეს ცვლილებების მართვის პროცესით. ეს იძლევა შეფასების გარანტიას და გავლენის გაგებას, რომელსაც ისინი მოახდენენ ბიზნესზე და მის პროცესებზე.

ამ დროს აუცილებელია ასევე რისკების ანალიზის მონაწილეობა. ახალი რისკები უნდა იქნას გამოვლენილი, შეფასებული და აყვანილი მართვის ქვეშ. ყველა მონაცემის შეკრების შემდეგ, ისინი შეიტანება SCD-ში.

15.3.4. კონტრაქტების, მიმწოდებლების და მათი მწარმოებლურობის მართვა

ორგანიზაციის და მიმწოდებლის ურთიერთობისას შეიძლება წარმოიშვას გაუგებრობა და სადავო მომენტები. ამიტომ ორივე მხარემ უნდა ეცადოს ერთმანეთთან კავშირის მოგვარება.

ITIL-ს შემოაქვს ტერმინი „ოფიციალური მიმოხილვითი შეხვედრები". ამ შეხვედრებისას დამკვეთის და მიმწოდებლის წარმომადგენლები განიხილავენ თანამშრომლობის საკითხებს, აანალიზებენ რეპორტებს წარმოდგენილი სერვისების მწარმოებლურობის შესახებ და ა.შ.

განსახილველი თემები შემდეგია:

- მწარმოებლურობის შესაბამისობა მიზნობრივ მაჩვენებლებთან;
- ინციდენტებისა და პრობლემების მიმოხილვა;
- უკუკავშირი ბიზნესთან და მომხმარებლებთან;
- მოსალოდნელი გლობალური ცვლილებები, რომლებიც მოახდენს გავლენას სერვისზე მომავალში; ასევე წარუმატებელი ცვლილებები და ინციდენტების გამომწვევი ცვლილებები;
- საკვანძო მოვლენები ბიზნესისთვის მომდევნო პერიოდში;
- სერვისების სრულყოფის გეგმები.

შეხვედრების გარდა მიმწოდებლის შესახებ ინფორმაციის კარგ წყაროდ ითვლება ანკეტირება და გამოკითხვა. მათ შეუძლია გამოავლინოს მიმწოდებლის უპირატესობები და ნაკლოვანებები, რომლებიც არ ჩანს სტანდარტულ რეპორტებში.

15.3.5. კონტრაქტების დასრულება და განახლება

კონტრაქტის შესაბამისობის უზრუნველსაყოფად ბიზნესის ცვალებად მოთხოვნილებებთან, იგი პერიოდულად უნდა გადაიხედოს და, აუცილებლობის შემთხვევაში, განახლდეს. კონტრაქტების მიმოხილვები უნდა შეიცავდეს შემდეგს:

- რამდენად კარგად მუშაობს კონტრაქტი და თუ გამოდგება მომავალში გამოსაყენებლად;
- რა ცვლილებებია აუცილებელი (სერვისების, პროდუქტების, კონტრაქტების, მიზნობრივი მაჩვენებლების, შეთანხმებების);
- ურთიერთმიმართებების შეფასება მომავლისთვის (ზრდა, შემცირება, ცვლილება, დამთავრება და ა.შ.);
- კონტრაქტის კომერციული მწარმოებლურობა, მიმოხილვები და შედარება კონკურენტებთან, ფასის და აუცილებელი რესურსის შესაბამისობა;

- კონტრაქტის განვითარების სამომავლო მიმართულების შერჩევა;
- კონტრაქტების და მიმწოდებლების მართვის მეთოდიკა.

რთული კონტრაქტებისთვის, რომლებიც დროის დიდი პერიოდითაა განსაზღვრული, დამახსიათებელია ხანგრძლივი მოლაპარაკებები. ორივე მხარე დაინტერესებულია იმით, რომ კონტრაქტში ცვლილებები არ შევიდეს მაქსიმალურად დიდი ხნის პერიოდში.

მიმწოდებელთა მართვის პროცესის შესასვლელებია:

1. ინფორმაცია ბიზნესიდან – ბიზნესის სტრატეგიები, გეგმები, ბიუჯეტი, აგრეთვე მისი ახლანდელი და მომავალი მოთხოვნები;

2. მიმწოდებელთა და ორგანიზაციათა კონტრაქტების სტრატეგია – გამოყენებულ კონტრაქტთა ტიპები, მიმწოდებლების შესაძლებლობათა გამოყენების პოლიტიკა, სტრატეგიის აგების ეტაპი;

3. მიმწოდებელთა სტრატეგიები და გეგმები – დეტალები ბიზნესგეგმების და მიმწოდებელთა სტრატეგიების, ინფორმაცია ტექნოლოგიის განვითარების შესახებ, ინფორმაცია მათი მიმდინარე ფინანსური მდგომარეობის შესახებ;

4. კონტრაქტები, შეთანხმებები და მიმწოდებლის მიზნები;

5. ინფორმაცია მიმწოდებელთა მწარმოებლურობასა და კონტრაქტებზე;

6. ინფორმაცია IT-დან – სტრატეგია, გეგმები და ბიუჯეტი;

7. მწარმოებლურობის საკითხები – ინფორმაცია ინციდენტების და პრობლემების მართვიდან, მათ შორის ცუდი კონტრაქტების და ცუდი მწარმოებლურობის;

8. ფინანსური ინფორმაცია – ღირებულება მიმწოდებელთა სერვისების, მათი უზრუნველყოფის კონტრაქტების და სარგებელი,

რომელსაც ჯამში მიიღებს ბიზნესი ურთიერთობიდან. აქვე შედის ასევე საფინანსო გეგმები და ბიუჯეტი, აღდგენის ხარჯებთან ერთად მტყუნებათა შემთხვევაში;

9. ინფორმაცია სერვისების შესახებ – ინფორმაცია *SLM* პროცესიდან, დეტალებით სერვისების პორტფელიდან და კატალოგიდან, სერვისების მიზნობრივი მაჩვენებლები, მოხსენიებული SLA, OLA, *SLR-ში;*

10. ინფორმაცია ბიზნესის ურთიერთმიმართების შესახებ სერვისებთან, დამხმარე სერვისებთან და ტექნოლოგიებთან.

მიმწოდებელთა მართვის პროცესის გამოსასვლელებია:

1. SCD – ინფორმაციის საცავი, აუცილებელი ყველა პროცესისთვის, სერვისების მიმწოდებელთა მართვის ფარგლებში;

2. რეპორტები მიმწოდებელთა მწარმოებლურობისა და კონტრაქტების შესახებ – ეს ინფორმაცია გამოიყენება მიმოხილვით შეხვედრებზე სერვისების ხარისხის ასახვისათვის, წარმოდგენილი მიმწოდებლების მიერ და კონტრაქტებით;

3. რეპორტები მიმოხილვითი შეხვედრების შესახებ;

4. მიმწოდებელთა სერვისების სრულყოფის გეგმები – ასახავს ყველა ქმედებას სერვისების სრულყოფისათვის, შეთანხმებულს მიმწოდებლებსა და დამკვეთებს შორის;

5. ადამიანთა ანკეტირება ორგანიზაციის შიგნით, რომლებიც უშუალოდ ეკონტაქტებიან მიმწოდებლებს.

ეფექტურობის საკვანძო მაჩვენებლებად განიხილება:

1. ბიზნესის დაცულობა მიმწოდებელთა ცუდი მწარმოებლურობისგან ან მტყუნებებისგან უზრუნველყოფაში:

- მიმწოდებელთა რაოდენობის გაზრდა, რომლებიც ასრულებენ კონტრაქტის მოთხოვნებს;
- კონტრაქტების დარღვევათა რაოდენობის შემცირება;

2. წარმოდგენილი სერვისების მაჩვენებელთა შესაბამისობა ბიზნესის მოთხოვნებთან:

- სერვისების და კონტრაქტების მიმოხილვათა რაოდენობის გაზრდა;
- მიმწოდებლებისა და კონტრაქტების მიზნობრივი მაჩვენებლების რაოდენობის გაზრდა, შესაბამისად მიზნობრივ მაჩვენებლებთან SLA და *SLR-ში.*

დაპროექტების და ახალი ტექნოლოგიების განვითარების ქმედება არ უნდა იყოს იზოლირებული, რადგან მოქმედებს სხვა სერვისებზე, სისტემებზე, ინსტრუმენტებზე, არქიტექტურაზე, პროცესებზე და ა.შ.

სხვა სიტყვებით, დაპროექტება უნდა ითვალისწინებდეს არა მხოლოდ სერვისების და კომპონენტების მოთხოვნებს და ფუნქციურობას. მმართველობითი და ოპერაციული მოთხოვნები ასევე უნდა იყოს ჩადებული დიზაინის აგების საფუძვლად ახლი ან შეცვლილი სერვისებისთვის.

მიმწოდებელთა მართვის ძირითად რისკებად განიხილავენ ინფორმაციის უკმარობას, ცუდად აწყობილი ინფორმაციის გაცვლა ბიზნესსა და მიმწოდებელს შორის, არაკორექტული ან შეუსრულებელი მიზნები, რესურსებისა და ფინანსების დეფიციტი.

ამგვარად, ჩვენ აქ განვიხილეთ სერვისების დაპროექტების ეტაპის ექვსი ძირითადი პროცესი, რომლებიც უზრუნველყოფს მას აუცილებელი ინფორმაციით ახალი ან შეცვლილი სერვისების დასაპროექტებლად.

16. დანერგვა – სერვისების სასიცოცხლო ციკლის ეტაპი

16.1. სერვისების დანერგვის ეტაპის არსი და ტერმინები, მიზნები და ამოცანები

ბიზნესის მართვის პროცესის სრულყოფა ხორციელდება პროექტების განხორციელების საშუალებით, რომლებშიც მონაწილეობს IT-დეპარტამენტიც. ნებისმიერი უმნიშვნელო ოპერაციული სრულყოფა ან გლობალური მოვლენა, რომელიც გარდაქმნის მთლიან ბიზნესს, საბოლოო ჯამში იწვევს ცვლილებას. კერძოდ, ახალი ან შეცვლილი სერვისის გამოყენებაც არის ცვლილება ბიზნესისთვის.

დანერგვის ეტაპი იძლევა გარანტიას, რომ სასიცოცხლო ციკლის წინა სტადიებზე დაგეგმილი და დაპროექტებული სერვისები შეძლებს ბიზნესისა და IT-ისთვის მოსალოდნელი შედეგების პრაქტიკულ მიღებას. ამგვარად, დანერგვა არის სერვისის ერთგვარი შემოწმების პროცესი, მისი უშუალოდ ექსპლუატაციაში გადაცემის წინ.

განვიხილოთ დანერგვასთან დაკავშირებული ტერმინები:

• გარდაქმნა (Transition) – მდგომარეობის ცვლილება, რომელიც შეესაბამება სერვისის ან კონფიგურაციული ერთეულის გადაადგილებას სასიცოცხლო ციკლის ერთი სტადიიდან მეორეზე.

• რელიზი (Release) – ერთობლიობა აპარატურული და პროგრამული უზრუნველყოფების, დოკუმენტაციის, პროცესების ან სხვა კომპონენტებისა, რომლებიც აუცილებელია სერვისში ერთი ან რამდენიმე შეთანხმებული ცვლილების დასანერგად. ყოველი რელიზის შედგენილობა იმართება, ტესტირდება, განთავსდება როგორც ცალკე არსი (ობიექტი).

• მოთხოვნა ცვლილებაზე (Request for Change ან RFC) – ფორმალური წინადადება ცვლილების სარეალიზაციოდ. RFC შეიცავს შემოთავაზებული ცვლილების დეტალურ აღწერას და შეიძლება ჩაიწეროს ქაღალდის ან ელექტრონულ ფორმატში.

• ტესტირება (Test) – ქმედება, რომელიც ამოწმებს (ადასტურებს), რომ სერვისი, პროცესი ან კონფიგურაციული ერთეული შეესაბამება სპეციფიკაციებს ან შეთანხმებულ მოთხოვნებს.

• აწყობა (Build) – ქმედება ერთი ან რამდენიმე კონფიგურაციული ერთეულის ასაწყობად სერვისის ნაწილის ფორმირებისათვის. მაგალითად, სერვერის აწყობა ან ნოუთბუკის აწყობა.

• განთავსება (Deployment) —ქმედება, რომელიც პასუხისმგებელია ახალი ან შეცვლილი დანადგარის, პროგრამის, დოკუმენტაციის, პროცესის გადაადგილებაზე სამრეწველო ექსპლ;უატაციის გარემოში.

• მხარდაჭერა ექსპლუატაციის დასაწყისში (Early Life Support) – მხარდაჭერა, რომელიც სჭირდება ახალ ან შეცვლილ სერვისს გარკვეული პერიოდის განმავლობაში, მისი ექსპლუატაციაში შესვლის შემდეგ. მხარდაჭერის პერიოდში სერვისის მიმწოდებელს შეუძლია გადახედოს KPI-ს, სერვისის დონეებს და საკონტროლო ზღვრულ მნიშვნელობებს. აგრეთვე შეუძლია დამატებითი რესურსების ამოქმედება ინციდენტების და პრობლემების სამართავად.

• გარემო (Environment) – IT-ინფრასტრუქტურის ქვესიმრავლე, რომელიც გამოიყენება სხვადასხვა მიზნებისთვის. რთული გარემოსთვის არის შესაძლებლობა კონფიგურაციული ერთეულების ერთობლივი გამოყენებისთვის. მაგალითად, ტესტირების გარემოს და სამრეწველო ექსპლუატაციის გარემოს შეუძლია გამოიყენოს სხვადასხვა განყოფილებები ერთ მაინფრეიმზე.

• სამრეწველო ექსპლუატაციის გარემო (Live Environment) – მართვადი გარემო, შეიცავს კონფიგურაციულ ერთეულებს სამრეწველო ექსპლუატაციის რეჟიმში, რომელიც გამოიყენება სერვისის მისაწოდებლად.

• ტესტირების გარემო (Test Environment) – საკონტროლებელი გარემო, რომელიც გამოიყენება სერვისების, კონფიგურაციული ერთეულების, პროცესების, ანაწყობების ტესტირებისათვის.

• ანაწყობის გარემო (Build Environment) – საკონტროლებელი გარემო, რომელშიც თავს იყრის აპლიკაციები, სერვისები და სხვა ანაწყობები მანამ, სანამ ისინი იქნება გადაცემული ტესტირების ან სამრეწველო ექსპლუატაციის გარემოში.

• მიღება (Acceptance) – ფორმალური შეთანხმება, რომელიც განსაზღვრავს, რომ სერვისი, პროცესი, გეგმა ან სხვა შედეგი დასრულებულია, არის სწორი, საიმედო და პასუხობს დადგენილ მოთხოვნებს. მიღებას წინ უსწრებს შეფასება ან ტესტირება. მიღება ხშირად სავალდებულოა პროექტის ან პროცესის მომდევნო ეტაპზე გადასასვლელად.

დანერგვის ეტაპის ძირითადი მიზნებია:

• დაგეგმვა / მართვა: სიმძლავრეების და რესურსების, რათა განხორციელდეს სერვისების დაკომპლექტება, აწყობა, ტესტირება და სამრწეველო ექსპლუატაციაში გაშვება, აგრეთვე სერვისების ფუნქციონირების უზრუნველყოფა ინვესტორების და დამკვეთების მოთხოვნების შესაბამისად.

• სერვისების სიმძლავრის ზუსტი და თანმიმდევრული შეფასების სისტემის აგება და რისკების სიის ფორმირება ხდება მანამ, სანამ ახალი ან შეცვლილი სერვისი იქნება გაშვებული სამრეწველო ექსპლუატაციაში.

• დანერგვის ეტაპზე გამოსაყენებელი სერვისის აქტივების ნაკრების და კონფიგურაციების ფორმირება და მათი მართვა.

• ინფორმაციის მიწოდება, რომელიც აუცილებელია გადაწყვეტილების მისაღებად სერვისის შეტანის შესახებ საწარმოო ექსპლუატაციაში ტესტირების შემდეგ.

• ეფექტური და განმეორებადი მექანიზმების წარმოდგენა ნაკრებისა და ინსტალირებისთვის, რომლებიც შეიძლება გამოყენებულ იქნას რელიზების განთავსებისთვის საწარმოო ექსპლუატაციის და ტესტირების გარემოში.

• სერვისების მართვის, მხარდაჭერის და კორექტული ექსპლუატაციის უზრუნველყოფა დაპროექტების ეტაპზე განსაზღვრული მოთხოვნების შესაბამისად.

დანერგვის ეტაპის ამოცანებია:

• დამკვეთთა მოლოდინის განსაზღვრა, თუ როგორ დაეხმარება ბიზნესს ახალი ან შეცვლილი სერვისი.

• ახალი ან შეცვლილი სერვისის ინტეგრაციის მიზნით დახმარება დამკვეთთა ბიზნესპროცესში.

• განსხვავების შემცირება პროგნოზირებულ და რეალურ მწარმოებლურობას შორის.

• ცნობილი შეცდომების და რისკების რაოდენობის შემცირება ახალი ან შეცვლილი სერვისის გაშვებისას საწარმოო ექსპლუატაციაში.

• სერვისის გამოყენების უზრუნველყოფა მისთვის დადგენილი მოთხოვნებისა და შეზღუდვების გათვალისწინებით.

დანერგვის ეტაპს აქვს ბიზნესისთვის შემდეგი ღირებულება:

• აუმჯობესებს ადაპტირების უნარს ახალი მოთხოვნების ან გარემოებებისადმი ბაზარზე.

• აუმჯობესებს მართვას დანერგვის დონეზე კომპანიების შთანთქმის, დაყოფის ფარგლებში, სერვისების შესყიდვის ან გადაადგილებისას.

• ამაღლებს ბიზნესისთვის წარმატებული ცვლილებების და რელიზების რაოდენობას.

• აუმჯობესებს პროგნოზირების სიზუსტეს ახალი ან შეცვლილი სერვისის დონის და ხარისხის შესაბამისად.

• აუმჯობესებს შეთანხმებულობას ბიზნესის და ხელმძღვანელობის მოთხოვნებთან.

• ამცირებს განსხვავების რაოდენობას დამტკიცებულ ბიუჯეტის გეგმასა და რეალობას შორის.

• ამაღლებს პერსონალის პროდუქტიულობას დაგეგმვის სრულყოფის, ახალი ან შეცვლილი სერვისების გამოყენების შედეგად.

• ამცირებს კონტრაქტების დროებითი შეჩერების ან ცვლილებების შემთხვევებს პროგრამულ და აპარატურულ უზრუნველყოფაზე, კომპონენტების გაერთიანების ან დაყოფის შედეგად.

• აუმჯობესებს რისკის დონის გაგებას ცვლილების დროს და მის შემდეგ.

დანერგვის ეტაპი იმყოფება დაპროექტებისა და ექსპლუატაციის ეტაპებს შორის სასიცოცხლო ციკლში. სწორედ ამ ეტაპებს უკავშირდება იგი უფრო მჭიდროდ და უწყვეტად. დანერგვის ეტაპს კავშირები აქვს ასევე ციკლის სხვა ეტაპებთანაც.

შესასვლელები, რომლებიც შემოდის სტრატეგიის აგების ეტაპიდან, გავლენას ახდენს დანერგვის მიდგომაზე, სტრუქტურებსა და შეზღუდვებზე:

1. სერვისების პორტფელი;

2. დამკვეთთა პორტფელი – მონაცემთა ბაზა ან სტრუქტურირებული დოკუმენტი, რომელიც გამოიყენება ინფორმაციის შესანახად სერვისის მიმწოდებლის ყველა დამკვეთის შესახებ;

3. ხელშეკრულებათა პორტფელი – მონაცემთა ბაზა ან სტრუქტურირებული დოკუმენტი, რომელიც გამოიყენება ხელშეკრულებათა მართვისათვის მომსახურების მიზნით ან შეთანხმებათა მართვისთვის სერვისების მიმწოდებლებსა და მათ დამკვეთებს შორის;

4. სერვისის სასიცოცხლო ციკლის მოდელი;

5. პოლიტიკა;

6. სტრატეგიები;

7. შეზღუდვები;

8. არქიტექტურები;

9. მოთხოვნები დანერგვისათვის;

10. სერვისების მართვის გეგმა.

სერვისების დაპროექტების ეტაპი არის ტრიგერების (ან გაშვების მექანიზმების) წყარო დანერგვის ეტაპისთვის. უპირველეს ყოვლისა, ესაა საპროექტო დოკუმენტაცია (SDP), რომელიც უნდა იქნას რეალიზებული. იგი მოიცავს შემდეგ კომპონენტებს:

8. სერვისის განსაზღვრა;

9. სერვისის სტრუქტურა;

10. ფინანსური მოდელი და დანახარჯების მოდელი;

11. სიმძლავრეების / რესურსების მოდელი;

12. სერვისების მართვის პროცესის იტერაციის მოდელი;

13. სერვისის ექსპლუატაციის მოდელი;

14. დიზაინის და ინტერფეისის სპეციფიკაცია;

15. რელიზის დიზაინი;

16. მიღების კრიტერიუმები.

17. მოთხოვნები ცვლილებებზე (RFC).

სერვისების უწყვეტი სრულყოფის ეტაპი აწვდის დანერგვის ეტაპის შესასვლელზე ინფორმაციას პოლიტიკის, პრაქტიკის და დანერგვის პროცესების სრულყოფის ტერმინებში.

ექსპლუატაციის ეტაპი აწვდის დანერგვის ეტაპის შესასვლელს ინფორმაციას სერვისების ტესტირებისა და მიღებისათვის, სერვისების მიერ მოთხოვნილი მაჩვენებლების მიღწევის ტერმინებში.

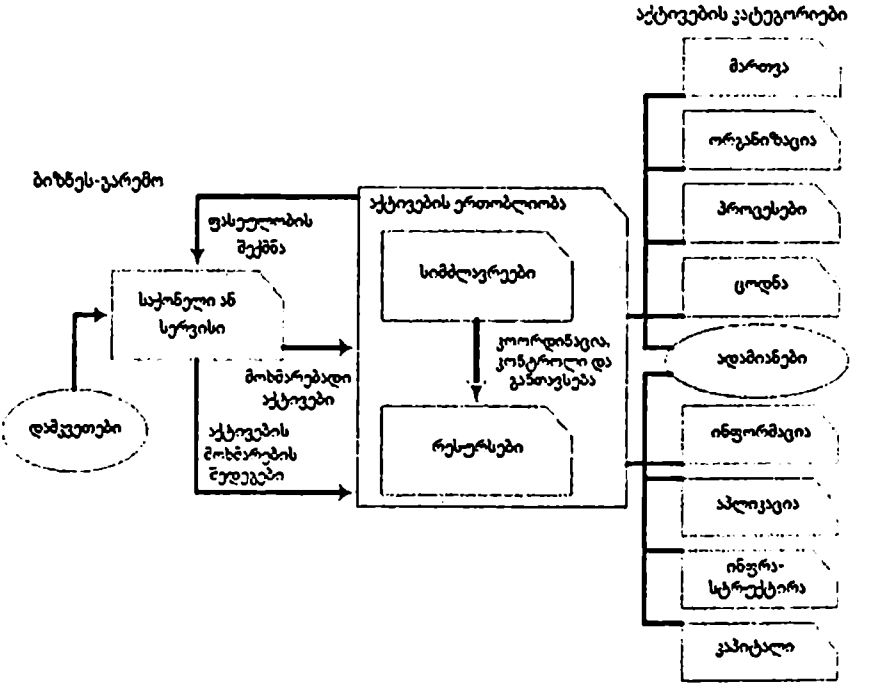
დანერგვის ეტაპის გამოსასვლელებია:

1. რელიზისა და სერვისების განთავსებისთვის დამტკიცებული დოკუმენტაცია;
2. სერვისების განახლებული პაკეტი;
3. განახლებული სერვისების კატალოგი და სერვისების პორტფელი;
4. დოკუმენტაცია დასანერგი ან ჩამოსაწერი სერვისებისთვის.

ITIL-ში გაინიხილება დანერგვის ეტაპის ორი ტიპის პროცესი:

1. პროცესები, რომლებიც მხარს უჭერს სერვისის სასიცოცხლო ციკლს:
   - ცვლილებების მართვა;
   - სერვისების შეფასება და კონფიგურაციების მართვა;
   - ცოდნის მართვა.
2. პროცესები დანერგვის ფარგლებში:
   - დანერგვის დაგეგმვა და მხარდაჭერა;
   - რელიზების და განთავსების მართვა;
   - სერვისების ტესტირება და დადასტურება;
   - შეფასება.

სტრატეგიის აგების ეტაპი უზრუნველყოფს სისტემას სერვისის განსაზღვრის მიზნით. სერვისის ფასეულობა დგინდება დამკვეთის მოთხოვნების კონტექტში. მიმწოდებლის აქტივების გამოყენება ბიზნესისა და დამკვეთებისთვის სერვისებით უზრუნველყოფის თვალსაზრისით მოცემულია 16.1 ნახაზზე.



ნახ.16.1. სერვისით უზრუნველყოფისთვის
საჭირო აქტივები

აქტივების ქვეშ აქ იგულისხმება სერვისების მიმწოდებლის რესურსები და შესაძლობლობანი.

სერვისები უზრუნველყოფს ფასეულობას ბიზნესის აქტივების მწარმოებლურობის ამაღლების გზით ან რისკების შემცირებით. სერვისის ფასეულობა გამოისახება ხარისხის და სარგებლიანობის ტერმინებში. *სარგებლიანობა* არის დამკვეთის აქტივების მწარმოებლურობის (შრომის ნაყოფიერების) ამაღლების შეფასება (ზომა), *ხარისხი* – დარწმუნება იმაში, რომ სერვისი შეასრულებს დადგენილ პირობებს.

განიხილავენ ხარისხის სამ ძირითად მახასიათებელს:

- სერვისების წვდომა და სიმძლავრე;
- გარანტია იმისა, რომ დამკვეთის აქტივები მიიღებს სარგებელს, არასასურველი მოვლენების შემთხვევაშიც კი ან სერვისების დონის დაქვეითებისას;
- უსაფრთხოების უზრუნველყოფა დამკვეთის განსაკუთრებით ფასეული აქტივებისთვის.

ხარისხის აღნიშნული ასპექტებიდან კონკრეტულ სიტუაციაში დამკვეთისთვის ერთ რომელიმეს შეიძლება ჰქონდეს მეტი მნიშვნელობა.

16.2. დანერგვის ეტაპის ძირითადი პრინციპები

განვიხილოთ დანერგვის ეტაპის ძირითადი პრინციპები ITILv3. *Service Transition* - პუბლიკაციის საფუძველზე [11,43].

16.2.1. დანერგვის ფორმალური პოლიტიკის განმარტება და განხორციელება

დანერგვის ფორმალური პოლიტიკა უნდა იყოს განსაზღვრული, დოკუმენტირებული და დამტკიცებული ხელმძღვანელობის მიერ. მას უნდა გაეცნოს ორგანიზაციის ყველა თანამშრომელი, მიმწოდებელი და პარტნიორი, რომელთაც აქვთ შეხება დანერგვასთან.

დანერგვის პრინციპები:

1. პოლიტიკაში გარკვევით უნდა იყოს ფორმირებული მიზნები, ხოლო მისგან ყოველი გადახრა უნდა შესწორდეს ან აღმოიფხვრას;
2. აუცილებელია შესაბამისობის უზრუნველყოფა დანერგვის პოლიტიკასა და სერვისების მართვის პოლიტიკას შორის;
3. პოლიტიკის მაფორმირებელი პასუხისმგებელი ადამიანები უნდა ახდენდნენ თავიანთი დაინტერესების დემონსტრირებას მისი რეალიზაციის მიზნით;

4. გამოყენებულ იქნას პროცესები, რომლებიც აერთიანებს გუნდებს; შერეულ იქნას კომპეტენციები ანგარიშგების წარმოების და პასუხისმგებლობის განაწილების ფარგლებში;

5. უზრუნველყოფილ იქნას ცვლილებები რელიზებში;

6. განხილულ იქნას განთავსების საკითხები უკვე რელიზების დაგეგმვისა და დაპროექტების ეტაპებზეც.

საუკეთესო პრაქტიკა:

მიღებულ იქნას ფორმალური ხელმოწერები მათგან, ვინც მონაწილეობს პოლიტიკის შემუშავებაში: მენეჯერები, სპონსორები და სხვა ადამიანები, რომლებიც იღებენ გადაწყვეტილებას.

16.2.2. ცვლილებების განხორციელება სერვისებში დანერგვის გზით

ყველა ცვლილება, რომელიც ეხება სერვისების პორტფელს და სერვისების კატალოგს, ექვემდებარება ცვლილებათა მართვის პროცესს. ამავდროულად, ყველა ცვლილება უნდა იყოს გარკვევით განსაზღვრული და შეთანხმებული.

ცვლილების პრინციპები:

1. ცვლილებების კონცენტრირება ერთ წერტილში ამცირებს კონფლიქტებს ცვლილებებს შორის, შემდგომ დარღვევებს და მტყუნებებს სამრეწველო ექსპლუატაციის გარემოში;

2. ადამიანებს, რომლებსაც არ აქვთ უფლებები ცვლილებების განსახორციელებლად და სერვისების საწარმოო ექსპლუატაციაში გადასაცემად, არ უნდა ჰქონდეთ წვდომა დანერგვის პროცესებთან;

3. მჭიდრო ურთიერთქმედება ექსპლუატაციის ეტაპთან ამაღლებს მობილობას და შესაძლებელს ხდის ორგანიზაციულ ცვლილებებს;

4. ცოდნის და გამოცდილების ამაღლება სერვისების და საწარმოო ექსპლუატაციის გარემოს ეფექტური გამოყენების საკითხებში;

5. ყოველი რელიზი უნდა იყოს დაპროექტებული ცვლილების მოთხოვნის საფუძველზე და გაიაროს ცვლილებათა მართვის პროცესი, რაც უზრუნველყოფს ეფექტურ მონიტორინგს;

6. ცვლილებების მართვისთვის საჭიროა სტანდარტული მეთოდებისა და პროცედურების გამოყენება, ცვლილებებთან დაკავშირებული ინციდენტების გავლენის შემცირების მიზნით, ბიზნესის უწყვეტობაზე, სერვისების ხარისხსა და სრულყოფაზე;

7. ცვლილების და რელიზის ყველა განახლება ფიქსირდება სერვისის აქტივის კონტექსტში და კონფიგურაციულ ერთეულებში, კონფიგურაციების მართვის სისტემაში (CMS).

საუკეთესო პრაქტიკა:

- ყოველი ცვლილება უნდა იყოს გარკვევით განსაზღვრული;
- უნდა გაიმიჯნოს შიგა და გარე ცვლილებები;
- ცვლილებები უნდა იყოს გამართლებული მკაფიო ბიზნეს-კეისის დახმარებით;
- ცვლილებები განსაზღვრულია საპროექტო დოკუმენტაციაში, რომელსაც დანერგვა იყენებს გეგმური და ფაქტობრივი მწარმოებლურობების შესადარებლად;
- შესაძლებელია ცვლილებათა მართვის არსებული პროცესის სტანდარტიზება და შესრულება;
- მენეჯერები უნდა მონაწილეობდნენ პროცესებში და ეს მკაფიოდ უნდა ჩანდეს ინვესტორებისთვის;
- აუდიტის აწყობა ყველა არაავტორიზებული ცვლილების იდენტიფიკაციისთვის;
- არ იქნას მიღებული „დაგვიანებული“ მოთხოვნები ცვლილებებზე, რომელთა მართვა შეუძლებელია ნორმალური სახით.

16.2.3. დანერგვის ზოგადი სტრუქტურის და სტანდარტების შემუშავება

დანერგვა უნდა აიგოს სტანდარტულ პროცესებსა და სისტემებზე, რომლებიც მრავალჯერადი გამოყენების საშუალებას იძლევა. ეს გააუმჯობესებს დანერგვის ცალკეული ქვეეტაპების ინტეგრაციას და შეამცირებს პროცესების შეუთანხმებლობას.

პრინციპები:

1. გამოყენებულ იქნეს კონკრეტული სფეროს საუკეთესო პრაქტიკა, როგორც დანერგვის სტანდარტიზაციის საფუძველი;

2. უნდა კონტროლირდებოდეს დანერგვის სტრუქტურა და სტანდარტები ცვლილებათა მართვის და კონფიგურაციათა მართვის დახმარებით;

3. იმის უზრუნველყოფა, რომ დანერგვის პროცესები გამოიყენებოდეს სერვისის მართვის სხვა პროცესების რეგულარული მიმოხილვების და აუდიტების თანამიმდევრულად.

საუკეთესო პრაქტიკა:

- დანერგვის სტანდარტების და საუკეთესო პრაქტიკის პუბლიკაცია;
- სისტემის აგება მიმდევრობითი პროცესების შესაქმნელად სერვისების სიმძლავრეების უზრუნველყოფის და გამოყენების მიზნით, რისკების სიის განსაზღვრა რელიზის განთავსებამდე და მის შემდეგ;
- მხარდამჭერი სისტემების შეთავაზება, რომლებიც ემსახურება ავტომატიზებულ პროცესებს წინააღმდეგობათა შემცირების მიზნით დანრეგვის დროს;
- დარწმუნება იმაში, რომ მენეჯმენტს ესმის სტანდარტიზაციის პროცესების აუცილებლობა დამუშავებისა და სრულყოფის შემოთავაზების ფარგლებში, რომლებიც დაფუძნებულია მკაფიო ბიზნესკეისზე.

16.2.4. დანერგვის გეგმების ფორმირება ბიზნესის მოთხოვნათა შესაბამისად

ცვლილებით შემოთავაზებული ფასეულობის მაქსიმიზაციის მიზნით აუცილებელია დანერგვის გეგმების შესაბამისობა ბიზნესის და დამკვეთების მოთხოვნებთან.

პრინციპები:

1. დაფორმირდეს დამკვეთების და მომხმარებლების სურვილების ერთობლიობა მწარმოებლურობის და ახალი ან შეცვლილი სერვისის გამოყენების შესახებ დანერგვის ეტაპზე;
2. ინფორმაციის და პროცესების მიწოდება რელიზის ინტეგრაციისთვის ბიზნესპროცესებში;
3. დამკვეთთა დაკმაყოფილების ამაღლების მიზნით უზრუნველყოფილ იქნეს სერვისის გამოყენება განსაზღვრული მოთხოვნებისა და შეზღუდვების შესაბამისად;
4. დამკვეთების, ინვესტორების და მომხმარებლების მიერ სერვისის გამოყენების მაქსიმიზაციის მიზნით, აუცილებელია მათი უზრუნველყოფა საჭირო ინფორმაციით და ცოდნით;
5. უზრუნველყოფილ იქნეს სერვისის გამოყენების მონიტორინგი და შეფასება (გაზომვა), რომლებსაც აპლიკაციები და ტექნიკური გადაწყვეტები უჭერს მხარს განთავსების პროცესში და ადრეულ სტადიებზე. ეს აუცილებელია სერვისის ხარისხის უზრუნველსაყოფად, სანამ დანერგვის პროცესი დასრულდება;
6. განხორციელდეს პრაქტიკულად მიღებული სერვისის მწარმოებლურობის შედარება დაგეგმილთან, სტრატეგიის აგების ეტაპზე. განხორციელდეს განსხვავების შესამცირებელი ღონისძიებები.

საუკეთესო პრაქტიკა:

- გამოყენებულ იქნეს საუკეთესო მმართველობითი პრაქტიკა რესურსების დაგეგმვისა და მართვის საქმეში, რომლებიც აუცილებელია სერვისის აწყობის, კომპლექტაციის, ტესტირების

და რელიზების განთავსების გასაუმჯობესებლად საწარმოო ექსპლუატაციაში, დადგენილი ხარჯების, დროისა და ხარისხის ფარგლებში;

- წარმოდგენილ იქნეს მკაფიო, გასაგები და სრულყოფილი გეგმები, რომლებიც უზრუნველყოფს ბიზნესისა და დამკვეთების ცვლილებათა პროექტების შესაბამისობას დანერგვის გეგმებთან;
- ინვესტორების ჩართულობის მართვა და მათთან კავშირი.

III ნაწილი
17 თავი. COBIT სტანდარტული მეთოდოლოგია

17.1. **COBIT**- ტექნოლოგია და ძირითადი ტერმინები

ინფორმაციული ტექნოლოგიების მენეჯმენტის საკითხებზე დღეისათვის არსებობს სტანდარტებისა და მეთოდოლოგიების გარკვეული სიმრავლე. მისი ერთ-ერთი წარმომადგენელია COBIT-ი (Control Objectives for Information and Related Technology – საკონტროლო ობიექტები საინფორმაციო და მასთან დაკავშირებული ტექნოლოგიებისთვის), რომელიც შეიქმნა ISACA (Information Systems Audit and Control Association – საინფორმაციო სისტემების აუდიტის და კონტროლის ასოციაცია) ორგანიზაციის მიერ ამერიკის შეერთებულ შტატებში 1969 წელს, საფინანსო აუდიტებისთვის ინფორმაციული ტექნოლოგიების კონტროლის მიზნით. ამჟამად ამ ორგანიზაციას აქვს მსოფლიოში ერთ-ერთი ლიდერის როლი ინფორმაციული ტექნოლოგიების აუდიტის სტანდარტების შემუშავების სფეროში [44,45].

COBIT არის ღია დოკუმენტების ერთობლიობა, 40-მდე საერთაშორისო სტანდარტი და სახელმძღვანელო IT მართვის, აუდიტის და ინფორმაციული უსაფრთხოების სფეროებში. ესაა ავტორიტეტული, თანამედროვე, საერთაშორისო დონეზე აღიარებული მეთოდოლოგიის კვლევა, დამუშავება, პუბლიკაცია კორპორაციული მენეჯმენტისათვის IT სფეროში. მისი დანიშნულებაა ორგანიზაციებში ამ სტანდარტების დანერგვა და ყოველდღიური გამოყენება IT სფეროს ბიზნეს-მენეჯერების და აუდიტორების მიერ [4, 46].

COBIT-ის ძირითადი მიზანია ინფორმაციული ტექნოლოგიების მენეჯმენტი. ამავე დროს, ინფორმაციული ტექნოლოგიების მენეჯმენტი, თავის მხრივ, არის კორპორაციული მენეჯმენტის განუყოფელი ნაწილი. კორპორაციული მენეჯმენტი მმართველობითი გადაწყვეტილების და მეთოდების კომპლექსია, რომელიც გამოიყენება უმაღლესი ხელმძღვანელობის მიერ შემდეგი მიზნებისთვის:

- სტრატეგიული მიმართულების განსაზღვრისთვის;
- მიზნების მიღწევის უზრუნველსაყოფად;
- რისკების ადეკვატურად სამართავად;
- კორპორაციული რესურსების ეფექტურად გამოსაყენებლად.

კორპორაციული მენეჯმენტი და IT მენეჯმენტი მოითხოვს მიზნებს შორის ბალანსს, რაც დაკავშირებულია ზემდგომი ხელმძღვანელობის მიერ დადგენილი მოთხოვნილებების შესაბამისობის აუცილებლობისა და ეფექტიანობის ამაღლებასთან.

COBIT-ში გამოიყენება ტერმინი „დაინტერესებული მხარეები“ (Stakeholders), რომლებსაც მიეკუთვნება:

- დირექტორთა საბჭო და უმაღლესი ხელმძღვანელობა: IT-ის განვითარების მიმართულების განსაზღვრა, შედეგების შეფასება და ნაკლოვანებათა აღმოფხვრის მოთხოვნების დადგენა;
- ბიზნესგანყოფილებების ხელმძღვანელები: ბიზნეს-მოთხოვნების განსაზღვრა IT-ის მიმართ, სარგებლიანობის მიღწევის უზრუნველყოფა IT-დან და რისკების მართვა;
- IT სამსახურის ხელმძღვანელობა: IT სერვისებით უზრუნ-ველყოფა და მათი სრულყოფა ბიზნესის მოთხოვნილებათა შესაბამისად;
- შიგა აუდიტი / შიგა კონტროლის სამსახური / IT აუდიტი: დამოუკიდებელი შეფასების უზრუნველყოფა, რომ IT იძლევა საჭირო სერვისებს;

- რისკების მართვა და შესაბამისობის დაცვა: ნორმატიულ დოკუმენტებთან შესაბამისობის შეფასება რისკების გათვალისწინებით.

17.2. COBIT-ის მიზნები და პრინციპები

COBIT-ის საკვანძო ცნებაა სერვისი ან მომსახურება (service). მაგალითად, ინტერნეტში წვდომის ან დაცულ მონაცემთა საცავთან მიმართვის უზრუნველყოფა მიეკუთვნება მომსახურების სახეებს. ჩვენ სერვისის განსაზღვრა შემოვიღეთ ITIL მეთოდოლოგიის განხილვისას, რომელიც ასევე სერვისის მენეჯმენტს ეხება. სერვისი არის გარკვეული ფასეულობის მიწოდების ხერხი დამკვეთისთვის, რომელიც მას ხელს უწყობს სასურველი შედეგების მისაღებად თავისი სისტემის გამოსასვლელზე, ყოველგვარი სპეციფიკური ხარჯების და რისკების გარეშე. სერვისის მიწოდება რთული და არატრივიალური ამოცანაა, რომელიც პირველ რიგში მოითხოვს შიგა კონტროლის სისტემას.

COBIT-ის ძირითადი პრინციპები:

- IT მიზნები უნდა შეესაბამებოდეს ბიზნესის მიზნებს;
- პროცესული მიდგომის გამოყენება;
- IT კონტროლის სისტემა უნდა იყოს შერჩევითი ანუ განსაზღვროს IT-ს ძირითადი რესურსები და იმუშაოს მასთან;
- კონტროლის მიზნები უნდა იყოს მკაფიოდ განსაზღვრული.

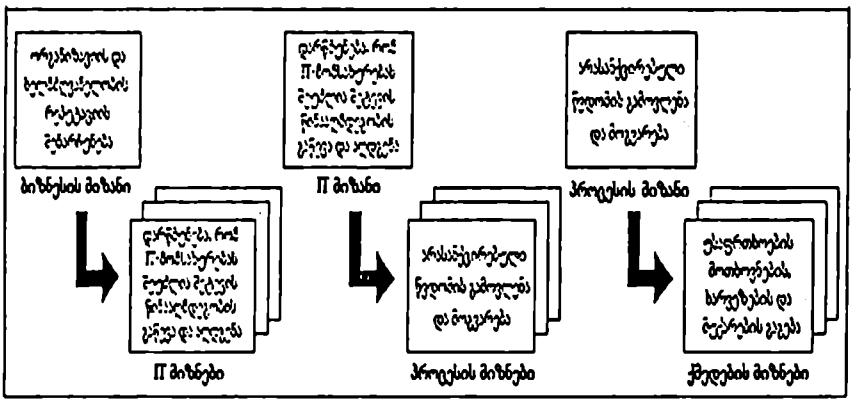
სერვისების მართვის თანამედროვე მიდგომა ყურადღებას ამახვილებს ბიზნესის და IT-ს ურთიერთდამოკიდებულებაზე.

მიზნები განსაზღვრულია დაღმავალად (top-down ზემოდან-ქვევით) ისე, რომ ბიზნეს-მიზანმა უნდა განსაზღვროს IT მიზნები თავის მხარდასაჭერად. IT მიზანი მიიღწევა ერთი პროცესის ან

რამდენიმე პროცესის ურთიერთმოქმედებით. ამრიგად, IT-ის მიზანია განსაზღვროს განსხვავებული პროცესების მიზნები.

თავის მხრივ, თითოეული პროცესის მიზანი მოითხოვს აქტიურობათა (ქმედებათა) გარკვეულ რაოდენობას, ასევე მათი მიზნების დადგენას.

17.1 ნახაზზე მოცემულია ბიზნესის, IT-ს, პროცესების და ქმედებათა მიზნების დამოკიდებულების მაგალითები.



ნახ.17.1

განვიხილოთ დეტალურად COBIT-ის ძირითადი პრინციპები:

1. ბიზნესის და IT-ს მიზნები უნდა იყოს ურთიერთდაკავშირებული, მაგრამ განმსაზღვრელი ამ ურთიერთობაში არის ბიზნესის მიზნები. კომპანიის მოგება პირდაპირ დამოკიდებულებაშია IT-ს ეფექტურ გამოყენებასთან. ამიტომ ხელმძღვანელობამ მეტი ყურადღება უნდა გაამახვილოს მის სარგებლიანობაზე, ინვესტირებაზე, შედეგების მონიტორინგსა და შეფასებაზე;

2. პროცესული მიდგომის გამოყენება. პროცესი არის საქმიანობათა სახეების სტრუქტურირებული ერთობლიობა, რომელიც დაპროექტებულია განსაზღვრული მიზნის მისაღწევად. ანუ პროცესი, ზოგადად, პროცედურების ერთობლიობაა, რომელზეც გავლენას ახდენს ორგანიზაციის პოლიტიკა და სხვა წყაროების პროცესები. ბიზნესი განაპირობებს პროცესის წარმოქმნის მიზეზს, მის პასუხისმგებელ მფლობელს, თანამდებობრივ მოვალეობებს, რომლებიც დაკავშირებულია პროცესის შევსების, შესრულების და ეფექტიანობის გაზომვის საშუალებებთან.

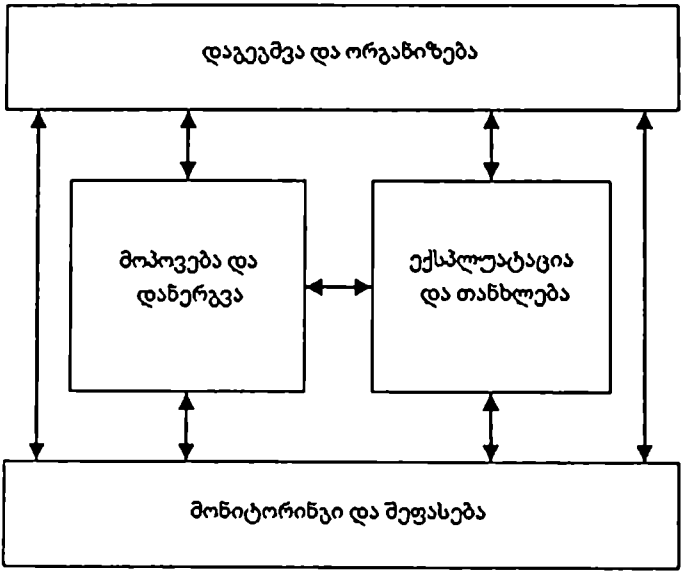
17.3. COBIT-ის პროცესები

პროცესს აქვს შემდეგი მახასიათებლები:

- პროცესები გაზომვადია, ანუ ისინი შეიძლება შეფასდეს რომელიმე შესაბამისი მეთოდით. მაგალითად, მენეჯერები იყენებენ პროცესების ღირებულებას და ხარისხს, მომხმარებლები კი - პროცესების ხანგრძლივობას და პროდუქტიულობას;
- პროცესი ემსახურება კონკრეტული შედეგების მიღწევას. პროცესის არსებობის მიზეზი არის კონკრეტული შედეგის მიღება, რომელიც შეიძლება იდენტიფიცირდეს (გამოვლინდეს) და რაოდენობრივად შეფასდეს (დათვლილ იქნეს);
- პროცესს ჰყავს მომხმარებლები. ყოველი პროცესი თავის შედეგებს აწვდის მომხმარებლებს ან სხვა პროცესებს, ორგანიზაციის შიგნით ან გარეთ;
- პროცესი შედგება ქმედებებისგან. ქმედება (Activity) არის საქმიანობის ძირითადი სახეები პროცესის ფარგლებში.

COBIT განიხილავს 34 IT-პროცესს, რომლებიც გაერთიანებულია 4 დომენში (Domain – საკონტროლო მიზნების დაჯგუფება ლოგიკურ ეტაპებში IT-ინვესტიციის სასიცოცხლო

ციკლის შიგნით). 17.2 ნახაზზე მოცემულია დომენების ურთიერთკავშირის სქემა.



ნახ.17.2. დომენების ურთიერთკავშირი

• დაგეგმვა და ორგანიზება (PO – Plan and Organise): განსაზღვრავს მიმართულებებს გადაწყვეტილებათა დანერგვის (AI) და სერვისების მიწოდების (DS – Delivery Services) თვალსაზრისით;

• მოპოვება და დანერგვა (AI – Acquire and Implement): უზრუნველყოფს გადაწყვეტილებათა დანერგვას და სერვისებს მათ საფუძველზე;

• ექსპლუატაცია და თანხლება (DS – Deliver and Support). უზრუნველყოფს გადაწყვეტილებათა შესრულებას და საბოლოო მომხმარებლებისთვის მათი გამოყენების მხარდაჭერას;

• მონიტორინგი და შეფასება (ME – Monitor and Evaluate). ახორციელებს პროცესის მონიტორინგს (კონტროლს) და შეფასებას.

პროცესების ასეთი სტრუქტურა იძლევა სფეროების სისტემატიზაციის და ინფორმაციის ორგანიზების უზრუნველყოფის საშუალებას, რომლებიც აუცილებელია მათი ბიზნესმიზნების მისაღწევად.

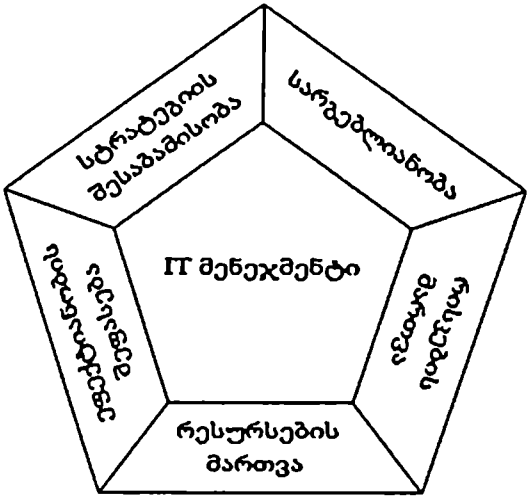
3. რესურსების რანჟირების პრინციპი. არაა აუცილებელი ყველა რესურსის თვალყური, მხოლოდ იმათზე უნდა გამახვილდეს ყურადღება, რომლებიც გავლენას ახდენს ბიზნესპროცესებზე და მათ შედეგებზე.

4. მიზნების განსაზღვრა – ერთ-ერთი ყველაზე რთული და მნიშვნელოვანი ამოცანაა. გლობალური გაგებით ხელმძღვანელობა და მენეჯერები ორ მიზანს ითვალისწინებენ – დასახული ბიზნეს-მიზნების მიღწევას და არასასურველი მოვლენების თავიდან აცილებას (ან მათი შედეგების გამოსწორებას).

მაგალითად, სარეზერვო კოპირების ამოცანას არ მოაქვს პირდაპირი მოგება ბიზნესისთვის, მაგრამ სისტემის მწყობრიდან გამოსვლის შემთხვევაში მისი საშუალებით შესაძლებელია ინფორმაციის სწრაფი აღდგენა, რაც მეტად მნიშვნელოვანია ბიზნესის ნორმალური ფუნქციონირებისთვის.

ასევე მნიშვნელოვანია საკითხები ხელმძღვანელობისთვის, მაგალითად, სადაა საჭირო პროცესების სრულყოფა, რამდენი ინვესტიციაა საჭირო და როგორ გაიზომოს შედეგი. COBIT-ი იძლევა მეთოდლოგიას IT ხელმძღვანელობისთვის დასახულ საკითხებზე.

COBIT-ი გამოყოფს IT მენეჯმენტის შემდეგ საკვანძო სფეროებს (ნახ.17.3):



ნახ.17.3. IT-მენეჯმენტის საკვანძო სფეროები

• სტრატეგიის შესაბამისობა. უზრუნველყოფს ბიზნესის და IT-ის თავსებადობას ერთმანეთთან;

• სარგებლიანობა პასუხს აგებს: იმის რეალიზაციაზე, რასაც შეუძლია ბიზნესისთვის ფასეულობის მოტანა; კონტროლზე, რათა IT-მ უზრუნველყოს სტრატეგიით განსაზღვრული უპირატესობები; ხარჯების ოპტიმიზაციასა და ჭეშმარიტი ღირებულების დადასტურებაზე;

• რესურსების მართვა პასუხისმგებელია კრიტიკული IT-რესურსების მენეჯმენტზე, ინვესტიციების ოპტიმიზაციასა და აპლიკაციების, ინფორმაციის, ინფრასტრუქტურის და პერსონალის სათანადო ხელმძღვანელობაზე;

• რისკების მართვა მოითხოვს ზემდგომი ხელმძღვანელობის ინფორმირებას რისკების სფეროში; კორპორაციული მიდგომის ნათლად წარმოდგენას მათთან მიმართებაში; გამჭვირვალობის

მოთხოვნების შესაბამისობას არსებულ რისკებთან დამოკიდებულებაში; ორგანიზაციის პრაქტიკაში რისკების მართვის ფუნქციების დანერგვას;

ეფექტიანობის შეფასება პასუხს აგებს სტრატეგიის, გეგმების, რესურსების გამოყენების და პროცესების ეფექტიანობის რეალიზაციის კონტროლზე;

ლიტარატურა:

1. სურგულაძე გ., ბულია ი., კორპორაციულ Web-აპლიკაციათა ინტეგრაცია და დაპროექტება. თბ.: სტუ, 2012.

2. Surguladze G., Turkia E., Topuria N., Lominadze T., Giutashvili M. Towards an Integration of Process-Modeling: from Business Method: from Business-Content to the Software Implementation. IV Intern. Conf. Problems of cybernetics and informatics (PCI' 2012). Baku, Azerbaijan, 2012.

3. ITIL moving towards Enterprise Architecture. http://blogs.msdn.com/b/mikewalker/archive/2007/07/06/itil-moving-towards-enterprise-architecture.aspx?Redirected=true.

4. COBIT: Framework for IT Governance and Control. http://www.isaca.org/knowledge-center/cobit/Pages/Overview.aspx.

5. Booch G., Jacobson I., Rumbaugh J. Unified Modeling Language for Object-Oriented Development. Rational Software Corporation, Santa Clara, 2006.

6. Бек К. Шаблоны реализации корпоративных приложений. Экстремальное программирование: Пер. с англ. М.: Вильямс, 2008.

7. Амблер С. Гибкие технологии: экстремальное программирование и унифицированный процесс разработки. Пер. с англ. С-Петербург: Питер. 2005.

8. Best Management Practice Portfolio. Office of Government Commerce (OGC). https://www.gov.uk/government/publications/best-management-practice-portfolio.

9. სურგულაძე გ., გულიტაშვილი მ., კაკულია ი., ჩერქეზიშვილი გ., ჯავახიშვილი ი. პროგრამული სისტემების სასიცოცხლო ციკლის პროცესის მოდელირება უნივერსალური და ექსტრემალური პროგრამირების პრინციპების კომპრომისული გადაწყვეტით. სტუ-ის შრ.კრ. "მას" N1(8). თბ., გვ. 63-70.

10. ურუშაძე ბ. პროგრამულ აპლიკაციათა ინტეგრაცია Agile და ITIL მეთოდოლოგიების საფუძველზე. სტუ-ის შრ.კრ. "მას" N3(16), თბ., 2013. გვ. 101-106.

11. ITILv3. Глоссарий терминов и определений. ITIL® V3 Glossary Russian Translation. v0.92, 30 Apr 2009.

12. The official introduction to the ITIL Service Lifecycle 2007.

13. ИТ сервис-менеджмент: введение "IT-Expert", 2003.

14. ISO – 8402 "Quality management and quality assurance – Vocabulary". 1994.

15. Полезность и гарантия: глупость или гениальная идея ? www.itexpert.ru/rus/biblio/articles/200406222006/01/. გად. 11.01.14.

16. Service Strategy. TSO (The Stationery Office) 2007; Published for the Office of Government Commerce (OGC)

17. http://www.itexpert.ru/rus /ITEMS/ 77-16-1/. გად. 11.01.14.

18. Service Strategy – Стратегия сервиса. http://www.dwh-club.ru/node/77. გადამოწ. 11.01.14.

19 Service Design. TSO (The Stationery Office) 2007; Published for the Office of Government Commerce (OGC).

20. რაზუმოვსკი კ. შესავალი პროგრამული უზრუნველყოფის მოქნილ დამუშავებაში. http://www.kv.by/index2008334201.htm. გადამოწმ. 10.01.14.

21. Agile and ITIL are complementary partners. http://www .information-age.com/it-management/skills-training-and-leadership/1149 583/agile-and-itil-are-complementary-partners. გადამოწმ. 10.01.14.

22. Maurer and S. Martel. Extreme Programming: Rapid Development for Web-Based Applications. IEEE Internet Computing, 6(1), January/February, 2002, pp 86-91.

23. Cockburn A. Using Both Incremental and Iterative Development. *STSC CrossTalk* (USAF Software Technology Support Center) 21 (5): 27–30.ISSN 2160-1593. Retrieved 2011-07-20. May 2008.

24. Защита_персональных_данных. http://wiki.rsu.edu.ru/wiki/. გადამოწ. 11.01.14.

25. Service Transition. TSO (The Stationery Office) 2007; Published for the Office of Government Commerce (OGC).

26. Service Operation. TSO (The Stationery Office) 2007; Published for the Office of Government Commerce (OGC).

27. Continual Service Improvement. TSO (The Stationery Office) 2007; Published for the Office of Government Commerce (OGC).

28. სურგულაძე გ., გულუა დ., ურუშაძე ბ., კაშიბაძე მ. ორგანიზაციის საინფორმაციო ინფრასტრუქტურის ავტომატიზების თანამედროვე მეთოდები. სტუ-ის შრ.კრ. „მას"-N 1(14). 2013. გვ.109–114.

29. BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS). Bundesamt für Sicherheit in der Informationstechnik, (BSI) Godesberger Allee 185-189, 53175 Bonn, 2008/2013.

30. BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise. (BSI) Godesberger Allee 185-189, 53175 Bonn, 2008/2013.

31. BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz. Bundesamt für Sicherheit in der Informationstechnik, Bonn. 2011.

32. BSI-Standard 100-4: Notfallmanagement Version 1.0 Inhaltverzeichnis. Bundesamt für Sicherheit in der Informationstechnik, (BSI) Godesberger Allee 185-189, 53175 Bonn, 2008/2013.

33. https://www.bsi.bund.de/DE/Home/home_node.html. Bundesamt für Sicherheit in der Informationstechnik, Bonn. 2013.

34. http://en.wikipedia.org/wiki/BSI_Group. გადამოწ. 15.01.14.

35. Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz - Prüfschema für ISO 27001-Audits, BSI, Version 1.2, März 2008, www.bsi.bund.de/gshb/zert. გადამოწ.10.01.14.

36. Zertifizierungsschema für Auditteamleiter für ISO 27001-Audits auf der Basis von IT-Grundschutz, BSI, März 2008, www.bsi.bund.de/gshb/zert. გადამოწ.10.01.14.

37. Goodchild J. Social Engineering: The Basics. http://www.csoonline.com/article/2124681/security-awareness/social-engineering-the-basics.html. გადამოწ.10.01.14.

38. Скрипник Д. ITIL : IT Service Management по стандартам V.3.1. http://www.intuit.ru/studies/courses/2323/623/info. გად.10.01.14

39. Information Systems Examinations Board (ISEB). http://www.bcs.org/. გადამოწ.10.01.14.

40. Foundation Certificate in IT Service Management. https:// www.exin.com/NL/en/exams/?exam=itil-v3-foundation. გად.10.01.14

41. Distributed Management Task Force. http://www.dmtf.org/

42. Скрипник Д. Управление ИТ на основе COBIT 4.1. http://www.intuit.ru/studies/courses/3704/946/info. გადამოწ.15.01.14.

43. http://www.best-management-practice.com/gempdf/Service_ Transition_Contents.pdf. გადამოწ.15.01.14.

44. COBIT Overview ISACA. http://www.isaca.org/knowledge-center/cobit/Pages/Overview.aspx. გადამოწ.15.01.14.

45. COBIT 5 for Information Security. http://www.isaca.org/COBIT/Documents/COBIT-5-for-Information-Security-Introduction.pdf.

46. Скрипник Д. Управление ИТ на основе COBIT 4.1. М., 2012. www.intuit.ru/studies/courses/3704/946/info. გადამოწ.15.01.14.

რედაქტორი ნ. ქაფიანიძე

გადაეცა წარმოებას 17.06.2014. ხელმოწერილია დასაბეჭდად 18.07.2014. ქაღალდის ზომა 60X84 1/16. პირობითი ნაბეჭდი თაბახი 19,5. ტირაჟი 100 ეგზ.

საგამომცემლო სახლი „ტექნიკური უნივერსიტეტი“, თბილისი, კოსტავას 77

