საქართველოს ტექნიკური უნივერსიტეტი

ინფორმაციის ტექნოლოგიის (IT) მართვის პოლიტიკა და პროცედურები

ვერსია 1.1

დამტკიცების/განახლების თარიღი: 2018 წლის 18 მარტი

2018 წელი

შესავალი

ინფორმაციის ტექნოლოგიის მართვის პოლიტიკის რეგულირების სფერო ვრცელდება საქართველოს ტექნიკური უნივერსიტეტის სტუდენტებზე, აკადემიურ პერსონალზე, მოწვეულ პროფესორ-მასწავლებლებზე, ადმინისტრაციის თანამშრომლებსა და ყველა პირზე, რომელსაც შეიძლება მიეცეს დაშვება უნივერსიტეტში არსებულ ინფორმაციულ რესურსებთან. იგი განსაზღვრავს უნივერსიტეტში დანერგილი ინფორმაციის ტექნოლოგიების, ქსელური სერვისების და სისტემების მოხმარების წესს.

უნივერსიტეტს წარმატებული სასწავლო და ბიზნესგარემოს შესაქმნელად სჭირდება:

- მხარდამჭერი ელექტრონული სერვისების და ციფრული მომსახურებების დანერგვა და განვითარება.
- ინფორმაციის ტექნოლოგიის სამართავად ეფექტური ინფორმაციული უსაფრთხოებისა და კონფიდენციალურობის პოლიტიკა, რომელიც უზრუნველყოფს კიბერთავდასხმებისგან დაცვას.

უნივერსიტეტის ინფორმაციული უსაფრთხოების პოლიტიკა ეფუძნება ინფორმაციული უსაფრთხოების საერთაშორისო სტანდარტს ISO 27002.

მართვის პოლიტიკის მიზანი

1. ინფორმაციის ტექნოლოგიის მართვის პოლიტიკის მიზანია უნივერსიტეტმა უზრუნველყოს ერთიანი პრინციპით მოქმედი, უსაფრთხო და ეფექტიანი ელექტრონული სერვისების ხელმისაწვდომობა სასწავლო, სამეცნიერო და ადმინისტრაციულ-დამხმარე სექტორისათვის, სათანადო ინფრასტრუქტურის გამოყენებით.
2. პოლიტიკა მიზნად ისახავს შიდა და გარე საფრთხეების მიმართ ინფორმაციული უსაფრთხოების დამცავი მექანიზმების, კრიზისული სიტუაციებისა და განზრახ დაზიანებების წინააღმდეგ ქცევის ძირითადი წესების შექმნასა და მისი მეშვეობით კონფიდენციალურობის, მთლიანობისა და ხელმისაწვდომობის უზრუნველყოფას.

1. ინფორმაციის ტექნოლოგიის ინფრასტრუქტურა

სტუ-ს კომპიუტერული ქსელი და მასში რეალიზებული ერთიანი ინფორმაციული სივრცე, ერთ-ერთ ყველაზე მაშტაბურია საქართველოში და იგი აერთიანებს სასწავლო კორპუსს და უნივერსიტეტის შემადგენლობაში არსებულ სამეცნიერო-კვლევით ინსტიტუტებს.

სტუ-ში დანერგილია სხვადასხვა ტიპის ინფორმაციის ტექნოლოგია სწავლების და მართვის უზრუნველყოფის მიზნით. ეს ტექნოლოგიები მოიცავს ინტერნეტ და ინტრანეტ სერვისებს.

სტუ – ს გააჩნია კომპიუტერული ქსელის შემდეგი ტიპის ფიზიკური ინფრასტრუქტურა: სერვერული, კაბელური და უკაბელო, ღრუბლოვანი ინფრასტრუქტურა, IP ტელეფონია, უსაფრთხოების, ინციდენტების აღმოჩენის და რეაგირების ტექნოლოგიები და მონიტორინგის სისტემები.

ინფრასტრუქტურა გამოყენებულია სხვადასხვა ტიპის საუნივერსიტეტო და ინტერნეტ კავშირის უზრუნველყოფის მიზნით, როგორიცაა: ვებგვერდი, ელექტრონული ფოსტა, ელექტრონული სწავლების სისტემა, ელექტრონული ტესტირების სისტემა, დოკუმენტ ბრუნვის და სხვა სერვისები.

1.1 კაბელური და უკაბელო კომპიუტერული ქსელური ინფრასტრუქტურა და მისი მართვის პოლიტიკა

აღწერა

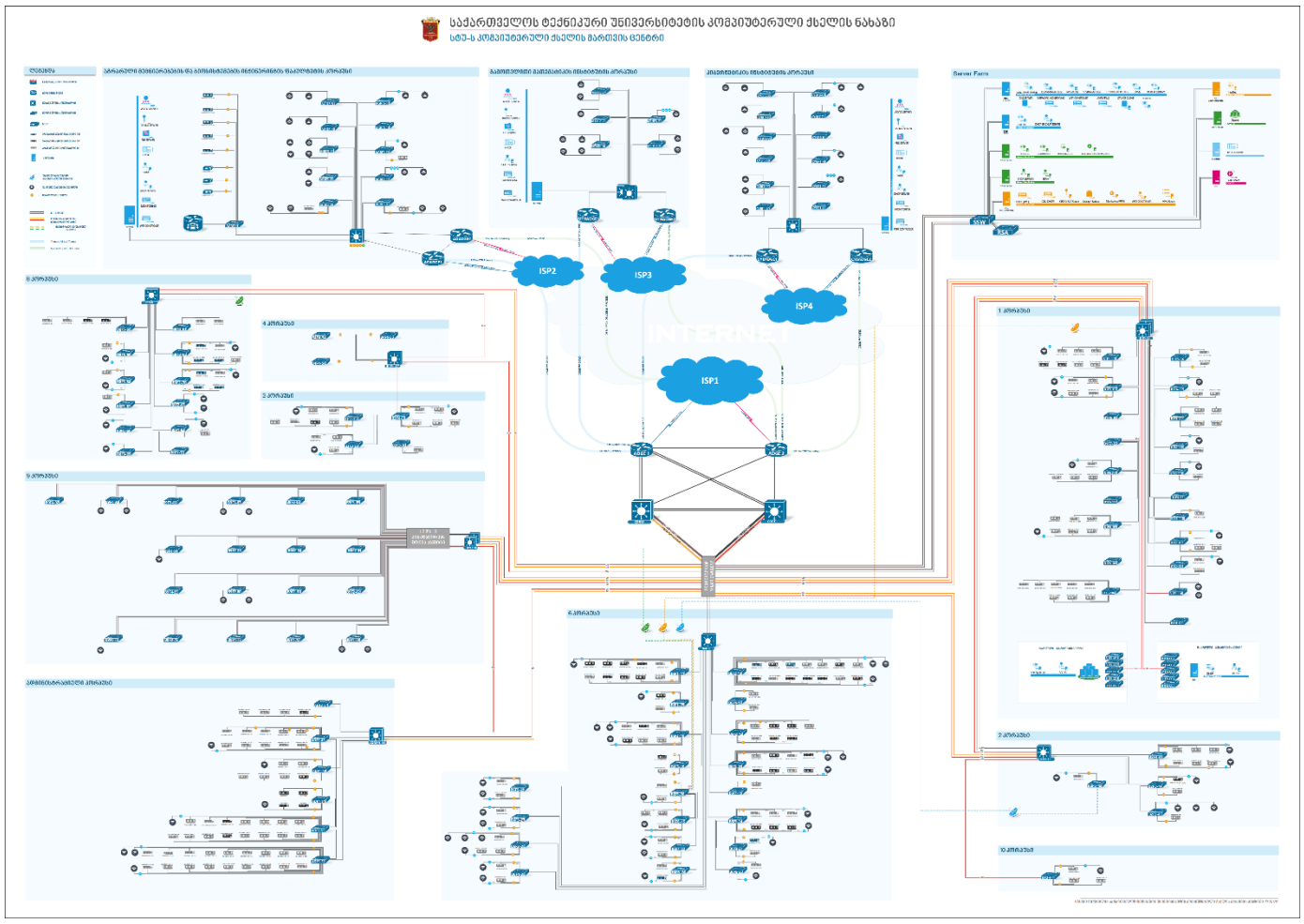
სტუ-ს ერთიანი კომპიუტერული ქსელი არის მნიშვნელოვანი ინფორმაციული რესურსი, რომელიც გამოიყენება აკადემიური, სამეცნიერო და ადმინისტრაციული-დამხმარე მიზნებით. კომპიუტერული ქსელი აერთიანებს ინტრანეტ და ინტერნეტ სერვისებს.

ქსელური ინფრასტრუქტურა

ერთიანი კომპიუტერული ქსელი, რომელშიც ჩართულია 4000-ზე მეტი ქსელური კვანძი და ფარავს უნივერსიტეტის თითქმის მთელ სივრცეს (ყველა სასწავლო და ადმინისტრაციულ

კორპუსს), სხვადასხვა ლოკაციაზე: კოსტავას ქ. № 77, გურამიშვილის გამზ. №17, სანდრო ეულის ქ.№16, გ. ფერაძის ქ. №4 და სხვა.

სტუ-ს ყველა კორპუსი დაკავშირებულია ოპტიკურ-ბოჭკოვანი მაგისტრალებით.



ნახ.1 სტუ-ს კომპიუტერული ქსელის სტრუქტურული სქემა.

უნივერსიტეტს აქვს საკუთარი BGP-ს ავტონომიური სისტემის ნომერი (AS29289) და IP მისამართები (109.205.36.0/23).

უნივერსიტეტში ჩართულ ყველა ქსელურ წერტილს მიეწოდება მინ 100მბ/წმ სიჩქარის ინტერნეტი.

მართვა

სტუ-ს კომპიუტერულ ქსელს მართავს სტუ-ს ქსელის მართვის ცენტრი, რომელიც პასუხისმგებელია უნივერსიტეტის სასწავლო, ადმინისტრაციულ კორპუსებში და კვლევით ინსტიტუტებში როგორც კაბელურ ისე უკაბელო ქსელური ინფრასტრუქტურის პროექტირებაზე, საინსტალაციო სამუშაოების მონიტორინგზე და მართვაზე.

1.2 კომპიუტერული ქსელის მართვის პოლიტიკა

ტექნიკური უნივერსიტეტის შიდა ქსელში ჩართული მოწყობილობები ექვემდებარება ერთიან უსაფრთხოების პოლიტიკას. ეს პოლიტიკა უზრუნველყოფს ტექნიკური უნივერსიტეტის ქსელში არასანქცირებული წვდომის შეზღუდვას, რესურსების ოპტიმალურ გამოყენებას, მომხმარებელთა კომპიუტერების დაინფიცირების თავიდან აცილებას ეფექტური ანტივირუსული მექანიზმის გატარებით, არასასურველი ტრაფიკის გენერირების და სისტემაზე არასასურველი გავლენის თავიდან აცილებას.

საქართველოს ტექნიკური უნივერსიტეტის კომპიუტერული ქსელის მართვის ცენტრი (კქმც) უზრუნველყოფს რისკების და ინფორმაციის სენსიტურობის და უსაფრთხოების შეფასებას. განსაზღვრავს კომპიუტერის ქსელთან მიერთების და დამისამართების წესს.

1.3 სტუ-ს უკაბელო ქსელის ინფრასტრუქტურა და მართვის პოლიტიკა

აღწერა

სტუ-ს ყველა სასწავლო კორპუსი, ადმინისტრაციული კორპუსი და კვლევითი ინსტიტუტების კორპუსები დაფარულია უსადენო კორპორატიული ქსელური ინფრასტრუქტურით.

უსადენო ქსელური ინფრასტრუქტურა (Wi-FI). სტუ-ს მთელ პერიმეტრზე რეალიზებულია ერთიანი ცენტრალიზებული უსადენო ქსელი. უსადენო წვდომისთვის, უნივერსიტეტის კომპუსების შიდა და გარე დაფარვის ზონებისთვის, გამოყენებულია უსადენო წვდომის წერტილები. ყველა უსადენო წვდომის წერტილის მართვა და მონიტორინგი ხდება ცენტრალიზებულად, შესაბამისი კონტროლერით. უსადენო ქსელით დაფარულია საუნივერსიტეტო კორპუსების დიდი ნაწილი.

ფიზიკური ინფრასტრუქტურა

ერთიანი უკაბელო კომპიუტერული ქსელი, რომელშიც ჩართულია 160-ზე მეტი უკაბელო ქსელური წვდომის წერტილი, ფარავს უნივერსიტეტში შემავალი შენობების დერეფნებს, ბიბლიოთეკას, ეზოეს და 30%-ზე მეტ სასწავლო და ადმინისტრაციულ ოთახებს.

განმარტებები

გლობალური (Public) IP მისამართები: გლობალურად ინტერნეტში მარშრუტიზირებადი IP მისამართები, რომლებიც მინიჭებულია ინტერნეტ მისამართების ნუმერაციის ორგანოს (IANA) მიერ. სტუ-სთვის გამოყოფილი რეგისტრირებული 512 IP მისამართებია:

109.205.46.0 მასკა 255.255.253.0

ლოკალური (Private) IP მისამართები: საწარმო და შიდა ქსელებისთვის IANA -ს გამოყოფილი აქვს IP მისამართები, რომლებიც გამოიყენება შიდა დამისამართებისთვის და არ არის მარშუტიზირებადი ინტერნეტში (მოხსენიებულია RFC1918 დოკუმენტში). აღნიშნული IP მისამართებია:

10.0.0.0 - 10.255.255.255
172.16.0.0 - 172.31.255.255
192.168.0.0 - 192.168.255.255

1.4. IP მისამართების მართვის პოლიტიკა

- სტუ-ს კომპიუტერული ქსელის მართვის ცენტრი განკარგავს ლოკალურ დამისამართებას, გამოყოფს და ანიჭებს IP მისამართებს.
- სისტემებს (სერვერებს), რომელთაც ჭირდებათ ინტერნეტთან პირდაპირი წვდომა და თუ აღნიშნული კავშირი კრიტიკულია სისტემისთვის, მათ სტუ-ს ქსელის მართვის ცენტრისგან გამოეყოფათ გლობალური IPv4 მისამართი.
- „ცენტრი“ იტოვებს უფლებას დაბლოკოს გლობალური მისამართი, თუ ამ მისამართით გაშვებული სერვისი საფრთხეს უქმნის უნივერსიტეტში ან მის გარეთ არსებულ ინფრასტრუქტურას.

- საჭიროების შემთხვევაში, რომელიმე კონკრეტული მოწყობილობისთვის, შესაძლებელია ლოკალური IP მისამართების რეზერვირება.
- დაუშვებელია ქმც-თან შეთანხმების გარეშე IP მისამართების თვითნებურად გაწერა.

1.5 საქართველოს ტექნიკური უნივერსიტეტში არსებული კომპიუტერული და ქსელური მოწყობილობების დასახელების წესი

B 06 D 306 WL 001

I სიმბოლო - სახელი იწყება ლათინური ასოთი და აღნიშნავს კორპუსს. მაგალითად: B

II –III სიმბოლო აღნიშნავს კორპუსის ნომერს. მაგალითად: 06

IV სიმბოლო აღნიშნავს სექტორის იდენტიფიკატორს. მაგალითად: D

V-VII სიმბოლო აღნიშნავს ოთახის ნომერს მაგალითად: 306

VIII-IX სიმბოლო აღნიშნავს თუ ვის ეკუთვნის მოწყობილობა. მაგალითად: WL

RO - მარშრუტიზატორი;

SW - კომუტატორი;

SV - სერვერი;

WA - მანქანა ადმ. პერსონალის;

WL - მანქანა ლაბორატორიის;

X-XII სამ ნიშნიანი ნომერი, ოთახში მანქანის უნიკალური ნომერი, რომლის ათვლაც ხდება საათის ისრის მიმართულებით.

ზემოთ მოყვანილი მაგალითი - **B06D306WL001**

ნიშნავს ლაბორატორიის კომპიუტერს, რომელიც მდებარეობს მეექვსე სასწავლო კორპუსის 306დ ოთახში.

1.6 საუნივერსიტეტო ქსელში საბოლოო მოწყობილობის ჩართვის წესი

კომპიუტერის საუნივერსიტეტო ქსელში ჩართვისას აუცილებელია:

- სტუ-ის კომპიუტერულ ქსელში ჩართვა ხორციელდება რექტორის, ადმინისტრაციის ხელმძღვანელის ან უნივერსიტეტის მიერ დანიშნული უფლებამოსილი პირის განკარგულების საფუძველზე.
- განაცხადში უნდა იყოს მოცემული კომპიუტერის განთავსების და მისი კუთვნილების შესახებ სრული ინფორმაცია.
- უნდა იყოს ცნობილი კომპიუტერზე დაკისრებული ამოცანა.
- კომპიუტერის ფიზიკური ადგილმდებარეობის და კუთვნილების მიხედვით იგი ერთვება ფაკულტეტისთვის ან ადმინისტრაციისთვის გამოყოფილ ვირტუალურ და ფიზიკურ სივრცეში.
- სტუდენტთათვის განკუთვნილი კომპიუტერული კლასები ერთვება მათთვის ცალკე გამოყოფილ ვირტუალურ სივრცეში.
- კომპიუტერის მიერთება ხდება მისი ადგილმდებარეობის მიხედვით, შესაბამისი უახლოესი საკომუნიკაციო კვანძის მართვად მოწყობილობასთან.
- კომპიუტერის საუნივერსიტეტო ქსელთან მიერთების მომენტში ცნობილი უნდა იყოს მასზე განთავსებული ოპერაციული სისტემა, მისი ტექნიკური მახასიათებლები და მასზე ჩაწერილი პროგრამული უზრუნველყოფა.
- მასზე უნდა გამოიყოს ინდივიდუალური IP მისამართი საუნივერსიტეტო ქსელის მართვის ცენტრის მხრიდან.
- მომხმარებელს არა აქვს უფლება თვითნებურად შეცვალოს მისთვის გამოყოფილი IP მისამართი.
- კომპიუტერზე მისი ტექნიკური მონაცემების გათვალისწინებით უნდა იყოს დაინსტალირებული უნივერსიტეტის მიერ შეძენილი ანტივირუსული პროგრამული უზრუნველყოფა.
- მომხმარებელს არა აქვს უფლება თვითნებურად წაშალოს ანტივირუსული პაკეტი კომპიუტერიდან.
- პრინტერის ინსტალაციის დროს უნდა განისაზღვროს მისი განთავსების ადგილი და რომელ ჯგუფს ემსახურება იგი.
- უნივერსიტეტის შიდა რესურსებზე წვდომა გარე ქსელიდან ხორციელდება კომპიუტერული ქსელის მართვის ცენტრის უფროსის გადაწყვეტილების საფუძველზე.
- ცენტრალური და პერიფერიული კვანძები თავსდება სატელეკომუნიკაციო ოთახებში შესაბამისი ტემპერატურული რეჟიმით ან საკომუნიკაციო კარადებში ფიზიკური უსაფრთხოების უზრუნველყოფის მიზნით
- ცენტრალურ და პერიფერიულ საკომუნიკაციო კვანძებთან წვდომა პრობლემების აღმოფხვრის ან გაფართოებითი სამუშაოების წარმოების

დროს ხორციელდება მხოლოდ საქართველოს ტექნიკური უნივერსიტეტის კომპიუტერული ქსელის მართვის ცენტრის ინჟინერის ან ადმინისტრატორის მიერ

- დაუშვებელია საუნივერსიტეტო ქსელთან თვითნებური მიერთება
- აკრძალულია საუნივერსიტეტო ქსელში რაიმე ქსელური მოწყობილობის ჩართვა მომხმარებლის მხრიდან, ცენტრთან შეთანხმების გარეშე
- საუნივერსიტეტო ქსელში პრობლემის წარმოქმნის დროს ხორციელდება მისი ლოკალიზაცია, მიზეზის დადგენა და პრობლემის აღმოფხვრა
- საკომუნიკაციო კვანძებთან კომუნიკაცია უნდა ხორციელდებოდეს დაშიფრული პროტოკოლის მეშვეობით
- მონიტორინგის სისტემის მეშვეობით რეგულარულად უნდა ხორციელდებოდეს საკომუნიკაციო კვანძებზე დაკვირვება
- სისტემის სრული მტყუნების შემთხვევაში აღდგენის გეგმის მიხედვით ხდება ჯერ ცენტრალური მაკომუტირებელი კვანძების აღდგენა და შემდგომ პერიფერიული მოწყობილობებთან კომუნიკაციის აღდგენა
- ნებისმიერი უარყოფითი მოვლენის შესახებ ინფორმაცია უნდა გადაიგზავნოს log სერვერზე.

1.7 დაშვებული პორტები და სერვისები

უსაფრთხოების პოლიტიკის შესაბამისად გახსნილია მხოლოდ ის პორტები და სერვისები, რომელიც საგანმანათლებლო მიზნებისთვის არის მიზანშეწონილი და საუნივერსიტეტო ქსელის გამართული და უსაფრთხო მუშაობისთვის არის აუცილებელი.

1.8 ნებადართული პორტების ჩამონათვალი:

TCP: 20, 21, 25, 53, 80, 110, 143, 443, 465, 578, 993, 995, 8000-8002, 8080, 81, 8081, 7501, 4444, 9933, 2082, 2222, 13000, 1110, 2110, 2082, 2083, 989, 4244, 5222, 5223, 5228, 5242, 49152-65535

UDP: 53,123,5060-5070,1000-2000,9785,5243,9090,3478-3481,49152-65535

უსაფრთხოების მიზნით დახურულია გარედან წვდომა სტუ-ს ქლაუდზე არსებული კრიტიკული სერვისების სამართავ ინტერფეისებზე (მათ შორის იმ სერვისებზეც, რომლის მართვას და მენეჯმენტს ახორციელებს სხვა სამსახური), ნებადართულია გარედან წვდომა მხოლოდ VPN კავშირის საშუალებით.

აღნიშნული პოლიტიკა გათვალისწინებულია იმისთვის, რომ სტუ-ს კომპიუტერული ქსელი იყოს მაქსიმალურად საუნივერსიტეტო გარემოზე მორგებული, ასევე ქსელისთვის დამახასიათებელი უსაფრთხოების მაღალი რისკების გათვალისწინების და სტუ-ს ინტერნეტ ტრაფიკის არა საუნივერსიტეტო მიზნებისთვის გამოყენების შესამცირებლად.

1.8 საქართველოს ტექნიკური უნივერსიტეტის უსადენო ქსელის (WI-FI) მართვის პოლიტიკა

საქართველოს ტექნიკური უნივერსიტეტის სტუდენტებისთვის (GTU STUDENTS), უსადენო ქსელში გამოყებებულია შემდეგი შეზღუდვები:

- სტუდენტებს უკაბელო ქსელის გამოყენებით აქვთ შესაძლებლობა გამოიყენონ ყველა ის რესურსი, რომელიც საგანმანათლებლო მიზნებით არის მიზანშეწონილი, ხოლო ყველა სხვა რესურსზე წვდომა შეზღუდულია
- ინტერნეტი-ტრაფიკის სიჩქარე შეადგენს 10 Mb/s
- შეზღუდულია წვდომა სტუ-ს ინტრანეტის ნაწილზე - ყველა სამართავი პანელების და კრიტიკული სერვისების სამართავ ინტერფეისებზე (მათ შორის იმ სერვისების, რომლის მართვას და მენეჯმენტს სტუ-ს სხვა სამსახური ახორციელებს*)

საქართველოს ტექნიკური უნივერსიტეტის სტუმრებისთვის (GTU GUEST) გამოყოფილ უსადენო ქსელში გამოყებებულია შემდეგი შეზღუდვები:

- შეზღუდულია წვდომა ინტერნეტთან, დახურულია ყველა სერვისი და გახსნილია წვდომა მხოლოდ ის პორტებზე, სერვისებზე და რესურსზე რომელიც საჯაროა უნივერსიტეტისთვის. ასევე გახსნილია წვდომა საგანგებო, სასწრაფო და საინფორმაციო რესურსებზე

- დახურულია ყველანაირი ტიპის გასართობი, ტორენტ და მსგავსი ტიპის საიტები
- შეზღუდულია წვდომა სტუ-ს ინტრანეტზე, ყველა სამართავი პანელების და კრიტიკული სერვისების სამართავ ინტერფეისებზე (მათ შორის იმ სერვისების, რომლის მართვას და მენეჯმენტს სხვა სამსახური ახორციელებს*)
- დახურულია წვდომა ყველა ადმინისტრაციულ კერძო საუნივერსიტეტო რესურსზე.

2. სერვერული ინფრასტრუქტურა და მისი მართვის პოლიტიკა

შესავალი

სტუ-ს სერვერული ინფრასტრუქტურა ემსახურება სტუ-ში არსებული სერვისების და სამეცნიერო-კველევითი ამოცანების მხარდაჭერას.

სტუ-ს სერვერული ინფრასტრუქტურა განთავსებულია სტუ-ს ხუთ ლოკაციაზე:

სტუ-ს მე-6 კორპუსი, 306-დ ოთახი (6 სერვერი), სტუ-ს პირველი კორპუსი (კომპიუტერული ცენტრი - 2 სერვერი), კიბერნეტიკის ინსტიტუტი, მათემატიკის ინსტიტუტი და აგრარული ფაკულტეტი.

ფიზიკური ინფრასტრუქტურა

სერვერული ინფრასტრუქტურა განთავსებულია სპეციალურ სარეკრიაციო ოთახებში, რომლებიც უზრუნველყოფილია გაგრილებით და უწყვეტი კვების მოწყობილობებით. სერვერულ ინფრასტრუქტურაში შედის სხვადასხვა ტიპის და სიმძლავრის სერვერები, რომლებიც ასრულებენ როგორც მთავარ, ასევე სხვა სერვერების სარეზერვო ფუნქციასაც.

ინფრასტრუქტურაში შედის სახვადასხვა ტიპის სერვერები: სტორიჯ, ბლეიდ და სტანდარტული ტიპის სერვერები.

სერვერულ ინფრასტრუქტურაში გამოყენებული ტექნოლოგია საშუალებას იძლევა მოხდეს სერვერების კლონირება (სარეზერვო ასლების) სხვადასხვა ფიზიკურ სერვერზე. სერვერის ფიზიკური, პროგრამული მტყუნების ან ჰაკერული თავდასხმის შემთხვევაში ინფრასტრუქტურა საშუალებას იძლევა გაეშვას სარეზერვო სერვერი.

სერვერული ინფრასტრუქტურა დაცულია მუდმივი კვების ელემენტებით რაც სისტემას საშუალებას აძლევს 2 საათამდე შენარჩუნდეს სერვერების ფუნქციონირება.

ინფრასტრუქტურაში გამოყენებული ტექნოლოგიები

ინფრასტრუქტურაში შემავალი სერვერების დიდი ნაწილი იმართება ე.წ. ღრუბლოვანი ტექნოლოგიის გამოყენებით (ვირტუალიზაცია). ტექნოლოგიაში გამოყენებულია vSphere Hypervisor და Citrix XenServer -ის თავისუფალი ლიცენზია. ინფრასტრუქტურის ფიზიკური სერვერებისთვის ზოგ შემთხვევაში გამოყენებულია UNIX, Linux და Microsoft Windows Server ოპერაციული სისტემები.

ინფრასტრუქტურა დაცულია ფაირფოლით.

ინფრასტრუქტურის ადმინისტრირება (მართვა)

სტუ-ს სერვერული და ქსელური ინფრასტრუქტურა იმართება ქსელის მართვის ცენტრის მიერ. ცენტრი პასუხისმგებელია სერვერული და ქსელური ინფრასტრუქტურის სისტემურ გამართვაზე და მის ტექნიკურ უზრუნველყოფაზე.

დაშვება ფიზიკურ ინფრასტრუქტურაზე

სერვერული ინფარსტრუქტურა განთავსებულია დაცულ სპეციალურ ოთახებში და მასზე წვდომა აქვს მხოლოდ კომპიუტერული ქსელის მართვის ცენტრის თანამშრომლებს. სერვერის ოთახის გასაღებები ინახება ცენტრის ერთ–ერთ ოთახში და საჭიროების შემთხვევაში ხდება მისი გამოყენება, დაუშვებელია სხვა თანამშრომლების შესვლა ამ ოთახებში.

ინფრასტრუქტურაში პაროლების შენახვის და გამოყენების წესი

ყველა პაროლები ინახება ამ მიზნისთვის გამოყოფილ სპეციალურ დაცულ ადგილას და ის ხელმისაწვდომია მხოლოდ უფლებამოსილი თანამშრომლებისთვის.

სერვერული ინფრასტრუქტურის მონაცემთა უსაფრთხოება

სტუ - ს სერვერებზე განთავსებული ინფორმაციის ასლები ინახება სარეზერვო ფიზიკური სერვერის მონაცემთა საცავებში .

კრიტიკულ სერვისებზე უნდა განხორციელდეს სარეზერვო ასლების შექმნა:

- კრიტიკულად მნიშვნელოვანი სერვისების (რომელზეც დღეში რამდენიმეჯერ შედის ცვლილება) დღეში ერთჯერ, ზოგ შემთხვევაში დღეში 5-ჯერ მოხდეს მონაცემთა ბაზების და სხვა მონაცემების არქივირება.
- სხვა შემთხვევაში მონაცემთა არქივირება უნდა განხორციელდეს კვირაში ერთჯერ.

3. ინფორმაციის უსაფრთხოების პოლიტიკა

მიზანი

პოლიტიკის მიზანია სტუდენტების და თანამშრომლების ინტერესების დაცვა, რომლებიც იყენებენ საქართველოს ტექნიკური უნივერსიტეტის ინფორმაციული რესურსებს, რომლის მართვას და ადმინისტრირებას ახდენს საქართველოს ტექნიკური უნივერსიტეტის კომპიუტერული ქსელის მართვის ცენტრი, ინფორმაციული ტექნოლოგიების დეპარტამენტი და სხვა საუნივერსიტეტო სტრუქტურები.

აღწერა

სტუ-ს ინფორმაციული ინფრასტრუქტურა აერთიანებს ინტრანეტ და ინტერნეტ სერვისებს.

ინტერნეტ და ინტრანეტ რესურსებთან წვდომისას მნიშვნელოვანია გარკვეული უსაფრთხოების უზრუნველყოფა. ამ მიზნით სტუ-ში შემუშავებულია უსაფრთხოების წესები.

უსაფრთხოების დოკუმენტი შექმნილია, რათა ტექნიკური უნივერსიტეტის ქსელში ჩართული მომხმარებლები და მოწყობილობები ექვემდებარებოდეს ერთიან უსაფრთხოების პოლიტიკას. ამ პოლიტიკის მიზანია ტექნიკური უნივერსიტეტის ქსელში არასანქცირებული წვდომის შეზღუდვა, რესურსების ოპტიმალური გამოყენება, მომხმარებელთა კომპიუტერების დაინფიცირების თავიდან აცილება ეფექტური ანტივირუსული მექანიზმის გატარებით, არასასურველი ტრაფიკის გენერირების და სისტემაზე არასასურველი გავლენის თავიდან აცილება, საფუძველის მომზადება კონვერგირებული (სხვადასხვა ტიპის ტრაფიკის გადაცემაზე ორიენტირებული) ქსელის შესაქმნელად.

უსაფრთხოების წესების მიზანია, აგრეთვე სტუ-ს მომხმარებლები ინფორმირებული იქნენ სხვადასხვა ტიპის საფრთხეების და მისგან თავის დაცვის საშულებების შესახებ. ასევე უსაფრთხოების დოკუმენტში თავმოყრილია გარკვეული წესები, რომელიც უნდა დაიცვას სტუ-ს ქსელში ჩართულმა თითოეულმა მომხმარებელმა.

უსაფრთხოების წესები ვრცელდება სტუ-ს ყველა მომხმარებელზე და მოწყობილობაზე. მისი დაცვა სავალდებულოა ყველა თანამშრომელის, სტუდენტის და ყველა იმ პირისათვის, რომელიც მიერთებულია სტუ-ს ერთიან ინფორმაციულ სივრცესთან.

ინტერნეტში და ინტრანეტში მუშაობისას არსებობს უამრავი საფრთხე, რომელმაც შეიძლება გამოიწვიოს ინფორმაციის და სერვისების სხვა დასხვა ტიპის დაზიანება. ცნობილი საფრთხეებია: თავდასხმები და დაზიანებები გამოწვეული ვირუსების ან ე.წ. ”ტროას ცხენების” მიერ, კომპიუტერული სისტემის მიერ მომსახურებაზე უარის თქმა, ფიშერები და სხვა, რომელებიც გამოწვეულია ადამიანის მიერ შექმნილი ბოროტგანზრახული პროგრამების მიერ. მსგავსი საფრთხეების თავიდან აცილების მიზნით, აუცილებელია უსაფრთხოების წესების დაცვა.

უნივერსიტეტის ქსელი შეიძლება გახდეს სხვადასხვა ტიპის ხშირი თავდასხმის ობიექტი. ინტერნეტში პერმანენტულად ხორციელდება ქსელური სერვისების სკანირება, სუსტი წერტილების აღმოჩენის მიზნით, ხოლო მათი აღმოჩენის შემთხვევაში ხორციელდება კიბერთავდასხმა, რამაც შეიძლება გამოიწვოს სხვადასხვა შეფერხებები.

უსაფრთხოების წესების დაცვა არის გარკვეული საშუალება რისკებიდან თავის ასაცილებლად, რაც ქსელში მუშაობას გახდის უფრო საიმედოს და უსაფრთხოს.

ინფორმაციული უსაფრთხოების მართვის ორგანიზაციული სტრუქტურა

ინფორმაციის ტექნოლოგიების მართვის პოლიტიკის განხორციელებასა და განახლებაზე უფლებამოსილია სტუ-ს კომპიუტერული ქსელის მართვის ცენტრი.

პოლიტიკის აღსრულების, პერიოდული განხილვის და განახლების პროცესში აქტიურადაა ჩართული უნივერსიტეტის ხელმძღვანელობა, ინფორმაციული ტექნოლოგიების დეპატრამენტი და კომპიუტერული ქსელის მართვის ცენტრი.

უნივერსიტეტის კომპიუტერული ქსელის მართვის ცენტრის უსაფრთხოების სპეციალისტი უზრუნველყოფს ინფორმაციული უსაფრთხოების მონიტორინგს, ინციდენტების შეგროვებას, მათზე რეაგირების მექანიზმების შემუშავებას და რექტორთან შესაბამისი ანგარიშების წარდგენას.

პაროლის პოლიტიკა

პოლიტიკის მიზანია შეიქმნას ძლიერი პაროლების შექმნის, მათი დაცვის და მათი ხშირად შეცვლის საჭიროების სტანდარტი საქართველოს ტექნიკური უნივერსიტეტის კომპიუტერულ სისტემებში. პაროლი არის მნიშვნელოვანი ასპექტი კომპიუტერულ უსაფრთხოებაში. სუსტი პაროლის პოლიტიკამ შეიძლება გამოიწვიოს საუნივერსიტეტო ქსელში არაავტორიზებული შესვლა და/ან მისი კრიტიკული რესურსის არასანქცირებული გამოყენება. აღნიშნული პოლიტიკა და პროცედურები სტუ-ს მომხმარებლებს დაეხმარება შეამცირონ საფრთხის რისკი.

აღნიშნული პოლიტიკა და პროცედურები ვრცელდება საქართველოს ტექნიკური უნივერსტიტეტის კომპიუტერული ქსელის მართვის ცენტრის ქვეჯგუფების (ქსელის ჯგუფი, ვების ჯგუფი, სისტემური ჯგუფი) და ცენტრის მხარდაჭერილი სისტემების მაშტაბით (მაგ: ვირტუალიზაციის)

სტუ-ს თანამშრომლები ვალდებულნი არიან შეცვალონ პაროლი ყოველ 6 თვეში.

პაროლი:

1. არ უნდა იყოს პირად ინფორმაციაზე დაყრდნობით შექმნილი(მაგ. სახელი, გვარი, დაბადების თარიღი და სხვა);

2. არ უნდა იყოს ე.წ. ლექსიკონის სიტყვა;

3. უნდა იყოს რაც შეიძლება გრძელი, მინიმუმ 10 სიმბოლო. უნდა შეიცავდეს მაღალი და დაბალი რეგისტრის ასოებს, ციფრებსა და სხვა სიმბოლოებს;

4. არ უნდა იყოს გამოყენებული სხვა ანგარიშებზე;

5. უნდა იყოს რაც შეიძლება ადვილად დასამახსოვრებელი;

6. კარგი პაროლის მაგალითი: K@rG1par0L1smaGaliT1

არასანქცირებული ფიზიკური მოწყობილობების მიერთების აკრძალვა

სტუდენტებს და თანამშრომლებს ეკრძალებათ ნებისმიერი ქსელური მოწყობილობის შეერთება საქართველოს ტექნიკური უნივერსიტეტის ქსელში გარდა იმ შემთხვევისა თუ მოწყობილობის გამოყენება ნებადართულია სტუ-ს კომპიუტერული ქსელის მართვის ცენტრის მიერ. არასანქცირებული ქსელის მოწყობილობები შეიძლება იყოს სერვერები, მარშრუტიზატორები, კომუტატორები, ჰაბები, უსადენო დაშვების წერტილები და სხვა. აღნიშნული მოწყობილობების არასწორად გამოყენებამ

შესაძლოა საფრთხე შეუქმნას უნივერსიტეტში არსებულ კომპიუტერული ინფრასტრუქტურის გამართულ მუშაობას.

უსაფრთხოების პოლიტიკის დარღვევა

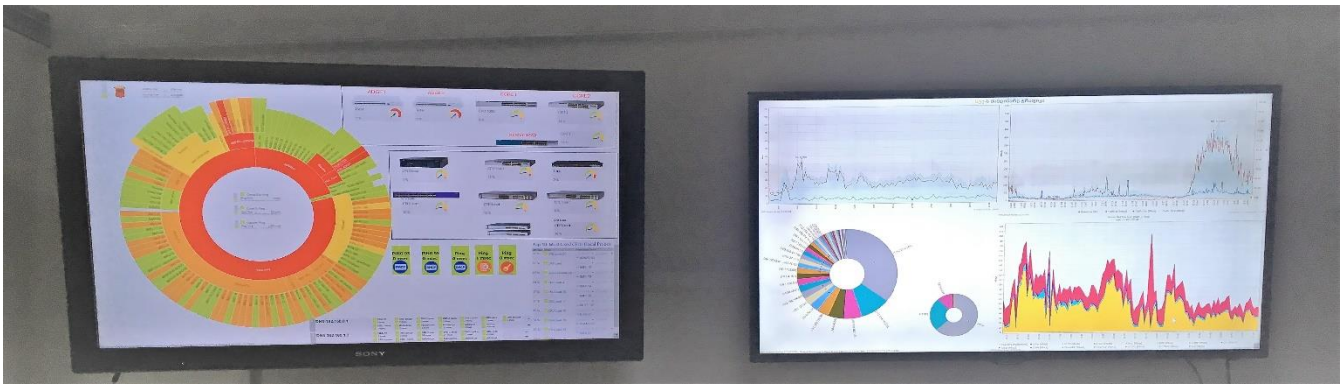
ქსელის მოწყობილობების არასანქცირებული გამოყენების მცდელობა წარმოადგენს უსაფრთხოების პოლიტიკის დარღვევას და გამოიწვევს დისციპლინარულ ქმედებას.

იმისათვის, რომ თავიდან იქნეს აცილებული შესაძლო არასანქცირებული საქმიანობა და გარკვეული სერვისების პარალიზება, ცენტრი უფლებას იტოვებს გათიშოს არასანქცირებული მოწყობილობა ქსელიდან და ამოიღოს ეს მოწყობილობა ხმარებიდან.

4. უსაფრთხოების, ინციდენტების აღმოჩენის და რეაგირების ტექნოლოგიები და მონიტორინგი

სტუ-ს კომპიუტერულ ქსელში გამოყენებულია სხვადასხვა მონიტორინგის სისტემები (PRTG, DUDE, KIWI SYSLOG Server) და პროტოკოლები (snmp, Netflow, syslog). რისი მართვაც ხდება ცენტრალიზებულად, ქსელის ოპერაციების ცენტრში (NOC).

ხორციელდება ინტერნეტის ლოკალური და გლობალური ტრაფიკის, აქტიური მომხმარებლების, მოთხოვნადი სერვისებისა და პროტოკოლების მუდმივი 24/7 მონიტორინგი, რის საფუძველზეც ხდება მონაცემების შეგროვება, მათი ბაზისის გამოთვლა და უჩვეულო ტრაფიკის იდენტიფიცირება და ანალიზი. მონიტორინგის საშუალებით ხდება სხვადასხვა კიბერ-შეტევების აღმოჩენა და პრევენცია.
ასევე ცენტრალიზებულად ხდება ქსელის მოწყობილობების მდგრადობის და სტაბილურად მუშაობის მუდმივი მონიტორინგი სხვადასხვა სენსორების გამოყენებით (CPU-დატვირთვა, თავისუფალი RAM, ტემპერატურა და ა.შ.). ცენტრალიზებულად ხდება ყველა ლოგის (LOG) შენახვა გარკვეული დროით და პრობლემის შემთხვევაში მათი ანალიზი.



სურათი №2. სტუ-ს ქსელის ოპერაციების ცენტრის ოთახი - 6 კორპუსი 306-დ .

5. ქსელის ინციდენტთა აღრიცხვის სისტემა

სტუ-ს კომპიუტერული ქსელი იყენებს საკუთარ ინციდენტთა აღრიცხვის სისტემას, სადაც ხდება ყველა შემოსული ზარის და პრობლემის დაფიქსირება. ავტომატურად ხდება პრობლემების გადანაწილება სხვადასხვა კომპეტენციის პირზე. კეთდება პრობლემური საკითხების გრაფიკული ჩარტები (ხშირად დაზიანებული მოწყობილობები, TOP პრობლემური კორპუსები, ფაკულტეტები, გადაჭრილი პრობლემები და ა.შ.).
ხდება ინფორმაციის შეგროვება, ხშირი პრობლემის გამოკვეთა, მათი ანალიზი და პრობლემის გადაწყვეტის გზები.