ზოგადოებას ადგება დიდი მატერიალური, ფინანსური და მორალური ზარალი [1, 4].

ინტერნეტის კრიმინალიზაციას ხელს უწყობს დამნაშავის ანონიმურობა, რომელიც ხშირ შემთხვევაში დანაშაულის ადგილიდან რამდენიმე ათას კილომეტრზე იმყოფება.

კომპიუტერული დანაშაულის პროფილაქტიკის გახსნისა და დამნაშავეთა დასჯის მიზნით საჭიროა გაირკვეს დანაშაულის არსი, მოქმედების ადგილი, მისი განხორციელების შედეგად მიყენებული მატერიალური და მორალური ზარალი, დანაშაულის ჩადენის მიზანი.

დღეისათვის შედარებით დაცულია სამართალდამცავ ორგანოებში განთავსებული ინფორმაცია, ხოლო სხვა დაწესებულებებში ინფორმაცია ნაკლებადაა დაცული. ამ უკანასკნელს მიეკუთვნებიან საგანმანათლებლო დაწესებულებები.

აღნიშნულიდან გამომდინარე სტატიაში გაანალიზებულია საგანმანათლებლო დაწესებულებებში ინფორმაციული უსაფრთხოების არსებული მდგომარეობა და შემოთავაზებულია მოთხოვნები, რომელიც უნდა დააკმაყოფილოს ამ დაწესებულებებში არსებულმა უსაფრთხოების სისტემამ.

ინფორმაციული უსაფრთხოება არის ინფორმაციისა და ინფორმაციული სისტემების დაცვა არაავტორიზებული წვდომისაგან. ინფორმაციასა და ინფორმაციულ სისტემებს მნიშვნელოვანი ადგილი უკავია ჩვენს ცხოვრებაში. შესაბამისად პრობლემატურია ინფორმაციის უსაფრთხოების საკითხიც.

ხშირია შემთხვევები, როდესაც კომპანიების მხრიდან ორგანიზაციების მართვისას ყურადღება ექცევა მხოლოდ კომპიუტერულ სისტემებს და არ ხორციელდება ინფორმაციის დაცვა, რის შედეგადაც მათ ხშირად დაუკარგავთ წლების განმავლობაში შეგროვილი ინფორმაცია და ამით კომპანიის მუშაობა იძულებით შეჩერებულა.

ინფორმაციული ტექნოლოგიების გამოყენებით კომპანიის მართვის სრულყოფისათვის, რომელიც საშუალებას იძლევა ავიცილოთ უამრავი გაუთვალისწინებელი ხარჯები და მივიღოთ მაქსიმალური სარგებელი აუცილებელია: ინფორმაციული უსაფრთხოების პოლიტიკის შემუშავება, დანერგვა და პერიოდულად გაუმჯობესებაც კი.

ორგანიზაციები თავიანთი ინფორმაციული სისტემებითა და ქსელებით უშუალოდ დგანან ისეთი საფრთხეების წინაშე, როგორიცაა: კომპიუტერული თაღლითობა, შპიონაჟი, საბოტაჟი, ვანდალიზმი, ხანძარი, წყალდიდობა და სხვა. მომხმარებლისათვის სერვისის შეფერხებით მიწოდების მიზნით მავნე კოდის შემცველი პროგრამები, კომპიუტერული ჰაკერობა, კომპიუტერულ პროგრამებზე თავდასხმა უფრო და უფრო დახვეწილი ხერხებით ხორციელდება. ასეთი ქმედებებით გამოწვეული ზარალი მუდმივად იზრდება [7, 8].

ინფორმაციული უსაფრთხოება მნიშვნელოვანია როგორც საჯარო, ასევე კერძო სექტორის საქმიანობისთვის. იგი გამოიყენება ელექტრონული მმართველობის ან ელექტრონული საქმისწარმოების მიზნებისთვის. ასევე ამ პროცესებთან დაკავშირებული რისკების შესამცირებლად ან თავიდან ასაცილებლად.

დღეისათვის რესპუბლიკის წამყვან საგანმანათლებლო დაწესებულებებში კომპიუტერთა რაოდენობა რამდენიმე ათასია, რომლებიც განთავსებულია კომპიუტერულ ცენტრებსა და ლაბორატორიებში, აკადემიური და ადმინისტრაციული პერსონალის სამუშაო ოთახებში, ბიბლიოთეკებში. 2010 წლიდან საგანმანათლებლო დაწესებულებებს შემოუერთდათ უმაღლესი სასწავლებლები და სამეცნიერო კვლევითი ინსტიტუტები, რომლებსაც საკუთარი კომპიუტერული პარკი გააჩნიათ.

საგანმანათლებლო დაწესებულებების ყველა სასწავლო კორპუსი უზრუნველყოფილია ინტერნეტით. საკომუნიკაციო საშუალებად გამოყენებულია ოპტიკურ-ბოჭკოვანი კაბელი ან ADSL-ტექნოლოგია. სასწავლებლის სტუდენტებისა და აკადემიური პერსონალისათვის პროგრამული პაკეტებით უზრუნველყოფა ხორციელდება მოთხოვნილების მიხედვით, საგანმანათლებლო სპეციფიკისა და საჭიროების გათვალისწინებით.

საგანმანათლებლო დაწესებულებების კვლევითი საქმიანობის მართვაში გამოიყენება შემდეგი საინფორმაციო-საკომუნიკაციო ტექნოლოგიები:

- ინტერნეტ-სერვისები: Web, FTP, SMTP, IMAP, POP3;
- ქსელის მართვისა და მონიტორინგის სერვისი SNMP და NetFlow;
- სასწავლო პროცესის მართვის ელექტრონული სისტემა;
- დაცვისა და უსაფრთხოების სამსახურის სერვისი IP კამერებით;
- თანამშრომელთა სამსახურში გამოცხადებისა და წასვლის რეგისტრაციის სერვისი (UDP პროტოკოლით);

- დისტანციური კავშირისა და ვიდეო-კონფერენციების სერვისი (H323 პროტოკოლით);
- ბანკი-კლიენტის სერვისი (VPN კავშირებით);
- ელექტრონული ჟურნალები და ელექტრონული საბიბლიოთეკო კატალოგი;
- ელექტრონული სწავლების კომპონენტი-ელექტრონული სწავლება (Moodle);
- მოკლე ტექსტური შეტყობინებების გაგზავნის სისტემა (SMPP პროტოკოლით) და ა.შ.

ინფორმაციის უსაფრთხოება მჭიდროდაა დაკავშირებული ელექტრონულ-ციფრულ ხელმოწერასთან და იდენტიფიკაციისა და აუტენტიფიკაციის საშუალებებთან [2, 5, 6].

ელექტრონულ-ციფრული ხელმოწერა არის ელექტრონული დოკუმენტის რეკვიზიტი, რომლის დანიშნულებაა კრიპტოგრაფიული გარდაქმნის შედეგად მიღებული ელექტრონული დოკუმენტი დაიცვას გაყალბებისაგან. დაადგინოს, რომ დოკუმენტში ადგილი არა აქვს დამახინჯებას და მოხდეს ელექტრონული ხელმოწერის გასაღების სერტიფიკატის მფლობელის იდენტიფიცირება [3].

თანამედროვე კორპორაციული ქსელების უსაფრთხოების დაცვის ამოცანები ყოველდღიურად რთულდება და შესაბამისად, იქმნება აპარატულ-პროგრამული პროდუქტები ამ ამოცანების შესასრულებლად. თუმცა, ინტერნეტის და ვებ-ტექნოლგიების განვითარების მაღალი ტემპის გამო, ისეთი სტანდარტული უსაფრთხოების მოწყობილობები და პროგრამები, როგორებიცაა ფაიერვოლი, პროქსი-სერვისი, VPN, Antimalware, სპამ-ფილტრი და სხვ. ვეღარ უზრუნველყოფენ კორპორაციული უსაფრთხოების დაცვის მაღალ დონეს. ამიტომ საჭიროა ინტეგრირებული მიდგომები და უსაფრთხოების ეშელონირებული სისტემების შექმნა.

თბილისის სახელმწიფო უნივერსიტეტის მონაცემთა ცენტრში მოქმედებს მონაცემთა უსაფრთხოების ეშელონირებული სისტემა.

ორგანიზაციის შიდასაინფორმაციო ინფრასტრუქტურა გარშემორტყმულია ინტერნეტით, რომლისგანაც იგი გამიჯნულია **პირველი ეშელონით – ქსელის პერიმეტრით (Network Edge)**. ქსელის პერიმეტრი მოიცავს შემდეგ ძირითად ქსელურ მოწყობილობებსა და აპლიკაციებს:

- მთავარი მარშრუტიზატორი (რუთერი, გეითვეი) — საინფორმაციო ინფრასტრუქტურის ჭიშკარი გარესამყაროსთან (ინტერნეტთან);
- გარებრანდმაუერი (ფაიერვოლი) — ინტერნეტში გამავალი და ინტერნეტიდან შემომავალი საინფორმაციო ნაკადების კონტროლი;
- VPN-სერვისი (რუთერზე ან ფაიერვოლზე) — დაშიფრული წვდომის უზრუნველყოფა საინფორმაციო ინფრასტრუქტურასთან.

მეორე ეშელონი — „დემილიტარიზებული ზონა“ (DMZ) პერიმეტრსა და შიდაქსელს შორისაა განლაგებული. მასში განთავსებულია საინფორმაციო ინფრასტრუქტურის კომპონენტები (მაგალითად ვებ-გვერდი).

DMZ-ში განთავსებულია შემდეგი მოწყობილობები და სერვისები:

- პროქსი-სერვისი — ინტერნეტში მომხმარებელთა მუშაობის კონტროლი (არასასურველი საიტების ბლოკირება) და ვებ-კონტენტის ქეშირება;
- IDS/IPS-სისტემები — ორგანიზაციის საინფორმაციოსივრცეშიარასანქცირებულიწვდომების (Intrusions) აღმოჩენა ან/და პრევენცია (მაგალითად, რომელიმე მავნე პროგრამის მეშვეობით ბოტნეტის ნაწილად ქცეული კომპიუტერების აღმოჩენა;
- შიდაბრანდმაუერი (ფაიერვოლი) — კლიენტთა და სერვერთა ქსელებს შორის მონაცემთა ნაკადების კონტროლი.

თავდაცვის მესამე ეშელონი ორგანიზაციის შიდასაინფორმაციო სივრცეს მოიცავს და შემდეგი კომპონეტების განშედგება:

- ცენტრალური ანტივირუსი — მავნე პროგრამული უზრუნველყოფის (ვირუსები, ქსელის ჭიები, ტროას ცხენები და სხვა.) აღმოჩენისა და უვნებელყოფის ერთიანი სისტემა;
- ორგანიზაციის დომენის ჯგუფური პოლიტიკა (Group Policy) — წვდომების შეზღუდვა ორგანიზაციის დომენში (მაგ. Active Directory) ჩასმული კომპიუტერების, მომხმარებლებისა და სხვა რესურსებისთვის (მაგალითად, Download-ფუნქციის გათიშვა, პაროლების იძულებითი შეცვლა გარკვეული დროის შემდეგ) წინასწარ განსაზღვრული შიდა IT-პოლიტიკის მიხედვით.

თავდაცვის მეოთხე ეშელონად უშუალოდ კლიენტთა და სერვერულ გამოთვლით სისტემებზე გამართული დაცვის სისტემები (მაგალითად, ოპერაციულ სისტემაში გააქტიურებული ფაიერვოლი და Antimalware) მოიაზრება.

თანამედროვე კორპორაციულ ქსელებში უსაფრთხოების პრობლემებთან გასამკლავებლად სულ უფრო ხშირად გამოიყენება UTM-მოწყობილობები, რომლებსაც სხვანაირად NG-ფაიერვოლებსაც უწოდებენ. პირველი აბრევიატურა იშიფრება როგორც Unified Threat Management — საფრთხეთა უნიფიცირებული მართვა, ხოლო მეორე Next Generation Firewall — მომავალი თაობის ფაიერვოლი. ორივე შემთხვევაში ერთი მოწყობილობის ფარგლებში რამდენიმე ფუნქციის შესაბამისი პროგრამული მოდულია ინტეგრირებული, რომელთა შორის გვხვდება უსაფრთხოების უზრუნველყოფის როგორც ტრადიციული (ფაიერვოლი, პროქსი-სერვისი, VPN, Antimalware, სპამ-ფილტრი), ისე ბოლო წლებში გავრცელებული ინსტრუმენტები, რომელთაგან ყველაზე მნიშვნელოვანია:

- ვებ-ფილტრი - ვებ-გვერდების შიგთავსის (კონტენტის) ფილტრაციის აპარატურულ-პროგრამული საშუალება;
- IDS/IPS-სისტემა – ინფორმაციულ სისტემაში არასანქცირებული შეღწევების გამოვლენისა (Intrusion Detection) დაპრევენციის (Intrusion Prevention) სისტემა;
- DLP-სისტემა (Data Leak Prevention) ინფორმაციის გაჟონვასთან საბრძოლველად.

თანამედროვე UTM (Unified Threat Management) – საფრთხეთა უნიფიცირებული მართვის სისტემები ხშირად საკუთარი აპარატული პლატფორმის თანხლებით მიეწოდება მოხმარებელს.

ამგვარი მიდგომის უპირატესობა სპეციალურ კონკრეტულ ამოცანებზე ორიენტირებული აპარატურის (ASIC — application-specific integrated circuit) გამოყენებაში მდგომარეობს, რომლის საშუალებითაც უსაფრთხოების დაცვის ამოცანათა გადაწყვეტის ეფექტურობა მკვეთრად იზრდება.

ზემოთქმულიდან გამომდინარე, ინტეგრირებული სისტემები ინფორმაციული სისტემების დაცვის საიმედო საშუალებებს წარმოადგენენ და ეფექტურობის თვალსაზრისით ტრადიციული დაცვის სისტემებს მკვეთრად აღემატებიან.

გარდა აღნიშნულისა აუცილებელია:

- უმაღლეს საგანმანათლებლო დაწესებულებებში ინფორმაციის კომპლექსური დაცვის განხორციელება, რაც გულისხმობს ინფორმაციის, ფიზიკურ, ტექნიკურ და ინტელექტუალურ დაცვას. კომპიუტერული სისტემები დაცული უნდა იქნეს მიტაცებისაგან, ყაჩაღური თავდასხმებისაგან, ფიზიკური განადგურებისაგან, წყალდიდობისაგან და სხვა საგანგებო სიტუაციებისაგან.
- რამდენადაც, ინფორმაციის დაცვაში დიდ როლს თამაშობს კომპიუტერული სისტემის უშუალო მომხმარებელი, საჭიროა ამ მიმართულებით ზოგიერთი განვითარებული ქვეყნის გამოცდილების გადმოღება (მაგ., აშშ). აშშ-ს წარმოება-დაწესებულებებში შემუშავებულია კომპიუტერული სისტემის მომხმარებლის ქცევის ნორმების ეთიკური კოდექსი, რომლის მიხედვითაც არაეთიკურად ითვლება კომპიუტერული სისტემის მომხმარებლის წინასწარ-განზრახული ან უნებლიე მოქმედება, რომლის გამოც ადგილი ექნება კომპიუტერული სისტემის ნორმალური ფუნქციონირების დარღვევას და დარღვეული ფუნქციონირების აღსადგენად დამატებითი რესურსების ხარჯვას [1].
- ინფორმაციის დაცვის მიზნით უმაღლეს საგანმანათლებლო დაწესებულებებში აუცილებელია ორგანიზაციული ღონისძიებების განხორციელება. კერძოდ საჭიროა სათანადო კადრების შერჩევა ინფორმაციულ უსაფრთხოებაზე დაკავებული კადრების პასუხისმგებლობის გაზრდა, უსაფრთხოების საკითხებზე ტრენინგების ჩატარება.
- ინფორმაციული უსაფრთხოების სისტემის გაუმჯობესების მიზნით აუცილებელია ინფორმაციული უსაფრთხოების შესახებ (კომპიუტერული დანაშაულის შესახებ კანონის) სამართლებლივი რეგულირების სრულყოფა.

ამრიგად, საგანმანათლებლო დაწესებულებებში ინტეგრირებული სისტემების დანერგვის პარალელურად ზემოთჩამოთვლილი ღონისძიებების გატარება ინფორმაციული უსაფრთხოების დონეს მნიშვნელოვნად აამაღლებს.

გამოყენებული ლიტერატურა:

1. მაღრაძე მ. ინფორმაციული მენეჯმენტი. თბ., „სამართალი“, 2013.
2. შონიაო., შეროზიათ. ინფორმაციული ტექნოლოგიები და უსაფრთხოება. სტუ, 2008.

3. კუცნავა ვ., კაცაძე გ., დიაკონიძე ქ. ინფორმაციის დაცვა. თბ., „ტექნიკური უნივერსიტეტი“, 2005.
4. Joseph T. Wells. (2010) Internet Fraud Casebook.
5. Экономическая информатика. Учебник и практикум для бакалавриата и магистратуры. Под. редакцией Ю. Д. Романовой М., "Юрайт", 2014.
6. Информационные технологии в экономике и управлении. Под редакцией В. В. Трофимова. М., "Юрайт", 2014.
7. Гафнер В. В. Информационная безопасность. Учебное пособие. Ростов-на-Дону, „Феникс“, 2010.
8. Блинов А. М. Информационная безопасность. Учебное посбие. Санкт-Петербург. Санкт-Петербургский Гос. университет экономики и финансов. 2010.

თავისუფალ ინდუსტრიულ ზონებში ინვესტირების ზოგიერთი პრობლემა

ზურაბ გარაყანიძე — სტუ-ს პროფესორი, ეკონომიკის დოქტორი
ნინო მაღრაძე — საქართველოს უნივერსიტეტის დოქტორანტი

Некоторые проблемы инвестирования в свободных индустриальных зонах

Гараканидзе Зураб Георгиевич
доктор экономики, профессор ГТУ

Резюме

В настоящее время, в связи с обострившей геополитической ситуацией в регионе, экономика Грузии находится в непростой ситуации. Под угрозу ставится экономическая безопасность, так как основной проблемой, в условиях колебания обменного курса Лари, является зависимость нашей экономики от ПИН (FDI), ее самодостаточность. В таких условиях, вопрос инвестиционной безопасности, которая является составной часть экономической безопасности, становится наиболее актуальным.

Экономическая Наука понятие экономической безопасности определяет, как «состояние национальной социально-экономической системы, при котором она поступательно развивается, становясь все более устойчивой к воздействию непредсказуемых или плохо предсказуемых эндогенных и экзогенных факторов». Таким образом, чем выше устойчивость производства, занятости, инвестиций, и одновременно больше возможности дальнейшего увеличения роста экономики, ее модернизации и развития, повышения конкурентоспособности, тем выше экономическая безопасность страны. Исходя из определения видно, что экономическая безопасность включает в себя и инвестиционную безопасность. Ее можно охарактеризовать, как способность национальной хозяйственной системы воздействовать на инвестиционный процесс, который может оказывать влияние на стратегическую конкурентоспособность экономики и устойчивый рост.

Обеспечение мер по усилению инвестиционной безопасности может происходить по следующим направлениям:

- обеспечение экономики достаточным количеством инвестиций для поддержания ее устойчивого развития;
- формирование оптимальной отраслевой и территориальной структуры, специальных зон, инвестиций;
- максимальное осуществление всех реализуемых внутри страны инвестиционных проектов на рынке ценных бумаг.

При реализации инвестиционных проектов необходимо учитывать ряд изменении в существующих законах, которые оказывают влияние на деятельность иностранных инвесторов на территории Грузии.

საკვანძო სიტყვები: ევროკავშირი, ზონები, ინვესტიციები, კაპიტალიზაცია, ფასიანი ქაღალდები, აფხაზეთი.

შესავალი

საინვესტიციო უსაფრთხოების საკითხებს საქართველოში თითქმის არასდროს არ ექცეოდა სათანადო ყურადღება. შედეგი სახეზეა: ხან ქსეროქსების კომპანიაზე რამდენჯერმე გაყიდული „ჭიათურმანგანუმი“, ხანაც ოფშორებში რეგისტრირებული რუსული კაპიტალის ე.წ. ცრუმაგიერ ფირმებზე პრივატიზებული მადნეულის კომბინატი და საეჭვო რეპუტაციის თურქ ბიზნესმენზე პრივატიზებული „ფერრო“. შედეგი – ქვეყნის შელახული საინვესტიციო იმიჯი და პირდაპირი უცხოური ინვესტიციების ნაკადების შემცირება... ამას ემატება ქვეყანაში სპეციალური ეკონომიკური ზონების არსებობა, რომელთა საქმიანობა აბსოლუტურ გახსნილობაზეა დამყარებული.

თავისუფალი ინდუსტრიული ზონების პრობლემები. საქართველოში თავისუფალი ინდუ-