INTERNATIONAL JOURNAL OF LAW: **"LAW AND WORLD"**
April 2021 (№17). Volume 7; Issue 2; Page No. 148-162
https://doi.org/10.36475/7.2.11
www.lawandworld.ge
ISSN: 2346-7916 (Print); ISSN: 2587-5043 (Online)

NATIONAL CYBERSECURITY SYSTEMS OF LEADING COUNTRIES AROUND THE WORLD

Irakli Nadareishvili
Doctor of Law, Assistant Professor at Caucasus International University, Head of The Department to Investigate Offenses Committed in the Course of Legal Proceedings, The Office of The General Prosecutor of Georgia

Jemal Lomsadze
Master of Law, Senior Prosecutor of The Department to Investigate, Offenses Committed in the Course of Legal Proceedings, The Office of The General Prosecutor of Georgia

ABSTRACT

The rapid development of technology in the 21st century has led to the fact that the geopolitical structure of the modern world depends not only on the strength of armies, but also on the proper functioning of cybersecurity systems. Based on this, the developed countries of the world „compete" with each other in the cyber defense field and taking active offensive measures. Unambiguously the US cybersecurity system has no competitors in the modern world, and the national cybersecurity systems of Great Britain and France are sufficiently effective. For their part, the Russian Federation and China are also actively trying to keep up with the development of modern technologies to meet the requirements and challenges of cyberspace. Every year, the leading countries of the world spend vast amounts of money on the improvement of their cybersecurity systems, as well as on the development of new technologies, which directly indicate the importance of strong cyber systems and the necessity to create a sustainable cybersecurity environment in the world.

KEYWORDS: Cybersecurity Systems, Cybercrime, Hacker, Cyberspace, Virus

BIBLIOGRAPHY:

1. Kokhreidze N., „Russia's Cyber Capabilities" (Research) http://ilawge.blogspot.com/2013/01/blog-post.html (In Georgian)
2. Svanadze V., Gotsiridze A., The main players in cyberspace. Cyber Security Policy, Strategy and Challenges (Collection of Papers and Articles) Tbilisi 2015. http://dspace.nplg.gov.ge/bitstream/1234/144787/1/Kibertavdacva.pdf (In Georgian)
3. Criminal Code of France (22.07.1992) https://www.legislationline.org/download/id/8546/file/France_CC_am012020_fr.pdf (In French)
4. COE Convention on Cybercrime, Budapest, 23.11.2001 http://conventions.coe.int/Treaty/en/Treaties/html/185.htm (In English)
5. Computer Fraud and Abuse Act of 1984, Public Law (18 USC 1030), July 30, 1984 https://www.energy.gov/

sites/prod/files/cioprod/documents/ComputerFraud-AbuseAct.pdf (In English)
6. National Information Infrastructure Protection Act of 1996, Public Law 104-294, 110 Stat. 3491-3494, October 11, 1996 https://www.govinfo.gov/content/pkg/STATUTE-110/pdf/STATUTE-110-Pg3488.pdf (In English)
7. Electronic Communications Privacy Act of 1986 (ECPA), Public law 99–508§, October 21, 1986 https://epic.org/privacy/ecpa/ (In English)
8. Government Communications Headquarters official web-site, mission, cyber-security, 18.03.2021https://www.gchq.gov.uk/section/mission/cyber-security (In English)
9. National Cyber Security Centre, The cyber threat to UK business 2017-2018 report, Crown Copyright, London, 2018 https://www.nationalcrimeagency.gov.uk/who-we-are/publications/178-the-cyber-threat-to-uk-business-2017-18/file (In English)
10. Computer Misuse Act 1990, August 29, 1990 https://www.legislation.gov.uk/ukpga/1990/18/contents (In English)
11. Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (Data Protection Directive), 2016/679, April 26, 2016 https://eur-lex.europa.eu/eli/reg/2016/679/oj (In English)
12. Ministry for Europe and Foreign Affairs official web-site, France and Cyber security (In English) https://www.diplomatie.gouv.fr/en/french-foreign-policy/security-disarmament-and-non-proliferation/fight-against-organized-criminality/cyber-security/
13. French National Cybersecurity Agency, French national digital security strategy, Paris, 2015 (In English) https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf
14. Computer Hygiene Guide, Strengthening the Security of Your Information System in 42 Measures, French National Cybersecurity Agency ANSSI – 51, boulevard de la Tour-Maubourg – Paris, 2017 https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/ (In French)
15. Susan W. Brenner Criminal threats from Cyberspace 2010, (In English) https://books.google.ge/books?id=gsWQ-xgbLbUC&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

მსოფლიოს წამყვანი ქვეყნების კიბერუსაფრთხოების ეროვნული სისტემები

ირაკლი ნადარეიშვილი
სამართლის დოქტორი, კავკასიის საერთაშორისო უნივერსიტეტის ასისტენტ პროფესორი, საქართველოს გენერალური პროკურატურის სამართალწარმოების პროცესში ჩადენილი დანაშაულის გამოძიების დეპარტამენტის უფროსი

ჯემალ ლომსაძე
სამართლის მაგისტრი, საქართველოს გენერალური პროკურატურის სამართალწარმოების პროცესში ჩადენილი დანაშაულის გამოძიების დეპარტამენტის უფროსი პროკურორი

საკვანძო სიტყვები: კიბერუსაფრთხოების სისტემები, კიბერდანაშაული, ჰაკერი, კიბერსივრცე, ვირუსი

შესავალი

XXI საუკუნეში ტექნოლოგიების სწრაფმა განვითარებამ განაპირობა, რომ თანამედროვე მსოფლიოს გეოპოლიტიკური მოწყობა დამოკიდებულია არა მხოლოდ ქვეყნების არმიის სიძლიერეზე, არამედ კიბერუსაფრთხოების სისტემების გამართულ მუშაობაზეც. სწორედ აღნიშნულიდან გამომდინარე, მსოფლიოს განვითარებული ქვეყნები ერთმანეთს „ეჯიბრებიან“ კიბერსფეროში მძლავრი თავდაცვითი სისტემებისა და აქტიური შეტევითი ღონისძიებების გატარებაში. შეიძლება ცალსახად ითქვას, რომ ამერიკის შეერთებული შტატების კიბერუსაფრთხოების სისტემას თანამედროვე მსოფლიოში კონკურენტი არ ჰყავს, ასევე საკმაოდ ეფექტურია გაერთიანებული სამეფოსა

და საფრანგეთის ეროვნული კიბერუსაფრთხოების სისტემები. თავის მხრივ, რუსეთის ფედერაცია და ჩინეთიც აქტიურად ცდილობენ, არ ჩამორჩნენ თანამედროვე ტექნოლოგიების განვითარებას, რათა შეესაბამებოდნენ კიბერსივრცეში არსებულ მოთხოვნებსა და გამოწვევებს. ყოველწლიურად მსოფლიოს წამყვანი ქვეყნები კოლოსალურ თანხებს ხარჯავენ საკუთარი ქვეყნების კიბერუსაფრთხოების სისტემების განვითარების, დახვეწისა და ახალი ტექნოლოგიების შემუშავების მიზნით, რაც პირდაპირ მიანიშნებს აღნიშნული სისტემებისა და მსოფლიოში მყარი კიბერუსაფრთხო გარემოს შექმნის მნიშვნელობაზე.

მსოფლიოს ქვეყნების კიბერუსაფრთხოების ეროვნული სისტემები

ამერიკის შეერთებული შტატები: კიბერდანაშაულის წინააღმდეგ ბრძოლის სტრატეგიის შერჩევისას, ცალსახად მნიშვნელოვანია ისეთი ქვეყნების გამოცდილების გაზიარება, როგორიც არის ამერიკის შეერთებული შტატები, ვინაიდან აღნიშნულ სახელმწიფოში კიბერდანაშაულის წინააღმდეგ ბრძოლის მეთოდოლოგია ათწლეულებს ითვლის.

კომპიუტერული ტექნოლოგიების გამოყენებით ჩადენილი დანაშაულის წინააღმდეგ ბრძოლის მიზნით პირველი სამართლებრივი დოკუმენტი აშშ-ის კონგრესმა 1984 წელს მიიღო და ის ცნობილია „კომპიუტერით თაღლითობისა და მისი ბოროტად გამოყენების შესახებ“ აქტის სახელწოდებით. აღნიშნული სამართლებრივი აქტით, თავდაპირველად გათვალისწინებული იყო სხვადასხვა სახის შეზღუდვები. კერძოდ, იგი ავალდებულებდა საგამოძიებო ორგანოებს, რომ კონკრეტული პირის მიერ კომპიუტერულ სისტემაში ნებისმიერი ფორმით შეღწევის შემთხვევაში, პირველ რიგში, მოეპოვებინათ მტკიცებულება იმის დასადასტურებლად, რომ შეღწევა განხორციელებული იყო უნებართვოდ. აღნიშნული სახის დებულება გამორიცხავდა იმ პირების სისხლისსამართლებრივ პასუხისმგებლობას, რომლებიც თუნდაც ნებართვის სხვადასხვა გზით მოპოვების შემდეგ, ასევე მოიპოვებდნენ სხვა მომხმარებლის კომპიუტერულ მონაცემებს. ხსენებული აქტი არ ითვალისწინებდა სისხლისსამართლებრივ პასუხისმგებლობას ისეთი ქმედებისათვის, როდესაც შეღწევა ხდებოდა კონკრეტული მიზნის გარეშე. 1994 წელს გარკვეული ცვლილებები შევიდა „კომპიუტერით თაღლითობისა და მისი ბოროტად გამოყენების შესახებ“ აქტში, რაც განპირობებული იყო კიბერდამნაშავეების მიერ, სხვისი კომპიუტერული სისტემების დაზიანების მიზნით, სხვადასხვა სახის ვირუსული პროგრამების შექმნით. აღნიშნულ აქტში ცვლილებების შეტანა აუცილებელი იყო, ვინაიდან ძველი რედაქციით ძირითადი აქცენტი გაკეთებული იყო ზოგადად კომპიუტერულ სისტემაში უკანონო შეღწევაზე და საერთოდ არ იყო დარეგულირებული კიბერდამნაშავის მიერ კომპიუტერული სისტემის გამოყენება სხვადასხვა სახის დანაშაულის ჩადენის მიზნით. განხორციელებული საკანონმდებლო ცვლილებების თანახმად, სისხლისსამართლებრივად დასჯადი ქმედება გახდა სხვისი კომპიუტერული სისტემის ან მისი მონაცემების დაზიანების მიზნით, სხვადასხვა სახის მავნე პროგრამის, კოდების ან ინფორმაციის გადაგზავნაც. ასევე სისხლისსამართლებრივი პასუხისმგებლობა განისაზღვრა კომპიუტერული მოწყობილობის მესაკუთრის თანხმობის გარეშე კომპიუტერულ სისტემაში უნებართვო შეღწევისათვის.[1]

აშშ-ის კონგრესმა 1996 წელს დაამტკიცა „ეროვნული ინფორმაციის ინფრასტრუქტურის შესახებ“ აქტი, რომელმაც გარკვეულწილად შეავსო „კომპიუტერით თაღლითობისა და მისი ბოროტად გამოყენების შესახებ“ აქტით განსაზღვრული დებულებები. კერძოდ, აღნიშნული აქტის მიღების შემდეგ სისხლისსამართლებრივი წესით დასჯადი ქმედება გახდა ზოგადად სხვის კომპიუტერულ სისტემაში დაცული ინფორმაციის ნახვა. ახალი აქტის მიღება განაპირობა იმ გარემოებამ, რომ ხშირ შემთხვევაში სხვადასხვა კომპანიების წარმომადგენლები ცდილობდნენ კონკურენტი კომპანიის კომპიუტერულ სისტემაში შეღწევას და მათი კომერციული მიზნებისა თუ საიდუმლოებების გაგებას, რაც ცალკე აღებული არ წარმოადგენდა დანაშაულს, ვინაიდან კომპიუტერულ სისტემაში შემღწევ პირს არ ამოძრავებდა სხვისი კომპიუტერული სისტემის დაზიანების ან ინფორმაციის გადმოტვირთვის განზრახვა.[2]

დღევანდელი მოცემულობით „კომპიუტერით თაღლითობისა და მისი ბოროტად გამოყენების შესახებ“ აქტით განსაზღვრულია სისხლისსამა-

1 Computer Fraud and Abuse Act of 1984, Public Law (18 USC 1030), July 30, 1984 https://www.energy.gov/sites/prod/files/cioprod/documents/ComputerFraud-AbuseAct.pdf

2 National Information Infrastructure Protection Act of 1996, Public Law 104-294, 110 Stat. 3491-3494, October 11, 1996 https://www.govinfo.gov/content/pkg/STATUTE-110/pdf/STATUTE-110-Pg3488.pdf

რთლებრივი პასუხისმგებლობა შვიდი სხვადასხვა სახის კიბერდანაშაულისათვის, კერძოდ: ა) ეროვნული უსაფრთხოების შესახებ ინფორმაციის მიღების მიზნით, ამერიკის შეერთებული შტატების ინტერესების საზიანოდ ან სხვა სახელმწიფოს ინტერესების სასარგებლოდ სხვის კომპიუტერულ სისტემაში უნებართვო შეღწევა; ბ) ფინანსური ან საკრედიტო ინფორმაციის მიღების მიზნით სხვის კომპიუტერულ სისტემაში უნებართვო შეღწევა; გ) ამერიკის შეერთებული შტატების ფედერალური მთავრობის სარგებლობაში არსებულ კომპიუტერულ სისტემაში უნებართვო შეღწევა; დ) თაღლითური ქმედების განხორციელების მიზნით სხვის კომპიუტერულ სისტემაში უნებართვო შეღწევა; ე) სხვისი კომპიუტერული სისტემის განზრახ დაზიანება სხვადასხვა კიბერტექნოლოგიების გამოყენებით; ვ) სხვისი კომპიუტერული მონაცემებით უკანონო ვაჭრობა, რომელიც შესაძლოა გამოყენებული იქნას კომპიუტერულ სისტემაში უნებართვო შეღწევის მიზნით; ზ) სხვისი კომპიუტერული სისტემის მიმართ განხორციელებული მუქარა, ფულის ან სხვა ფასეულობის გამოძალვის მიზნით.

„ელექტრონული კომუნიკაციების კონფიდენციალურობის შესახებ“ აქტი აშშ-ში მიიღეს 1986 წელს და აღნიშნული აქტით ცვლილება შევიდა „მოსმენების შესახებ“ ფედერალურ კანონში. კერძოდ, აღნიშნული აქტით სამართალდამცავ ორგანოებს შეეზღუდათ უფლებამოსილება და აეკრძალათ შესაბამისი ნებართვის გარეშე მოეპოვებინათ ელექტრონული კომუნიკაციის შედეგად გადაგზავნილი ან დაგროვილი ინფორმაცია. ზემოაღნიშნული აქტით ცალსახად განისაზღვრა, რომ სამართალდამცავ ორგანოებს არ ჰქონდათ უფლება, მოეთხოვათ ინტერნეტმომსახურების პროვაიდერებისგან ელექტრონული კომუნიკაციების შემცველი მასალის გადაცემა, შესაბამისი სამართლებრივი პროცედურების გავლის გარეშე.[3] ზემოხსენებულ აქტში 1994 წელს შევიდა ცვლილება, რომლის თანახმადაც ინტერნეტმომსახურების პროვაიდერებს დაეკისრათ ვალდებულება ელექტრონული კომუნიკაციის შედეგად დაგროვილი ინფორმაციების გარკვეული ვადით შენახვის შესახებ. აღნიშნული სახის ცვლილება განპირობებული იყო საგამოძიებო მოქმედებათა გარკვეულ ვადებში ჩატარების ინტერესებით. 2002 წელს ამერიკის შეერთებულ შტატებში „სახელმწიფო უსაფრთხოების შესახებ“ აქტთან ერთად მიიღეს „კიბერუსაფრთხოების გაუმჯობესების შესახებ“ აქტიც, რომლითაც უფლებამოსილებები გაეზარდათ სამართალდამცავ ორგანოებს და ასევე გაიზარდა სანქციები „კომპიუტერით თაღლითობისა და მისი ბოროტად გამოყენების შესახებ“ აქტით განსაზღვრული დანაშაულების ჩადენისათვის.

„ელექტრონული კომუნიკაციების კონფიდენციალურობის შესახებ“ აქტის თანახმად, სასამართლოს ნებართვის გარეშე ინტერნეტმომსახურების პროვაიდერებს აკრძალული ჰქონდათ მათი მომხმარებლების ელექტრონული კომუნიკაციის ამსახველი ინფორმაციის გადაცემა სამართალდამცავი ორგანოებისათვის. „კიბერუსაფრთხოების გაუმჯობესების შესახებ“ აქტით შემცირდა აღნიშნული კატეგორიის ინფორმაციის კონფიდენციალურობის ხარისხი და ინტერნეტმომსახურების პროვაიდერებს მიენიჭათ (სასამართლოს მიერ გაცემული სათანადო ნებართვის გარეშე) მომხმარებელთა ელექტრონული კომუნიკაციის ამსახველი ინფორმაციის სახელმწიფოს შესაბამის წარმომადგენელთათვის გადაცემის უფლებამოსილება იმ შემთხვევაში, თუ იარსებებდა საფუძვლიანი ეჭვი, რომ აღნიშნული ინფორმაცია შეიცავდა მძიმე კატეგორიის დანაშაულის ნიშნებს.

არსებული საკანონმდებლო რეგულაციების ფონზე, გამოყოფენ ამერიკის შეერთებული შტატების კიბერუსაფრთხოების სამსაფეხურიან სისტემას, სადაც პირველი საფეხური ფედერალური დონის სახელმწიფო უწყებებს უკავიათ, კერძოდ:

- აშშ-ის თავდაცვის სამინისტრო – აღნიშნული უწყების დაქვემდებარებაშია „ეროვნული უსაფრთხოების სააგენტო“ (National Security Agency, NSA). აღნიშნული სააგენტო კიბერუსაფრთხოების სფეროში აქცენტებს აკეთებს შეიარაღებული ძალების მიზნებსა და ამოცანებზე. სააგენტოში დასაქმებულია დაახლოებით 120 000 სპეციალისტი და მისი წლიური ბიუჯეტი 3,5-დან 13 მლრდ დოლარამდე მერყეობს;
- აშშ-ის შიდა უსაფრთხოების სამინისტრო – (Department of Homeland Security, DHS). აღნიშნული სამინისტროს სისტემაში შედის „კიბერუსაფრთხოებისა და კომუნიკაციების ოფისი“ (Office of Cyber Security and Communications) და მისი წლიური ბიუჯეტი დაახლოებით 400 000 000 აშშ დოლარს შეადგენს;
- აშშ-ის იუსტიციის დეპარტამენტი – აღნიშნული დეპარტამენტის შემადგენლობაში შემავალი „გამოძიების ფედერალური ბიუროს“ ერთ-ერთი ქვედანაყოფია „ეროვ-

3 Electronic Communications Privacy Act of 1986 (ECPA), Public law 99–508§, October 21, 1986 https://epic.org/privacy/ecpa/

ნული კიბერ საგამოძიებო ჯგუფი“ (National Cyber Investigative Joint Task Force, NCIJTF). აღნიშნული საგამოძიებო ჯგუფის ძირითად მიზანს წარმოადგენს ქვეყნის შიგნით მომხდარი კიბერდანაშაულის გამოძიება.

ამერიკის შეერთებული შტატების კიბერუსაფრთხოების სისტემის მეორე საფეხური შედგება ექვსი სტრუქტურული ქვედანაყოფისგან: 1. კომპიუტერული უსაფრთხოების ინციდენტებზე რეაგირების ჯგუფი (United States Computer Emergency Response Team, US-CERT); 2. კიბერუსაფრთხოების ეროვნული ცენტრი (National Cyber Security Division, NCSD); 3. კიბერდანაშაულთან ბრძოლის ცენტრი (Cyber Crimes Center); 4. კიბერსაფრთხეების საოპერაციო ცენტრი (NSA/CSS Threat Operations Center, NTOC); 5. შეიარაღებული ძალების კიბერხელმძღვანელობა – (United States Cyber Command, USDCYBERCOM); 6. სადაზვერვო სამსახური – ინციდენტებზე რეაგირების ცენტრი.

ზემოთ ჩამოთვლილ სტრუქტურულ ქვედანაყოფებს სხვადასხვა სახის ამოცანები და მიზნები აქვთ. აღნიშნული სტრუქტურები ორიენტირებულნი არიან როგორც კიბერშეტევების შედეგად დამდგარი შედეგების ლიკვიდაციაზე, ასევე მიზნად ისახავენ კიბერსაფრთხეების პრევენციისთვის აუცილებელი ღონისძიებების გატარებას, ამასთანავე ახდენენ კიბერშეტევების ორგანიზებას. ამერიკის შეერთებული შტატების კიბერუსაფრთხოების სისტემის მესამე საფეხურს შეადგენენ სხვადასხვა რეგიონალური სტრუქტურული ქვედანაყოფები, რომლებსაც, თავის მხრივ, ზედამხედველობას უწევენ ზემოთ ჩამოთვლილი უწყებები.

კიბერუსაფრთხოების საკითხის აქტუალურობიდან გამომდინარე, 2015 წლის თებერვალში აშ-შ-ის პრეზიდენტის ადმინისტრაციამ მიიღო გადაწყვეტილება, რომ ქვეყნის ეროვნული დაზვერვის დირექტორის დაქვემდებარებაში შექმნილიყო ახალი სპეციალური სამსახური – „კიბერსაფრთხეებზე სადაზვერვო მონაცემების ინტეგრაციის ცენტრი“ (Cyber Threat Intelligence Integration Center, CTIIC). აღნიშნული უწყების ამოცანას წარმოადგენს ზემოთ მითითებული პირველი საფეხურის უწყებებიდან, სახელმწიფო სტრუქტურებიდან და კერძო სექტორიდან მიღებული სადაზვერვო მონაცემების შეგროვება, მათი ანალიზი და შესაბამისი რეკომენდაციების გაცემა.

გაერთიანებული სამეფო: გაერთიანებულ სამეფოს კიბერუსაფრთხოებას უზრუნველყოფს სპეციალური სამსახური GCHQ (Government Communications Headquarters), მთავრობის კომუნიკაციების შტაბი. ეს არის დიდი ბრიტანეთის სიგნალების დაზვერვის სამსახური, რომელიც აგროვებს და აანალიზებს ციფრულ და ელექტრონულ სიგნალებს მსოფლიოს ყველა კუთხიდან. აღნიშნული სამსახური აგრეთვე შეიმუშავებს რჩევებს და მითითებებს, თუ როგორ უნდა იქნას დაცული მონაცემები, კომუნიკაციები და ინფორმაციული სისტემები ჰაკერებისგან და სხვა საფრთხეებისგან.

ბრიტანული სიგნალების დაზვერვა დაარსდა 1914 წლის აგვისტოში, პირველი მსოფლიო ომის დაწყების შემდეგ. პირველი მსოფლიო ომის მიმდინარეობისას აღნიშნული სამსახურის მიერ მოპოვებულ იქნა არაერთი მნიშვნელოვანი ინფორმაცია მოწინააღმდეგის გეგმების თაობაზე. 1919 წელს, აღნიშნული ორგანიზაციის წარმატებული საქმიანობის გაგრძელების მიზნით შეიქმნა მშვიდობიანი დროის კრიპტო-ანალიტიკური დანაყოფი. თავდაპირველად აღნიშნულ სამსახურს ეწოდებოდა კოდირების და დაშიფვრის სახელმწიფო სკოლა, შემდგომში კი დაერქვა მთავრობის კომუნიკაციების შტაბი. აღნიშნულმა უწყებამ წარმატებული საქმიანობა მეორე მსოფლიო ომის პერიოდშიც გააგრძელა. შემდგომში, ტექნოლოგიურ პროგრესთან ერთად, მოხდა უწყების შესაძლებლობების ადაპტაცია თანამედროვეობის ახალ გამოწვევებთან გამკლავების მიზნით. დღეის მდგომარეობით, მთავრობის კომუნიკაციების შტაბის მთავარი სამუშაო მიმართულებებია: ტერორიზმთან ბრძოლა, კიბერუსაფრთხოება, სტრატეგიული უპირატესობა, ორგანიზებულ დანაშაულთან ბრძოლა და თავდაცვის მხარდაჭერა. 2016 წელს მთავრობის კომუნიკაციების შტაბში შეიქმნა კიბერუსაფრთხოების ეროვნული ცენტრი (National Cyber Security Centre (NCSC)), რომლის მთავარი ამოცანა გაერთიანებული სამეფოს კიბერუსაფრთხოების უზრუნველყოფაა. აღნიშნული ცენტრი უზრუნველყოფს გაერთიანებული სამეფოს სტრატეგიულად მნიშვნელოვანი უწყებების დაცულობას კიბერთავდასხმებისგან, მართავს მნიშვნელოვან შემთხვევებს და ტექნოლოგიური გაუმჯობესებისა და რეკომენდაციების შემუშავების გზით, ამაღლებს ბრიტანული ინტერნეტის უსაფრთხოების დონეს. კიბერუსაფრთხოების ეროვნული ცენტრი ახორციელებს გაერთიანებული სამეფოს სტრატეგიულად მნიშვნელოვანი უწყებების, საჯარო სექტორის, ინდუსტრიის, საშუალო და მცირე მეწარმეობის მხარდაჭერას; უზრუნველყოფს შემთხვევებზე მყისიერ და ეფექტიან რეაგირებას შესაძლო ზიანის მინიმუმამდე დაყვანის მიზნით და მონაწილეობს მიყენებული ზიანის აღმოფხვრის პროცესში.

კოვიდ 19-ის პანდემიის პირობებში, NCSC-ის მთავარი პრიორიტეტი გახდა ჯანდაცვის სექტორის უსაფრთხოების გაძლიერება. აგრეთვე საკმაოდ დიდი მხარდაჭერა გაეწია პანდემიის პირობებში სახლიდან მომუშავე ორგანიზაციებსა და ბიზნესს. გასული წლის აპრილში გამოიცა „კიბერ ინფორმირებულობა“, გაერთიანებული სამეფოს მთავრობის რჩევები ონლაინ რეჟიმში უსაფრთხოების დაცვის საკითხებზე. ამავე დროს, აღნიშნული სამსახურის მიერ დაინერგა სრულიად ახალი, საექვო ელ. ფოსტის შესახებ შეტყობინების სერვისი, რომლის საშუალებითაც შესაძლებელი გახდა საექვო გზავნილის გადამისამართება სპეციალურად ამისთვის შექმნილ საფოსტო მისამართზე (report@phishing.gov.uk). მომსახურების ამოქმედებიდან პირველ ორ თვეში, აღნიშნულ მისამართზე შევიდა ორ მილიონზე მეტი შეტყობინება, შედეგად გამოვლინდა 9000-მდე თაღლითური სქემა და 22 000 პოტენციურად ზიანის მომტანი ვებგვერდი.[4]

გაერთიანებულ სამეფოში კიბერდანაშაულთან ბრძოლაში აქტიურ როლს თამაშობს დანაშაულთან ბრძოლის ეროვნული სააგენტო (NCA – National Crime Agency). აღნიშნული უწყება სათავეში უდგას ბრძოლას მძიმე და ორგანიზებული დანაშაულის შემცირების მიზნით. ქვეყნისთვის დიდი საფრთხის მატარებელი კრიმინალური სამყაროს წარმომადგენლების სისხლისსამართლებრივი დევნისა და პასუხისგებაში მიცემის გზით, უწყება უზრუნველყოფს საზოგადოების დაცულობას. სააგენტოს მონაცემებით, ორგანიზებული დანაშაული, მათ შორის კიბერდანაშაული, გაერთიანებული სამეფოსთვის წარმოადგენს ერთ-ერთ ყველაზე მნიშვნელოვან გამოწვევას, რომლის შედეგადაც წლიური ზიანის ოდენობა 37 მილიარდ ფუნტს აღწევს. კიბერდანაშაულის კუთხით ძირითად საფრთხეს გაერთიანებული სამეფოსთვის წარმოადგენენ რუსულენოვანი კიბერჯგუფები, თუმცა ყოველდღიურად მატულობს საფრთხე ადგილობრივი კიბერკრიმინალების მხრიდანაც.[5]

გაერთიანებული სამეფოში, კარგად განვითარებულ პრეცედენტულ სამართალთან ერთად, კიბერდანაშაულთან ბრძოლისთვის 1990 წელს მიღებულ იქნა „აქტი კომპიუტერის ბოროტად გამოყენების შესახებ“, რომლითაც გათვალისწინებულია პასუხისმგებლობა კომპიუტერულ სისტემასთან დაკავშირებული მთელი რიგი ქმედებისთვის, მათ შორისაა:

1. კომპიუტერულ მასალებთან არასანქცირებული (არამართლზომიერი) წვდომა.

2. კომპიუტერულ სისტემაში უნებართვო შეღწევა, შემდგომში დანაშაულებრივი ქმედების განხორციელების, ან მისი გაადვილების მიზნით.

3. უნებართვო, განზრახი ან გაუფრთხილებელი ქმედებები, მიმართული კომპიუტერული სისტემის მუშაობის გაუარესებისკენ, ანდა მის დასაზიანებლად, რაც ხელს უშლის კომპიუტერის გამართულად მუშაობას და ა.შ.

3ZA. უნებართვო ქმედებები, რომლებიც სერიოზულ ზიანს აყენებს ან ქმნის ასეთი ზიანის წარმოშობის რისკს.

3A. ზემოაღნიშნულ პუნქტებში ჩამოთვლილი ქმედებების ჩასადენად გამოსაყენებელი ნივთების დამზადება, მომარაგება ან მიღება (შეძენა).

ამავე აქტში გაწერილია კომპიუტერულ დანაშაულთან დაკავშირებით არსებული მიდგომები, პროცედურები და ძირითადი პრინციპები (ტერიტორიულობის, მოქალაქეობის და ა.შ.).[6]

2018 წლის მაისში, გაერთიანებულ სამეფოში, რომელიც იმჟამად ევროკავშირის წევრ ქვეყანას წარმოადგენდა, ამოქმედდა ახალი „მონაცემთა დაცვის ზოგადი რეგულაცია“ ((EU) 2016/679), რომელიც მიმართულია ევროკავშირის წევრი ქვეყნების კიბერუსაფრთხოების ამაღლებისკენ. აღნიშნული რეგულაციის თანახმად ორგანიზაციებს ეკისრებათ ვალდებულება, შეატყობინონ შესაბამის ზედამხედველ ორგანოს, ინფორმაციის კომისრის სამსახურს, მონაცემთა სისტემაში ნებისმიერი შეღწევის შესახებ, რამაც შეიძლება საფრთხე შეუქმნას ინდივიდების უფლებებსა და თავისუფლებებს. ცალკეულ შემთხვევებში, როდესაც არსებობს მაღალი რისკი, რომ კონკრეტული პირის ინტერესები შეიძლება დაზიანდეს, შესაბამის უწყებას ევალება აღნიშნული პირის ინფორმირება. აღნიშნული შეტყობინება უნდა განხორციელდეს ფაქტის გამოვლენიდან 72 საათში, გადაუდებლად. ფაქტზე გამოძიების მიმდინარეობა არ ათავისუფლებს ორგანიზაციას შეტყობინების განხორციელების მოვალეობისგან. გარდა ზემოაღნიშნულისა, ორგანიზაციებს ევალებათ პრევენციული სამუშაოების გატარებაც,

4 Government Communications Headquarters official website, mission, cyber-security, 18.03.2021 https://www.gchq.gov.uk/section/mission/cyber-security

5 National Cyber Security Centre, The cyber threat to UK business 2017-2018 report, Crown Copyright, London, 2018 https://www.nationalcrimeagency.gov.uk/who-we-are/publications/178-the-cyber-threat-to-uk-business-2017-18/file

6 Computer Misuse Act 1990, 29 August 1990 https://www.legislation.gov.uk/ukpga/1990/18/contents

როგორიცაა რისკების შეფასება და სათანადო უსაფრთხოების ზომების უზრუნველყოფა. მათ აგრეთვე ეკისრებათ ყველა შესაძლო შემთხვევის სწრაფი გამოვლენისა და რეაგირების მოხდენის ვალდებულება, რასთან დაკავშირებითაც უნდა არსებობდეს შესაბამისი გეგმა. მაქსიმალურად უნდა იყოს უზრუნველყოფილი ბიზნესის უწყვეტობის გარანტიები.[7]

საფრანგეთი: 2015 წელს საფრანგეთმა დაამტკიცა ეროვნული კიბერუსაფრთხოების სტრატეგია. აღნიშნული სტრატეგიის მთავარი მიზანი ფრანგული საზოგადოების ციფრულ ტექნოლოგიაზე უსაფრთხოდ გადასვლის უზრუნველყოფა და ახალ გამოწვევებთან გამკლავებაა. სტრატეგიის თანახმად, ხუთ ძირითად მიზნად სახელდება:

1. ეროვნული სუვერენიტეტის უზრუნველყოფა; 2. კიბერდანაშაულის ქმედებებზე ძლიერი რეაგირება; 3. საზოგადოების ინფორმირება; 4. ფრანგული ბიზნესისთვის ციფრული უსაფრთხოების კონკურენტულ უპირატესობად ქცევა; 5. საფრანგეთის ავტორიტეტის ამაღლება საერთაშორისო დონეზე.

2017 წელს, საფრანგეთის ევროპისა და საგარეო საქმეთა სამინისტრომ წარმოადგინა საფრანგეთის საერთაშორისო ციფრული სტრატეგია. მასში ასახულია საფრანგეთის ყველა სტრატეგიული მიზანი ციფრულ სფეროში, რაც დაკავშირებულია ხელისუფლების სამივე შტოსთან, ეკონომიკასთან და უსაფრთხოებასთან. 2018 წელს, პრემიერ მინისტრის დავალებით, საფრანგეთის თავდაცვისა და ეროვნული უსაფრთხოების გენერალურმა სამდივნომ, წარმოადგინა კიბერ თავდაცვის სტრატეგიული მიმოხილვა. მასში ასახულია კიბერ კრიზისების მართვის დოქტრინა. ეს მიმოხილვა განმარტავს კიბერთავდაცვის ეროვნული სტრატეგიის მიზნებს და ადასტურებს ფრანგული მოდელის შესაბამისობას დადგენილ სტანდარტებთან, აგრეთვე მთავრობის პასუხისმგებლობას ამ სფეროში.[8]

საფრანგეთში კიბერუსაფრთხოების საკითხი არ განიხილება ცალკე აღებულად და ის ეროვნული უსაფრთხოების განუყოფელ ასპექტად მოიაზრება. საფრანგეთის ეროვნული უსაფრთხოების კოდექსის L111 მუხლის პირველი ნაწილი ადგენს, რომ სახელმწიფო ვალდებულია შეინარჩუნოს უსაფრთხოება. აღნიშნული ვრცელდება კიბერსივრცეზეც. როგორც ზემოთ უკვე აღვნიშნეთ, ამ სფეროში საფრანგეთს შემუშავებული აქვს კონკრეტული სტრატეგიები, თუმცა აქვე გამოვყოფთ რამდენიმე მნიშვნელოვან სამართლებრივ აქტს, ესენია:

- 2018 წლის სამხედრო პროგრამირების აქტი (მოიცავს 2019 წლიდან, 2025 წლამდე პერიოდს). აქტის მიხედვით სახელმწიფოს ეკისრება ვალდებულება და პასუხისმგებლობა გაატაროს შესაბამისი ზომები, რათა უზრუნველყოფილ იქნეს „სახელმწიფოსთვის სასიცოცხლოდ მნიშვნელოვანი“ დარგების უსაფრთხოება, როგორიცაა ბანკები, საავადმყოფოები და ატომური სადგურები. აღნიშნულ აქტში კიბერთავდაცვას ცალკე თავი ეძღვნება;
- ევროკავშირის მონაცემთა დაცვის ზოგადი რეგულაციის ძალაში შესვლამდე (2018 წლის 25 მაისი), 1978 წლიდან, საფრანგეთში მოქმედებდა მონაცემთა დაცვის კანონი, რომლის 34-ე და 34-ე BIS მუხლები ეძღვნებოდა კიბერუსაფრთხოებას. კანონის მიხედვით, პერსონალური მონაცემების დამუშავებისას, კერძო თუ საჯარო სტრუქტურამ უნდა გაატაროს ტექნიკური და ორგანიზაციული ზომები, რათა მონაცემთა დამუშავებისას უზრუნველყოს უსაფრთხოების შესაბამისი დონე, მათ შორის, მოიაზრება არასანქცირებული შეღწევისგან, მონაცემთა ქურდობისგან და გაყალბებისგან დაცვა. ამასთანავე ინტერნეტის პროვაიდერებს, რომლებსაც უწევთ პერსონალური მონაცემების დამუშავება, ეკისრებათ მოვალეობა, სისტემაში უნებართვო შეღწევის ფაქტის გამოვლენისას, აღნიშნული დაუყოვნებლივ შეატყობინონ ინფორმატიკისა და თავისუფლებების ეროვნულ კომისიას (Commission nationale de l'informatique et des libertés). გარდა ამისა, ინტერნეტის პროვაიდერებს ეკისრებათ ვალდებულება, შეინახონ ინფორმაცია თითოეულ ინციდენტზე. 2018 წლის ევროკავშირის მონაცემთა დაცვის ზოგადი რეგულაციით, შეტყობინების გაგზავნის ვალდებულება გავრცელდა ყველა უწყებაზე, საჯაროსა თუ კერძოზე, რომელიც ახდენს მონაცემების დამუშავებას. 1978 წლის მონაცემთა დაცვის კანონით, სათანადო ღო-

7 Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (Data Protection Directive), 2016/679, 26 April 2016 https://eur-lex.europa.eu/eli/reg/2016/679/oj

8 Ministry for Europe and Foreign Affairs official web-site, France and Cyber security https://www.diplomatie.gouv.fr/en/french-foreign-policy/security-disarmament-and-non-proliferation/fight-against-organized-criminality/cyber-security/

ნისძიებების გაუტარებლობის შემთხვევაში მონაცემთა დამმუშავებელი ჯარიმდებოდა სამი მილიონი ევროს ოდენობის ჯარიმით. ახალი რეგულაციით, უსაფრთხოების სათანადო ზომების გაუტარებლობის, ან ინფორმაციის სათანადო უწყებისთვის მიუწოდებლობის შემთხვევაში, მონაცემთა დამმუშავებელი, ადმინისტრაციული წესით დაჯარიმდება წინა ფინანსური წლის მთლიანი წლიური ბრუნვის 2 პროცენტამდე ოდენობის ჯარიმით ან 10 მილიონი ევროთი, იმისდა მიხედვით, თუ რომელი იქნება უფრო მეტი. 2018 წლის 21 ივნისის N2018-493 კანონით, საფრანგეთმა მოახდინა ევროკავშირის მონაცემთა დაცვის ზოგადი რეგულაციის იმპლემენტაცია თავის კანონმდებლობაში.

გარდა ამისა, საფრანგეთის სისხლის სამართლის კოდექსის 226-17 მუხლის თანახმად, ზემოაღნიშნული სამართალდამრღვევების გამოვლენის შემთხვევაში, პირს შეიძლება დაეკისროს სისხლისსამართლებრივი პასუხისმგებლობა და დაენიშნოს ხუთ წლამდე ვადით თავისუფლების აღკვეთა და ჯარიმა 300,000 ევრომდე. ამავე კოდექსის 131-38-ე მუხლის შესაბამისად ჯარიმის თანხა ხუთმაგდება იურიდიული პირის შემთხვევაში.

- ევროკავშირის 2016 წლის 6 ივლისის ქსელისა და ინფორმაციის უსაფრთხოების შესახებ დირექტივა (NIS), რომელიც აგრეთვე იმპლემენტირებულ იქნა საფრანგეთის კანონმდებლობაში.[9]

ცალკე ყურადღებას იმსახურებს საფრანგეთის ეროვნული საინფორმაციო სისტემების უსაფრთხოების სააგენტო (იგივე კიბერუსაფრთხოების ეროვნული სააგენტო), რომელიც შეიქმნა 2009 წლის 7 ივლისს. აღნიშნული სამთავრობო სააგენტო ექვემდებარება საფრანგეთის თავდაცვისა და ეროვნული უსაფრთხოების გენერალური მდივნის სამსახურს. სააგენტოს მთავარი მიზანი არსებული საკანონმდებლო რეგულაციების სწორად გატარებისა და საინფორმაციო სისტემების დაცულობის უზრუნველყოფაა.

2017 წლის სექტემბერში, სააგენტომ რეკომენდაციის სახით გამოაქვეყნა 42 ღონისძიების ჩამონათვალი, რაც უნდა გატარდეს, რათა უზრუნველყოფილ იქნეს მონაცემების და IT სისტემების დაცულობა კიბერსაფრთხეებისგან. რეკომენდაციის მიხედვით კიბერუსაფრთხოება სერიოზულ ყურადღებას იმსახურებს და სხვა ღონისძიებებთან ერთად კომპანიებმა და ორგანიზაციებმა უნდა უზრუნველყონ:

1. ცნობიერების ამაღლება; 2. სისტემების რეგულარული განახლება; 3. მონაცემთან წვდომის მაქსიმალური შეზღუდვა და ავტორიზაციის მძლავრი მექანიზმის გამოყენება; 4. აუდიტის ჩატარება; 5. ინფორმაციის გადაცემისას მონაცემების დაშიფვრა; 6. ქსელის დეცენტრალიზება.

საფრანგეთმა დანერგა საუკეთესო პრაქტიკა და პროცედურები ელექტრონულ სისტემაში უნებართვო შეღწევებთან საბრძოლველად და ზიანის გამოსწორების პროცესის სამართავად. ინფორმატიკისა და თავისუფლებების ეროვნულმა კომისიამ და საფრანგეთის კიბერუსაფრთხოების ეროვნული სააგენტომ ერთობლივად შეიმუშავეს არაერთი რეკომენდაცია და ქცევის პროტოკოლი, რომელიც შესასრულებლად სავალდებულოა არსებითი მნიშვნელობის მქონე დაწესებულებებისთვის.

სისტემაში უნებართვო შეღწევის თაობაზე ეჭვის არსებობისას, პირველ რიგში, რეკომენდებულია აღნიშნული შემოწმდეს ე.წ. „მასპინძელზე“ (Host – მასპინძელი, მომსახურების გამწევი კომპანია, რომელიც უზრუნველყოფს თავის სერვერზე კლიენტის ფაილების განთავსებას და შენახვას) დაფუძნებული შეტევების გამოვლენის სისტემისა და უშუალოდ ქსელზე დაფუძნებული შეტევების გამოვლენის სისტემის მეშვეობით, რათა რეალურ დროში იდენტიფიცირებულ იქნეს საფრთხე და დადგინდეს შეტევის მოცულობა.

შეღწევის გამოვლენის შემთხვევაში, ორგანიზაციამ უნდა: 1. უზრუნველყოს დაინფიცირებული IT სისტემის გათიშვა ქსელიდან; 2. ამის შესახებ აცნობოს ადგილობრივ კომპიუტერულ სიტუაციებზე რეაგირების საგანგებო ჯგუფს; 3. უზრუნველყოს მონაცემების ასლის შენახვა მყარ მეხსიერების ბარათზე; 4. შეაგროვოს და შეინახოს მტკიცებულებები და მოძებნოს ციფრული კვალი; 5. საჩივრით მიმართოს პოლიციას.

არსებითი მნიშვნელობის მატარებელმა ორგანიზაციებმა ელექტრონულ სისტემაში შეღწევის თაობაზე უნდა შეატყობინონ უშუალოდ საფრანგეთის კიბერუსაფრთხოების ეროვნული სააგენტოს. კერძო და საჯარო მონაცემთა მაკონტროლებლებმა და დამმუშავებლებმა შეტყობინება უნდა გაუგზავნონ ინფორმატიკისა და თავისუფლებების ეროვნულმა კომისიას. კიბერთავდასხმის შემთხვევაში, ფაქტის სათანადოდ შესწავლისა და სათანადო რეაგირების მიზნით, ორგანიზაციებმა უნდა: 1. მოიკვლიონ

9 French National Cybersecurity Agency, French national digital security strategy, Paris, 2015 https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf

ოპერაციული სისტემასა და ოპერაციული სისტემის ფაილებში შეტანილი ნებისმიერი ცვლილება; 2. გააანალიზონ, მოხდა თუ არა მონაცემთა შეცვლა ან მოდიფიცირება; 3. მოიძიონ ნებისმიერი მონაცემი ან ინსტრუმენტი, რომელიც შესაძლოა გამოიყენა ჰაკერმა; 4. მოახდინონ ჟურნალების ანალიზი; 5. ქსელში მოძებნონ ნებისმიერი ე.წ. „სნიფერი“ (Sniffer არის პროგრამული უზრუნველყოფა ან აპარატურა, რომელიც მომხმარებელს საშუალებას აძლევს რეალურ დროში მიიღოს ან დააკვირდეს თქვენს ინტერნეტ ტრაფიკს, აიღოს ყველა მონაცემები, რომლებიც მიედინება თქვენს კომპიუტერში და მისგან); 6. შეამოწმონ ნებისმიერი სხვა ქსელი თუ მოწყობილობა, რომელიც დაკავშირებულია დაზარალებულ ქსელთან.[10]

1988 წლიდან დღემდე, საფრანგეთის სისხლის სამართლის კოდექსში აისახა არაერთი ნორმა, რომელიც შეეხება კიბერდანაშაულის საკმაოდ ფართო წრეს. შეგვიძლია ცალკე გამოვყოთ შემდეგი ქმედებები:

- საინფორმაციო სისტემაზე ნებისმიერი კიბერთავდასხმა უნებართვო შეღწევის ან ტექნიკური საშუალებების გამოყენების გზით, ისჯება 60,000 ევრომდე ოდენობით ჯარიმით ან ორ წლამდე ვადით თავისუფლების აღკვეთით (იურიდიული პირისთვის ჯარიმის ოდენობა ხუთმაგდება);
- თუკი რომელიმე ზემოაღნიშნულმა ქმედებამ გამოიწვია სისტემაში შენახული ინფორმაციის დაზიანება, შეცვლა ან განადგურება, ან სხვა მხრივ შეეშალა ხელი სისტემის გამართულად ფუნქციონირებას, აღნიშნული ჩაითვლება ცალკე დანაშაულად, რომლისთვისაც სანქციის სახით გათვალისწინებულია 100,000 ევრომდე ოდენობით ჯარიმა (იურიდიული პირის შემთხვევაში ჯარიმის თანხა ხუთმაგდება) ან/და თავისუფლების აღკვეთა სამ წლამდე ვადით;
- სახელმწიფოს მიერ კონტროლირებულ საინფორმაციო სისტემაზე თავდასხმა ისჯება 150,000 ევრომდე ოდენობით ჯარიმით (იურიდიული პირის შემთხვევაში ჯარიმის თანხა ხუთმაგდება) და თავისუფლების აღკვეთით ხუთ წლამდე ვადით;
- ნებისმიერი კიბერშეტევა, რომელიც არღვევს ან აფერხებს ინფორმაციული სისტემის გამართულ მუშაობას, ისჯება 150,000 ევრომდე ოდენობით ჯარიმით (იურიდიული პირის შემთხვევაში ჯარიმის თანხა ხუთმაგდება) ან/და თავისუფლების აღკვეთით ხუთ წლამდე ვადით. თუკი იგივე შედეგი დადგა სახელმწიფოს მიერ კონტროლირებულ საინფორმაციო სისტემასთან მიმართებით, ქმედებისთვის ჯარიმის სახით გათვალისწინებულია 300,000 ევრომდე ოდენობით ჯარიმა (იურიდიული პირის შემთხვევაში ჯარიმის თანხა ხუთმაგდება) ან/და თავისუფლების აღკვეთა შვიდ წლამდე ვადით;
- ინფორმაციული სისტემის მონაცემების დანერგვა, მოპოვება, კლონირება, გადაცემა, შეცვლა ან წაშლა (იგივე სანქცია, რაც ზემოაღნიშნული ქმედებისთვისაა გათვალისწინებული);
- ნებისმიერი მოწყობილობის, პროგრამული უზრუნველყოფის ან სხვა ინსტრუმენტის იმპორტი, გასაღება ან ფლობა, რომელიც შემუშავებულია კიბერ კრიმინალური საქმიანობის განსახორციელებლად, ექვემდებარება იმავე სასჯელს, როგორც თავად ქმედება, რომლისთვისაც ის გამოიყენება, იმისდა მიხედვით, თუ რომელი სასჯელი უფრო მძიმეა.
- კიბერ კრიმინალური საქმიანობის ორგანიზებული განხორციელება ისჯება იმავე სასჯელით, როგორც თავად ქმედება, რომლისთვისაც ის ხორციელდება, იმისდა მიხედვით, თუ რომელი სასჯელი უფრო მძიმეა. თუმცა იგივე ქმედება, ჩადენილი სახელმწიფოს მიერ კონტროლირებული საინფორმაციო სისტემის წინააღმდეგ, ისჯება 300,000 ევრომდე ოდენობით ჯარიმით (იურიდიული პირის შემთხვევაში ჯარიმის თანხა ხუთმაგდება) ან/და თავისუფლების აღკვეთით 10 წლამდე ვადით (აღნიშნული დანაშაულის მცდელობის შემთხვევაში გამოიყენება იგივე სანქცია, რაც კონკრეტული ქმედებისთვის არის გათვალისწინებული);
- პირადი მონაცემების უკანონო შეგროვება, გამოყენება, შენახვა, გადაცემა და დამუშავება, აგრეთვე უსაფრთხოების ვალდებულებების შეუსრულებლობა ისჯება 300,000 ევრომდე ოდენობით ჯარიმით (იურიდიული პირის შემთხვევაში ჯარიმის თანხა ხუთმაგდება) ან/და თავისუფლების აღკვეთით 5 წლამდე ვადით.
- სხვა პირად წარმოდგენა ან „ვინაობის ქუ-

10 Guide d'hygiène informatique renforcer la sécurité de son système d'information en 42 mesures, ANSSI – 51, boulevard de la Tour-Maubourg – 75700, Paris, 2017 https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/

რდობა“ ისჯება ერთ წლამდე ვადით პატიმრობით ან/და 15,000 ევრომდე ოდენობით ჯარიმით (იურიდიული პირის შემთხვევაში ჯარიმის თანხა ხუთმაგდება);

- თაღლითობა საკრედიტო ან სადებეტო ბარათის მეშვეობით ისჯება შვიდ წლამდე ვადით პატიმრობით ან/და 750,000 ევრომდე ოდენობით ჯარიმით (იურიდიული პირის შემთხვევაში ჯარიმის თანხა ხუთმაგდება). იგივე სასჯელია გათვალისწინებული ზემოაღნიშნული ქმედების ჩასადენად საჭირო მოწყობილობის, პროგრამული უზრუნველყოფის ან სხვა ინსტრუმენტის იმპორტისთვის, გასაღებისთვის ან ფლობისთვის;
- კიბერთაღლითობები, როგორიცაა ე.წ. „ფიშინგი“, ისჯება ხუთ წლამდე ვადით პატიმრობით ან/და 375,000 ევრომდე ოდენობით ჯარიმით (იურიდიული პირის შემთხვევაში ჯარიმის თანხა ხუთმაგდება);
- ნდობის დარღვევა, რაც გამოწვეულია ინფორმაციულ სისტემაში შეღწევის გზით, ისჯება სამ წლამდე ვადით პატიმრობით ან/და 375,000 ევრომდე ოდენობით ჯარიმით (იურიდიული პირის შემთხვევაში ჯარიმის თანხა ხუთმაგდება).

გარდა ზემოაღნიშნული ქმედებების ინკრიმინირებისა, კიბერდანაშაულებთან ეფექტიანი ბრძოლის მიზნით, კანონმდებელმა გააძლიერა და გააფართოვა პოლიციის საგამოძიებო უფლებამოსილებები და შექმნა სპეციალიზებული კიბერდანაშაულის სასამართლოები. ამასთანავე, კიბერდანაშაულთან საბრძოლველად, ამოქმედდა სპეციალიზებული ინტერნეტგვერდი, სადაც მოქალაქეებს შეუძლიათ დანაშაულის თაობაზე შეტყობინებების განთავსება და რეკომენდაციების გაცნობა (www.cert.ssi.gouv.fr).[11]

ჩინეთის სახალხო რესპუბლიკა: ჩინეთში არსებული სახელმწიფო პოლიტიკური წყობიდან გამომდინარე, აღნიშნული ქვეყანა კიბერუსაფრთხოების სისტემებს აერთიანებს სამხედრო უწყებებში. ჩინეთში კიბერუსაფრთხოების განვითარების სტრატეგია და სისტემის შექმნა დაიწყო 2002 წლიდან. ჩინეთის სახელმწიფოს მიერ მიღებული გეგმის თანახმად, კიბერუსაფრთხოების სტრატეგია უნდა გამხდარიყო ერთიანი „ეროვნული სამხედრო სტრატეგიის“ (Military Strategic Guidelines) ნაწილი. სტრატეგიის შემუშავება და მისი რეალიზაცია დაევალა გენერალური შტაბის ორ სტრუქტურას – მესამე და მეოთხე სამმართველოებს. მესამე სამმართველოს ძირითად ფუნქციას წარმოადგენს კიბერსივრცეში სადაზვერვო სამუშაოების წარმოება და ჩინეთის სახალხო-განმანთავისუფლებელი არმიის უსაფრთხოებაზე ზრუნვა. რაც შეეხება მეოთხე სამმართველოს, მის ფუნქციაში შედის კიბერსივრცეში შეტევითი და პრევენციული ტიპის ოპერაციების დაგეგმვა და განხორციელება. კიბერუსაფრთხოებაზე ჩინეთში ამჟამად პასუხისმგებელია ცენტრალური სამხედრო საბჭო, სადაც შედიან როგორც უშიშროების სამინისტროს, ისე მეცნიერებათა და ტექნოლოგიათა სამინისტროს წარმომადგენლები. 2017 წლის 01 ივნისს ჩინეთში მიღებული იქნა კანონი კიბერუსაფრთხოების შესახებ. ეროვნული უსაფრთხოების პოლიტიკიდან გამომდინარე, კანონის შექმნის ძირითადი მოტივი გახდა კიბერსუვერენიტეტის დაცვა გარე ფაქტორებისგან. ამ კუთხით გამკაცრდა სახელმწიფოს კონტროლი ინტერნეტსივრცეში არსებულ ბიზნეს საქმიანობებზეც. შემუშავებული სტრატეგიის თანახმად შეიქმნა ე.წ. „ოქროს ფარი“, რომლის ძირითად ფუნქციას ინტერნეტ კონტენტების ფილტრაცია, გარე ჩარევებისაგან კომპ. სისტემების დაცვა და ინფორმაციაზე წვდომის შეზღუდვა წარმოადგენს. ფაქტობრივად, იგი ერთგვარი კონტროლისა და ცენზურის ელ. სისტემაა. უნდა აღინიშნოს, რომ საჯარო სივრცეში ინფორმაცია ჩინეთის კიბერუსაფრთხოების სისტემების შესახებ საკმაოდ მწირია.

რუსეთის ფედერაცია: რუსეთის ფედერაციის კიბერუსაფრთხოების სისტემა გარკვეულწილად ჩინეთის მოდელს არის მიმსგავსებული. სხვადასხვა სპეცსამსახურებში შექმნილია სპეციალიზებული სტრუქტურები, რომლებიც აქტიურად მოქმედებენ კიბერსფეროში. ამერიკელი ანალიტიკოსების აზრით, რუსეთიდან მომდინარე კიბერშეტევების საფრთხე პრიორიტეტულია. მიუხედავად აღნიშნულისა, კიბერუსაფრთხოების სფეროში დოქტრინალური კუთხით რუსეთის ფედერაციის ჩამორჩენა აშკარაა, ვინაიდან მას არ აქვს შემუშავებული სისტემის განვითარების კონცეფცია. სტრატეგიის შემუშავების კუთხით პირველი ნაბიჯების გადადგმა რუსეთის ფედერაციაში დაიწყო 2012-2013 წლებში, როდესაც რუსეთის ფედერაციის პრეზიდენტმა დაავალა უსაფრთხოების ფედერალურ სამსახურს საინფორმაციო ტექნოლოგიებზე კიბერშეტევების აღმოჩენის, გაფრთხილების და შედეგების ლიკვიდაციის სისტემის ჩამოყალიბება. 2012 წელს დაანონსდა შეიარაღებულ ძალებში შეერთებული შტატების ანალოგიური

11 საფრანგეთის სისხლის სამართლის კოდექსი, Code pénal (22.07.1992) https://www.legislationline.org/download/id/8546/file/France_CC_am012020_fr.pdf

(U.S.CYBERCOM) „კიბერ სარდლობის“ შექმნა, რაც პრაქტიკულად ნიშნავდა ინფორმაციული უსაფრთხოების საკითხებში სპეციალურ სამსახურებზე დომინირებას. 2014 წლის იანვარში, რუსეთის ფედერალურმა საბჭომ ფართო განხილვისათვის წარმოადგინა „რუსეთის ფედერაციის კიბერუსაფრთხოების სტრატეგიის კონცეფცია“, რომელიც ექსპერტთა აზრით ვერ აკმაყოფილებდა მოთხოვნებს და აზრთა სხვადასხვაობა გამოიწვია. მიუხედავად თავდაცვის სამინისტროს შემადგენლობაში გარკვეული დანაყოფის ჩამოყალიბებისა, რუსეთში ძირითადი ფუნქცია კიბერუსაფრთხოების კუთხით, რუსეთის სპეციალური სამსახურებს (ФСБ, ФСО და ФСТЭК) აკისრიათ (ყველას თავისი სტრუქტურული დანაყოფი ჰყავს) და ერთიანი ცენტრალიზებული მმართველობა ამ სფეროში არ არსებობს.

მიუხედავად არაცენტრალიზებულობისა, Defensetech.org-ის მონაცემების თანახმად, რუსეთი საკუთარი კიბერშესაძლებლობებით მსოფლიოში მეოთხე-მეხუთე ადგილს იკავებს. მას გააჩნია სპეციალიზებული სახელმწიფო სტრუქტურები, რომლებიც კიბერდაზვერვასა და კონტრდაზვერვას ეწევიან. ერთ-ერთი მათგანი FAPSI შეიქმნა 1991 წელს და დღემდე ფედერალური სააგენტოს ნაწილია. „FAPSI საკმაოდ დახურული ორგანიზაციაა, რომელიც მუშაობს რადიოელექტრონულ დაზვერვებზე. FAPSI პირდაპირ ექვემდებარება პრეზიდენტს და მისი თანამშრომელთა რაოდენობა აღემატება ფედერალური უსაფრთხოების სააგენტოს ე.წ. „ეფ-ეს-ბე“-ს თანამშრომელთა რიცხვს, რაც იმაზე მეტყველებს, რომ აღნიშნულ სააგენტოს, სახელმწიფო უსაფრთხოების მხრივ, უდიდესი მნიშვნელობა ენიჭება. კანონის თანახმად, FAPSI-ის ძირითად მოვალეობებში შედის სამთავრობო ქსელების მომსახურება, სახელმწიფო საიდუმლოების შენახვისათვის ხელშეწყობა და რუსეთიდან მომდინარე დაშიფრული კომუნიკაციების უსაფრთხოება. რუსეთის სამხედრო დანაყოფები იყენებენ FAPSI-ს, რათა ებრძოლონ სამთავრობო და სამხედრო მასალებთან არასანქცირებულ შეღწევებს. მათი ძირითადი მიზანია მოიპოვონ უპირატესობა ინფორმაციის დამუშავებაში და ელექტრონული ომისათვის აუცილებელი სისტემების ცოდნაში.“[12] 2007-2008 წლების მონაცემებით რუსეთის ე.წ. „კიბერ არმია“ 7000 წევრს ითვლიდა, თუმცა გონივრული იქნება ვივარაუდოთ, რომ დღეის მონაცემებით, მათი რაოდენობა და შესაძლებლობლები მნიშვნელოვნად გაზრდილია.

ყოველივე ზემოაღნიშნულიდან გამომდინარე, შესაძლებელია ცალსახად ითქვას, რომ კიბერდანაშაული არის სწორედ XXI საუკუნის გამოწვევა თანამედროვე მსოფლიოსთვის. იგი ფაქტიურად ერთადერთი დანაშაულებრივი მიმართულებაა, რომელიც ვითარდება ყოველდღიურად და მის შესაჩერებლად აუცილებელია უზარმაზარი ადამიანური და მატერიალური რესურსის მობილიზება, ახალი უსაფრთხოების სისტემების დანერგვა და სწორი კიბერუსაფრთხოების პოლიტიკის გატარება. ბოლოდროინდელი ტენდენციები მიანიშნებს, რომ მომავალში კიბერსივრცე კიდევ უფრო მასშტაბური გახდება, რაც გამოიწვევს სახელმწიფო სტრუქტურების მეტად დამოკიდებულებას ინფორმაციულ ტექნოლოგიებზე, ხოლო აღნიშნული კი გახდება ახალი რისკებისა და საფრთხეების წარმოქმნის საფუძველი. ამდენად აუცილებელია კიბერუსაფრთხოების ისეთი მოქნილი სისტემებისა და მექანიზმების შექმნა, რომლებიც ეფექტურად უპასუხებენ ახალ გამოწვევებსა და პოტენციურ საფრთხეებს.

12 კოხრეიძე ნ., „რუსეთის კიბერ შესაძლებლობები“ (კვლევა) http://ilawge.blogspot.com/2013/01/blog-post.html

ბიბლიოგრაფია:

1. კოხრეიძე ნ., „რუსეთის კიბერშესაძლებლობები“ (კვლევა) http://ilawge.blogspot.com/2013/01/blog-post.html
2. სვანაძე ვ., გოცირიძე ა., კიბერსივრცის მთავარი მოთამაშეები. კიბერუსაფრთხოების პოლიტიკა, სტრატეგია და გამოწვევები (ნაშრომების და სტატიების კრებული). თბილისი, 2015 წ. http://dspace.nplg.gov.ge/bitstream/1234/144787/1/Kibertavdacva.pdf
3. საფრანგეთის სისხლის სამართლის კოდექსი, Code pénal (22.07.1992) https://www.legislationline.org/download/id/8546/file/France_CC_am012020_fr.pdf
4. ევროპის კავშირის კონვენცია კიბერდანაშაულის შესახებ, http://conventions.coe.int/Treaty/en/Treaties/html/185.htm

5. Computer Fraud and Abuse Act of 1984, Public Law (18 USC 1030), July 30, 1984 https://www.energy.gov/sites/prod/files/cioprod/documents/ComputerFraud-AbuseAct.pdf
6. National Information Infrastructure Protection Act of 1996, Public Law 104-294, 110 Stat. 3491-3494, October 11, 1996 https://www.govinfo.gov/content/pkg/STATUTE-110/pdf/STATUTE-110-Pg3488.pdf
7. Electronic Communications Privacy Act of 1986 (ECPA), Public law 99–508§, October 21, 1986 https://epic.org/privacy/ecpa/
8. Government Communications Headquarters official web-site, mission, cyber-security, 18.03.2021 https://www.gchq.gov.uk/section/mission/cyber-security
9. National Cyber Security Centre, The cyber threat to UK business 2017-2018 report, Crown Copyright, London, 2018 https://www.nationalcrimeagency.gov.uk/who-we-are/publications/178-the-cyber-threat-to-uk-business-2017-18/file
10. Computer Misuse Act 1990, August 29, 1990 https://www.legislation.gov.uk/ukpga/1990/18/contents
11. Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (Data Protection Directive), 2016/679, April 26, 2016 https://eur-lex.europa.eu/eli/reg/2016/679/oj
12. Ministry for Europe and Foreign Affairs official web-site, France and Cyber security https://www.diplomatie.gouv.fr/en/french-foreign-policy/security-disarmament-and-non-proliferation/fight-against-organized-criminality/cyber-security/
13. French National Cybersecurity Agency, French national digital security strategy, Paris, 2015 https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf
14. Guide d'hygiène informatique renforcer la sécurité de son système d'information en 42 mesures, ANSSI – 51, boulevard de la Tour-Maubourg – 75700, Paris, 2017 https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/
15. Susan W. Brenner Criminal threats from Cyberspace 2010, https://books.google.ge/books?id=gsWQ-xgbLbUC&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false