საქართველოს ეროვნული ბანკის პრეზიდენტის

ბრძანება №56/04
2019 წლის 22 მარტი

ქ. თბილისი

კომერციული ბანკების კიბერუსაფრთხოების მართვის ჩარჩოს დამტკიცების შესახებ

„საქართველოს ეროვნული ბანკის შესახებ“ საქართველოს ორგანული კანონის მე-15 მუხლის პირველი პუნქტის „ზ“ ქვეპუნქტის საფუძველზე:

მუხლი 1

დამტკიცდეს კომერციული ბანკების კიბერუსაფრთხოების მართვის ჩარჩო თანდართული რედაქციით.

მუხლი 2

ეს ბრძანება ამოქმედდეს 2019 წლის 1 აპრილიდან.

ეროვნული ბანკის პრეზიდენტი **კობა გვენეტაძე**

კომერციული ბანკების კიბერუსაფრთხოების მართვის ჩარჩო

მუხლი 1. ზოგადი დებულებები

1. საქართველოში მოქმედ ყველა კომერციულ ბანკს უნდა გააჩნდეს კიბერუსაფრთხოების მართვის ჩარჩო.

2. კიბერუსაფრთხოების მართვის ჩარჩო უნდა იყოს კომერციული ბანკის ზომისა და სირთულის შესაფერისი და შესაბამისობაში უნდა იყოს კომერციული ბანკის მიერ გაწეულ საქმიანობასთან.

3. კიბერუსაფრთხოების მართვის ჩარჩო სრულიად ინტეგრირებული უნდა იყოს კომერციული ბანკის მთლიანი რისკების მართვის პროცესში.

მუხლი 2. კიბერუსაფრთხოების ჩარჩოს კომპონენტები

კიბერუსაფრთხოების მართვის ჩარჩო (შემდგომში – ჩარჩო) უნდა მოიცავდეს შემდეგ ძირითად მიმართულებებს:

ა) რისკის იდენტიფიცირება – კიბერუსაფრთხოების რისკის გათვითცნობიერება კომერციული ბანკის მასშტაბით, რომელიც გულისხმობს კიბერუსაფრთხოების რისკის მართვას. აღნიშნული, თავის მხრივ, მოიცავს კომერციული ბანკის სისტემებთან, აქტივებთან, მონაცემებთან და პროცესებთან დაკავშირებულ კიბერუსაფრთხოების რისკის მართვას;

ბ) დაცვა – კომერციული ბანკის მიერ ადეკვატური კონტროლის გარემოს უზრუნველყოფას, დაინტერესებული მხარეებისთვის გასაწევი მომსახურების მიზნით;

გ) აღმოჩენა – კიბერუსაფრთხოების მოვლენებთან დაკავშირებული აღმოჩენითი მექანიზმების შემუშავება და დანერგვა;

დ) რეაგირება – კიბერუსაფრთხოების მოვლენასთან დაკავშირებული რეაგირების ფორმალიზებული მექანიზმების შემუშავება და ჩამოყალიბება;

ე) აღდგენა – კიბერუსაფრთხოების მოვლენებთან დაკავშირებული ფორმალიზებული აღდგენის გეგმის შემუშავება და ჩამოყალიბება.

მუხლი 3. კიბერუსაფრთხოების რისკის იდენტიფიცირება

კომერციული ბანკის მიერ კიბერუსაფრთხოების რისკის იდენტიფიცირების პროცესი უნდა შედგებოდეს შემდეგი საკითხებისგან/კომპონენტებისგან:

ა) აქტივების მართვა, რომელიც მოიცავს:

ა.ა) კომერციული ბანკის ფიზიკური მოწყობილობების, აპარატურისა და საინფორმაციო სისტემების სრულფასოვან აღრიცხვას;

ა.ბ) პროგრამული უზრუნველყოფისა და აპლიკაციების სრულფასოვან აღრიცხვას;

ა.გ) კომერციულ ბანკში არსებული კომუნიკაციის არხებისა და ინფორმაციული ნაკადების დადგენას, შესწავლასა და ფორმალურ იდენტიფიცირებას;

ა.დ) კომერციული ბანკის მიერ გამოყენებული გარე (მესამე მხარის მიერ წარმოებული) საინფორმაციო სისტემების კატალოგს;

ა.ე) ფორმალიზებულ სისტემას, რომელიც მოიცავს კომერციულ ბანკში არსებული რესურსების კლასიფიკაციას კრიტიკულობისა და ბიზნესპრიორიტეტულობის მიხედვით;

ა.ვ) კომერციული ბანკის ყველა თანამშრომლის როლისა და პასუხისმგებლობების ნათლად და გასაგებად განსაზღვრას კიბერუსაფრთხოების რისკის მართვის ჭრილში;

ა.ზ) მესამე მხარეებთან ურთიერთობებში, მათ შორის, კომერციული ბანკის მიმწოდებლებთან და კლიენტებთან, კიბერუსაფრთხოების როლებისა და პასუხისმგებლობების ნათლად და გასაგებად განსაზღვრას.

ბ) ბიზნესგარემოს, რომელიც მოიცავს:

ბ.ა) კომერციული ბანკის როლის განსაზღვრას ქვეყნის კრიტიკულ ინფრასტრუქტურაში (ასეთის არსებობის შემთხვევაში);

ბ.ბ) კომერციული ბანკის მისიის, მიზნებისა და საქმიანობის ფარგლებში კიბერუსაფრთხოების როლის განსაზღვრას;

ბ.გ) კრიტიკული მომსახურების/პროცესების მიწოდების ფარგლებში დამოკიდებულებებისა და ფუნქციების განსაზღვრას;

ბ.დ) ბიზნესუწყვეტობის მაღალი დონის უზრუნველყოფას კრიტიკული მომსახურების მიწოდების ფარგლებში.

გ) მართვა:

გ.ა) კომერციულ ბანკს უნდა გააჩნდეს ინფორმაციული უსაფრთხოების პოლიტიკა;

გ.ბ) ინფორმაციული უსაფრთხოების ფარგლებში, ყველა როლი და პასუხისმგებლობა შესაბამისობაში უნდა მოვიდეს კომერციულ ბანკში არსებულ თანამშრომელთა შიდა როლებთან და ასევე გარე პარტნიორებთან;

გ.გ) კომერციული ბანკის მიერ სამართლებრივ ჭრილში ნაკისრი ვალდებულებები კიბერუსაფრთხოების სფეროში, მათ შორის, სამოქალაქო თავისუფლების და პირადობის დაცვის თვალსაზრისით, კარგად უნდა იყოს გათვითცნობიერებული კომერციული ბანკის მიერ;

გ.დ) კომერციული ბანკის აღმასრულებელი მმართველობისა და რისკების მართვის პროცესები უნდა მოიცავდეს კიბერუსაფრთხოების რისკს;

გ.ე) კომერციული ბანკის მიერ ახალი ან ინოვაციური პროდუქტების დანერგვის პროცესი უნდა ითვალისწინებდეს კიბერუსაფრთხოების რისკს;

გ.ვ) კომერციული ბანკის მიერ მესამე მხარეების შერჩევის/ურთიერთობის წარმართვის პროცესში კიბერუსაფრთხოების რისკი უნდა იყოს გათვალისწინებული;

დ) კიბერუსაფრთხოების რისკების შეფასება:

დ.ა) კომერციული ბანკის ინფორმაციული აქტივები ფორმალიზებულად უნდა იყოს იდენტიფიცირებული;

დ.ბ) კომერციულმა ბანკმა, საფრთხეების და სისუსტეების შესახებ ინფორმაცია უნდა მიიღოს სხვადასხვა ინფორმაციის გაცვლის წყაროებიდან;

დ.გ) შიდა და გარე საფრთხეები ფორმალურად უნდა იყოს იდენტიფიცირებული;

დ.დ) კიბერუსაფრთხოების მოვლენების პოტენციური ზეგავლენა კომერციულ ბანკზე იდენტიფიცირებული უნდა იყოს;

დ.ე) კომერციული ბანკი უნდა იყენებდეს მეთოდოლოგიას, რომლის მეშვეობითაც ის გამოავლენს საფრთხეებს, სისუსტეებს, ალბათობებსა და ზეგავლენას კიბერუსაფრთხოების რისკის დასადგენად;

დ.ვ) კომერციული ბანკის კიბერუსაფრთხოების რისკის ტოლერანტობა და ზღვარი უნდა შეესაბამებოდეს კომერციული ბანკის როლსა და მნიშვნელობას კრიტიკულ ინფრასტრუქტურაში (ამის არსებობის შემთხვევაში).

მუხლი 4. დაცვა

კომერციული ბანკის მიერ შემუშავებული დაცვის პროცესი უნდა შედგებოდეს შემდეგი საკითხებისგან/კომპონენტებისგან:

ა) წვდომის კონტროლი:

ა.ა) კომერციული ბანკი უნდა ახორციელებდეს ავტორიზებული მომხმარებლებისა და მოწყობილობების სრულფასოვან მართვას;

ა.ბ) კომერციული ბანკის მიერ უნდა ხორციელდებოდეს კუთვნილი ინფორმაციული აქტივების წვდომის მართვა და დაცვა;

ა.გ) კომერციული ბანკი უნდა ახორციელებდეს ფიზიკური წვდომის მართვას, ხელმისაწვდომობასა და კონტროლს;

ა.დ) დისტანციური წვდომა ინფორმაციულ აქტივებზე სრულფასოვნად უნდა იყოს მართული კომერციული ბანკის მიერ;

ა.ე) კომერციული ბანკის მიერ წვდომის უფლებების განსაზღვრა უნდა ხორციელდებოდეს მინიმალური პრივილეგიის პრინციპის დაცვით და მოვალეობების გამიჯვნის პრინციპის შესაბამისად;

ა.ვ) უნდა ხორციელდებოდეს ქსელის მთლიანობის დაცვა, ქსელის გამიჯვნა/დანაწევრების პრინციპის გათვალისწინებით, სადაც ეს შესაძლებელია.

ბ) ცნობიერება და ტრენინგი:

ბ.ა) კომერციული ბანკის მიერ უნდა ხდებოდეს კომერციული ბანკის ყველა რგოლის თანამშრომლის, მათ შორის აღმასრულებელი, საშუალო მენეჯერული და საოპერაციო რგოლების კიბერუსაფრთხოების ტრენინგი, არანაკლებ წელიწადში ერთხელ;

ბ.ბ) კომერციული ბანკის საინფორმაციო სისტემების ყველა მომხმარებელი ინფორმირებული უნდა იყოს კიბერრისკების შესახებ;

ბ.გ) კომერციული ბანკის პრივილეგირებულ მომხმარებლებს გათვითცნობიერებული უნდა ჰქონდეთ საკუთარი როლი და კომერციული ბანკის წინაშე ნაკისრი ვალდებულებები;

ბ.დ) კომერციული ბანკის მესამე მხარეებს გათვითცნობიერებული უნდა ჰქონდეთ კიბერუსაფრთხოების როლები და პასუხისმგებლობები;

ბ.ე) კიბერუსაფრთხოების ფარგლებში, კომერციული ბანკის დირექტორატს გათვითცნობიერებული უნდა ჰქონდეს საკუთარი როლი და ნაკისრი პასუხისმგებლობები;

ბ.ვ) კომერციული ბანკის ფიზიკური და საინფორმაციო უსაფრთხოების თანამშრომლებს კარგად უნდა ჰქონდეთ გათვითცნობიერებული საკუთარი როლები და ნაკისრი პასუხისმგებლობები.

გ) მონაცემთა დაცვა:

გ.ა) კომერციულ ბანკში არსებული სტატიკური მონაცემები უნდა იყოს სათანადოდ დაცული;

გ.ბ) კომერციულ ბანკში არსებული მოძრავი/ტრანზიტული მონაცემები უნდა იყოს სათანადოდ დაცული;

გ.გ) კომერციული ბანკი სრულფასოვნად უნდა მართავდეს ყველა ინფორმაციულ აქტივს (განადგურება, გაგზავნა, შენახვა/განლაგებისას);

გ.დ) კომერციულ ბანკს უნდა გააჩნდეს მონაცემთა კონტროლისა და ინფორმაციის გაჟონვის პრევენციული მექანიზმი;

გ.ე) კომერციულ ბანკს უნდა გააჩნდეს პროგრამული უზრუნველყოფის, მონაცემების/ინფორმაციის მთლიანობის შემოწმების მექანიზმი;

გ.ვ) პროგრამული უზრუნველყოფის ძირითადი და საცდელი გარემო ერთმანეთისგან უნდა იყოს გამიჯნული.

დ) ინფორმაციის დაცვის პროცესები და პროცედურები:

დ.ა) ინფორმაციული ტექნოლოგიების, მათ შორის, საინფორმაციო სისტემების საბაზისო კონფიგურაცია უნდა ჩამოყალიბდეს კომერციული ბანკის მიერ;

დ.ბ) უნდა არსებობდეს სისტემების განვითარების სასიცოცხლო ციკლი;

დ.გ) კომერციულ ბანკს უნდა გააჩნდეს სისტემების კონფიგურაციის ცვლილების მართვის ფორმალური მექანიზმი/პროცესი;

დ.დ) კომერციულ ბანკს უნდა გააჩნდეს მონაცემების/ინფორმაციის დაზღვევა/შენახვის ფორმალიზებული მექანიზმები, რომელიც თავის მხრივ მოიცავს ინფორმაციის აღდგენის პროცესის ტესტირებას;

დ.ე) კომერციულ ბანკში მონაცემები უნდა განადგურდეს კომერციული ბანკის პოლიტიკის შესაბამისად;

დ.ვ) კომერციული ბანკი უნდა ზრუნავდეს ინფორმაციული აქტივების დაცვის პროცესის მუდმივად გაუმჯობესებაზე;

დ.ზ) დაცვითი ტექნოლოგიების ეფექტიანობა რეგულარულად უნდა გაანალიზდეს;

დ.თ) კომერციული ბანკს უნდა გააჩნდეს ინციდენტებზე რეაგირების სრულფასოვანი გეგმა;

დ.ი) კომერციული ბანკი უნდა ახორციელებდეს ინციდენტებზე რეაგირების გეგმის რეგულარულ ტესტირებას;

დ.კ) კომერციულ ბანკს უნდა გააჩნდეს სისუსტეების მართვის გეგმა.

ე) შენარჩუნება:

ე.ა) კომერციული ბანკი უნდა ახორციელებდეს კომერციული ბანკის აქტივების მართვასთან დაკავშირებული ქმედებების დროულ აღრიცხვას, შესაბამისი, დამტკიცებული და აღიარებული პროცესის/ხელსაწყოების მეშვეობით;

ე.ბ) კომერციული ბანკის ინფორმაციული აქტივების დისტანციური მართვა უნდა იყოს ფორმალურად დამტკიცებული, აღრიცხული და განხორციელებული ისე, რომ არაავტორიზებული წვდომა იყოს აღკვეთილი;

ვ) დაცვითი ტექნოლოგიები:

ვ.ა) კომერციულ ბანკს უნდა გააჩნდეს აუდიტის კვალის აღრიცხვის ფორმალიზებული მექანიზმი, რომელიც შეესაბამება კომერციული ბანკის პოლიტიკას;

ვ.ბ) პორტატიული მოწყობილობები დაცული უნდა იყოს და მათი გამოყენება კომერციულ ბანკში უნდა იყოს შეზღუდული კომერციული ბანკის პოლიტიკის შესაბამისად;

ვ.გ) კომერციული ბანკის სისტემებზე და აქტივებზე წვდომა უნდა იყოს ფორმალურად გაკონტროლებული, მინიმალური წვდომის პრინციპის უზრუნველყოფით;

ვ.დ) კომერციული ბანკის კომუნიკაციის და მართვის ქსელი უნდა იყოს დაცული.

მუხლი 5. აღმოჩენა
კომერციული ბანკის მიერ ჩამოყალიბებული კიბერუსაფრთხოების მოვლენების აღმოჩენის პროცესი უნდა შედგებოდეს შემდეგი საკითხებისგან/კომპონენტებისგან:
ა) ანომალიები და მოვლენები:

ა.ა) კომერციულ ბანკში უნდა არსებობდეს საინფორმაციო სისტემებისა და მომხმარებლებთან დაკავშირებული ქსელური ოპერაციებისა და მოსალოდნელი მონაცემთა ნაკადების საბაზისო გარემო;

ა.ბ) კომერციულ ბანკში უნდა ხდებოდეს აღმოჩენილი მოვლენების ანალიზი იმისათვის, რომ მოხდეს პოტენციური კიბერშეტევის სამიზნეებისა და მეთოდების შესწავლა;

ა.გ) უნდა ხორციელდებოდეს კიბერუსაფრთხოების მოვლენებთან დაკავშირებული მოვლენების შეჯამება და პოტენციური კორელირება სხვადასხვა წყაროებთან;

ა.დ) კომერციულ ბანკს უნდა გააჩნდეს ინციდენტის გაფრთხილების მექანიზმები, შესაბამისი რისკის ინდიკატორებისა და სხვა მეტრიკის სახით:

ბ) აღმოჩენითი პროცესები:

ბ.ა) კომერციულ ბანკს უნდა გააჩნდეს კიბერუსაფრთხოების მოვლენის აღმოჩენასთან დაკავშირებული, მკაფიოდ განსაზღვრული როლები და პასუხიმგებლობები;

ბ.ბ) უნდა ხორციელდებოდეს მოვლენის აღმოჩენის პროცესების (მათ შორის შესაბამისი კონტროლების) ტესტირება;

ბ.გ) უნდა ხდებოდეს კონკრეტული მოვლენის აღმოჩენასთან დაკავშირებული ინფორმაციის შეტყობინება შესაბამის პირებთან და უწყებებთან;

ბ.დ) კომერციული ბანკის დირექტორატმა უნდა შეიმუშაოს მსხვილი კიბერუსაფრთხოების მოვლენის შესახებ საქართველოს ეროვნული ბანკისათვის შეტყობინების მექანიზმი;

ბ.ე) მსხვილი კიბერუსაფრთხოების მოვლენის მაღალი ალბათობით მოლოდინის ან დაფიქსირების შემთხვევაში, კომერციული ბანკი ვალდებულია დაუყოვნებლივ აცნობოს აღნიშნულის შესახებ საქართველოს ეროვნულ ბანკს;

ბ.ვ) უნდა ხდებოდეს კომერციული ბანკის მოვლენათა აღმოჩენის პროცესების მუდმივი გაუმჯობესება.

მუხლი 6. რეაგირება
კიბერუსაფრთოხების მოვლენებთან დაკავშირებული რეაგირების პროცესი უნდა შედგებოდეს შემდეგი საკითხებისგან/კომპონენტებისგან:
ა) რეაგირების დაგეგმვა:

ა.ა) კომერციულ ბანკებს უნდა გააჩნდეთ კიბერუსაფრთხოების მოვლენებთან დაკავშირებული ფორმალიზებული რეაგირების გეგმა, რაც თავის მხრივ მოიცავს ორგანიზაციის მზადყოფნას კიბერუსაფრთხოების შესაძლო/მოსალოდნელ რისკთან მიმართებაში;

ა.ბ) რეაგირების გეგმა უნდა ამოქმედდეს კონკრეტული მოვლენის დაფიქსირების დროს ან მოვლენის დაფიქსირების შემდეგ;

ბ) შეტყობინება:

ბ.ა) კომერციული ბანკის თანამშრომლებს კარგად უნდა ჰქონდეთ გათვითცნობიერებული საკუთარი როლი/როლები კიბერუსაფრთხოების მოვლენაზე რეაგირებისას;

ბ.ბ) უნდა ხორციელდებოდეს კიბერუსაფრთხოების მოვლენების შეტყობინება დადგენილი მოთხოვნებისა და კრიტერიუმების შესაბამისად;

ბ.გ) კიბერუსაფრთხოების მოვლენებთან დაკავშირებული ინფორმაციის გაცვლა უნდა ხდებოდეს რეაგირების გეგმის შესაბამისად;

ბ.დ) კიბერუსაფრთოხების მოვლენებთან დაკავშირებული ქმედებების კოორდინირება სხვა უწყებებთან უნდა ხდებოდეს რეაგირების გეგმის შესაბამისად;

გ) ანალიზი:

გ.ა) კომერციული ბანკი უნდა ახორციელებდეს სხვადასხვა სისტემიდან (აღმოჩენითი კონტროლი) მიღებული შეტყობინებების მოკვლევასა და ანალიზს;

გ.ბ) კომერციული ბანკი სრულად უნდა ათვიცნობიერებდეს კიბერუსაფრთხოების ინციდენტის ზეგავლენას კომერციულ ბანკზე;

გ.გ) საჭიროების შემთხვევაში უნდა განხორციელდეს ინციდენტთან დაკავშირებული ექსპერტიზა;

გ.დ) კომერციული ბანკი უნდა ახდენდეს ინციდენტების კლასიფიკაციას, ინციდენტებზე რეაგირების გეგმის შესაბამისად.

დ) მიტიგაცია/შერბილება:

დ.ა) კომერციული ბანკის ვალდებულებაა, რომ მოხდეს კიბერუსაფრთხოების ინციდენტის ზეგავლენის სათანადო შერბილება, თუ ინციდენტი კომერციულ ბანკში დაფიქსირდა;

დ.ბ) კომერციული ბანკი უნდა ახორციელებდეს ახლად აღმოჩენილი სისუსტეების შესწავლას და მოცემული სისუსტეებიდან გამომდინარე საფრთხეების მიტიგაციას ან მიღებას, თუ მოცემული სისუსტე მნიშვნელოვან საფრთხეს არ წარმოადგენს კომერციული ბანკისთვის;

ე) გაუმჯობესება:

ე.ა) კომერციული ბანკის ინციდენტებზე რეაგირების გეგმა უნდა ითვალისწინებდეს წარსულ გამოცდილებასა და პრაქტიკას;

ე.ბ) უნდა ხდებოდეს ინციდენტებზე რეაგირების სტრატეგიის რეგულარული განახლება.

მუხლი 7. აღდგენა

კიბერუსაფრთოხების მოვლენისგან აღდგენის პროცესი უნდა შედგებოდეს შემდეგი საკითხებისგან/კომპონენტებისგან:

ა) კომერციულ ბანკს უნდა გააჩნდეს კიბერუსაფრთხოების მოვლენის შემდეგ ოპერაციების აღდგენის ფორმალური მექანიზმი;

ბ) აღდგენის პროცესი, თავის მხრივ, უნდა ითვალისწინებდეს წარსულში დაფიქსირებული მოვლენებისგან მიღებულ გამოცდილებას;

გ) კომერციულ ბანკს უნდა გააჩნდეს საზოგადოებასთან ურთიერთობის ფორმალური პროცედურა და მექანიზმი, რომლის ფარგლებშიც კომერციული ბანკი უზრუნველყოფს საზოგადოების ინფორმირებას კიბერუსაფრთხოების ინციდენტის დაფიქსირებისას, ამის საჭიროების შემთხვევაში და ასევე რეპუტაციული რისკის მართვას;

დ) კომერციული ბანკი უნდა ახორციელებდეს კონკრეტულ მოვლენასთან დაკავშირებით განხორციელებული ქმედებების შეტყობინებას შიდა დაინტერესებულ მხარეებთან, მათ შორის, კომერციული ბანკის მენეჯმენტთან.

მუხლი 8. კიბერუსაფრთხოების პროგრამის მართვა

1. კომერციული ბანკის მენეჯმენტი ვალდებულია რეგულარულად გადაამოწმოს კომერციული ბანკის კიბერუსაფრთხოების/საინფორმაციო უსაფრთხოების პროგრამის ეფექტიანობა.
2. კომერციულმა ბანკმა ყოველწლიურად უნდა ჩაატაროს კიბერუსაფრთხოებასთან დაკავშირებული თვითშეფასება.

3. კომერციულმა ბანკმა უნდა დაიცვას მსოფლიო ბანკთაშორისი საფინანსო ტელეკომუნიკაციების საზოგადოების (SWIFT) მომხმარებელთა უსაფრთხოების პროგრამის სავალდებულო მოთხოვნები.

4. კომერციული ბანკმა, არანაკლებ წელიწადში ერთხელ, უნდა ჩაატაროს შეღწევადობის ტესტირება, რომელიც მოიცავს კომერციული ბანკის ყველა იმ საინფორმაციო სისტემას, რომელიც ქსელში არის ჩართული.

5. კომერციული ბანკი ვალდებულია ყოველწლიურად ჩაატაროს კომერციული ბანკის კიბერუსაფრთხოების მართვის ჩარჩოს ყველა კომპონენტის დამოუკიდებელი აუდიტი, საინფორმაციო სისტემების რეგულარული აუდიტის ფარგლებში. საინფორმაციო სისტემების აუდიტმა უნდა მოიცვას კონფიდენციალობასთან, მთლიანობასთან და ხელმისაწვდომობასთან დაკავშირებული რისკები.