Scientific and Practical Cyber Security Journal (SPCSJ) 8(4): 157 – 163 ISSN 2587-4667
Scientific Cyber Security Association (SCSA)

CYBERSECURITY VS INFORMATION SECURITY

Ketiladze Dachi[1]
[1]JSG "TBC Insurance"

კიბერუსაფრთხოების მეცნიერება VS ინფორმაციული უსაფრთხოების დარგი

კეთილაძე დაჩი[1]
[1]სს „თიბისი დაზღვევა"

ABSTRACT: Some Georgian information security professionals, even those with international certifications, incorrectly claim that 'cybersecurity is part of information security.' This misplaces cybersecurity within the realm of information security, rather than recognizing it as a separate field of IT security. Such a viewpoint is clearly unprofessional and subjective. This study seeks to elevate understanding of information security, particularly among both experienced and novice professionals. It clearly delineates and substantiates the differences between information security and cybersecurity.

KEYWORDS*:* Cybersecurity, security awareness, information security, IT security, digital security

ანოტაცია: საქართველოში, ინფორმაციული უსაფრთხოების სფეროს, მათ შორის საერთაშორისო სერტიფიცირებების მქონე სპეციალისტების ნაწილი თვლის, რომ ციტატა: „კიბერუსაფრთხოება ინფორმაციული უსაფრთხოების შემადგენელი ნაწილია". აშკარაა, რომ ისინი კიბერუსაფრთხოების მეცნიერებას ინფორმაციული უსაფრთხოების დარგის დაფარვის ზონაში მოიაზრებენ, და არა ზოგადად, ინფორმაციული უსაფრთხოების (IT უსაფრთხოების) სფეროს ქვეშ, - რაც გახლავთ არაპროფესიონალური და სუბიექტური შეფასება. მოცემული კვლევა ორიენტირებულია ცნობიერების დონის ამაღლებაზე როგორც ინფორმაციული უსაფრთხოების სფეროს სპეციალისტებს შორის, ასევე დამწყებ სპეციალისტებშიც. ის მკაფიოდ განმარტავს და ქვემოთ მოყვანილი, მყარი, დასაბუთებული არგუმენტებით ასაბუთებს ინფორმაციული უსაფრთხოების დარგსა და კიბერუსაფრთხოების მეცნიერებას შორის განსხვავებას.

საკვანძო სიტყვები: კიბერუსაფრთხოება, უსაფრთხოების ცნობიერების ამაღლება, ინფორმაციული უსაფრთხოება, IT უსაფრთხოება, ციფრული უსაფრთხოება

შესავალი:

ინფორმაციული უსაფრთხოების დარგის დეფინიცია: „ინფორმაციული უსაფრთხოება გულისხმობს ინფორმაციისა და საინფორმაციო სისტემების დაცვას არასანქცირებული წვდომის, გამოყენების, გამჟღავნების, შეცვლის ან/და განადგურებისგან, - კონფიდენციალურობის, მთლიანობისა და ხელმისაწვდომობის უზრუნველყოფის მიზნით". (nist n.d.)
კიბერუსაფრთხოების მეცნიერების დეფინიცია: „კიბერუსაფრთხოება არის ქსელების, მოწყობილობებისა და მონაცემების დაცვის მეცნიერება არასანქცირებული წვდომისა და დანაშაულებრივი გამოყენებისაგან, ასევე ინფორმაციის კონფიდენციალურობის, მთლიანობისა და ხელმისაწვდომობის უზრუნველყოფის პრაქტიკა". (cisa 2021)
ტერმინი „ინფორმაციული უსაფრთხოება" გამოიყენება როგორც ინფორმაციული უსაფრთხოების სფეროს, ასევე ინფორმაციული უსაფრთხოების დარგის

განმარტებისთვისაც. სხვა სიტყვებით რომ ვთქვათ, ერთი და იგივე ტერმინი „ინფორმაციული უსაფრთხოება“ გამოიყენება როგორც ზოგადად სფეროს განმარტება (იგივე IT უსაფრთხოება), ასევე, ინფორმაციული უსაფრთხოების დარგის - როგორც ინფორმაციული უსაფრთხოების სფეროს ადმინისტრაციული მიმართულების დარგის აღნიშთვისთვისაც.

ეს გახლავთ ამოსავალი წერტილი, რომელიც ინფორმაციული უსაფრთხოების სფეროს წარმომადგენელთა ნაწილისთვის ჰბადებს გაუგებრობას იქიდან გამომდინარე, რომ არცერთ ოფიციალურ, საერთაშორისო სტანდარტში, დეფინიციის დონეზე არ არსებობს მკაფიო ზღვარი ამ ორ ცნებას შორის და ინფორმაციული უსაფრთხოების დარგს, როგორც ასეთი, საკუთარი დასახელება არ გააჩნია, თუმცა სხვაგვარადაა მკაფიოდ გამიჯნული კიბერუსაფრთხოების მეცნიერებისაგან.

ამის შედეგად საქართველოში, ზოგიერთი, როგორც წესი - ინფორმაციული უსაფრთხოების დარგის სპეციალისტი თვლის, რომ ციტატა „კიბერუსაფრთხოება ინფორმაციული უსაფრთხოების შემადგენელი ნაწილია“, და რაც მთავარია, გულისხმობენ ინფორმაციული უსაფრთხოების დარგს და არა ზოგადად, ინფორმაციული უსაფრთხოების (IT უსაფრთხოების) სფეროს. სხვა სიტყვებით რომ ვთქვათ, კიბერუსაფრთხოების მეცნიერებას ინფორმაციული უსაფრთხოების დარგის დაფარვის ზონაში განიხილავენ და ვერ ანსხვავებენ ერთმანეთისგან, რაც თავისთავად არ შეესაბამება ობიექტურ რეალობას.

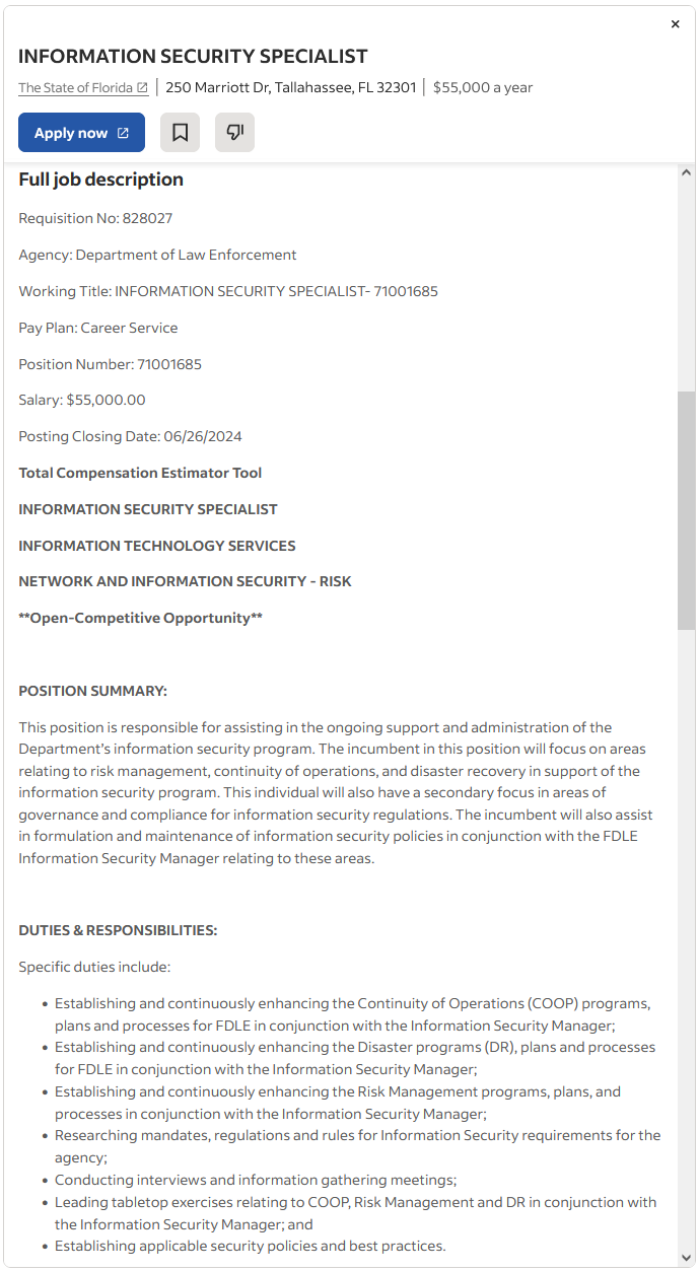
სწორი პასუხია - ინფორმაციული უსაფრთხოების დარგი და კიბერუსაფრთხოების მეცნიერება შედიან ინფორმაციული უსაფრთხოების (IT უსაფრთხოების) სფეროს დაფარვის ზონაში და ამის უამრავი ფაქტი და მტკიცე არგუმენტი არსებობს, ასე მაგალითად:

1. არცერთ საერთაშორისოდ აღიარებულ ან/და ოფიციალურ სტანდარტში არ არსებობს დეფინიცია ან/და განმარტება, რომელიც ადგენს ან/და განსაზღვრავს, რომ კიბერუსაფრთხოების მეცნიერება ინფორმაციული უსაფრთხოების დარგის შემადგენელი ნაწილია;
2. უფრო მეტიც, საერთაშორისოდ აღიარებული ინფორმაციული უსაფრთხოების სტანდარტში „ISO/IEC 27001“ სათაურშივე გამოკვეთილად გამიჯნულია ინფორმაციული უსაფრთხოების დარგი და კიბერუსაფრთხოების მეცნიერება. დამატებით, სათაურშივე, თავისთავად ცალკეა გატანილი ასევე პრივატულობის ცნება, რომელიც ნაწილობრივ იკვეთება ინფორმაციული უსაფრთხოების სფეროსთან, მაგრამ ასევე სცილდება მის ფარგლებს (ისევე, როგორც კიბერუსაფრთხოების მეცნიერება ნაწილობრივ იკვეთება, მაგრამ სცილდება ინფორმაციული უსაფრთხოების დარგის ფარგლებს): (ISO/IEC 2022)
3. ზემოთხსენებულს კიდევ ერთხელ ადასტურებს ის ფაქტიც, რომ პირობითად, თუ არსებობს “ISO/IEC 27001:2022”, რომელიც აუცილებელი ფორმით ადგენს ინფორმაციული უსაფრთხოების მართვის სისტემების შექმნის, დანერგვის, მხარდაჭერისა და მუდმივი გაუმჯობესების მოთხოვნებს, ასევე არსებობს „ISO/IEC 27032:2023 Cybersecurity“, რომელიც გახლავთ კიბერუსაფრთხოების მეცნიერების სახელმძღვანელო, რომელიც მოცემულ დოკუმენტში ფოკუსირებულია ინტერნეტის უსაფრთხოების უნიკალურ ასპექტებზე და მის კავშირზე ინფორმაციის უსაფრთხოებასთან, ქსელურ უსაფრთხოებასთან და კრიტიკული ინფრასტრუქტურის დაცვაზე. (ISO n.d.)
4. კიდევ ერთი ფაქტი და უტყუარი არგუმენტია ისიც, რომ ღია წყაროების ანალიზის მეთოდი (OSINT) (Gill 2023) და ე.წ. “Threat Intelligence” (IBM, https://www.ibm.com n.d.) - აბსოლუტურად სცდებიან ინფორმაციული უსაფრთხოების დარგის ფარგლებს და ამავდროულად წარმოადგენენ კიბერუსაფრთხოების მეცნიერების განუყოფელ ნაწილს.

5. კიდევ ერთ მაგალითად შეიძლება მოვიყვანოთ ინფორმაციული უსაფრთხოების სფეროს, საერთაშორისოდ აღიარებული სერთიფიცირების მქონე აკადემიების სასწავლო კურსები, მათი დასახელებები და მათში მოცემული სასწავლო მასალების განსხვავებები.
განვიხილოთ საერთაშორისოდ ცნობილი და აღიარებული ორგანიზაცია "EC-Council", რომლის მიერ გაცემულ სერტიფიკატებსაც გააჩნია საერთაშორისო აღიარება ინფორმაციული უსაფრთხოების სფეროში, როგორც ინფორმაციული უსაფრთხოების დარგის, ასევე კიბერუსაფრთხოების მეცნიერების მიმართულებებით.
შედარებისთვის, დავადაროთ მისი ორი, დამოუკიდებელი სასერტიფიკატო კურსი:
"Certified Cybersecurity Technician" (C|CT)
ქართულად - „კიბერუსაფრთხოების სერთიფიცირებული სპეციალისტი / ტექნიკოსი "
სასწავლო მასალაში შემავალი საკითხები:
მოდული 01: ინფორმაციული უსაფრთხოების საფრთხეები და დაუცველობა
მოდული 02: ინფორმაციული უსაფრთხოების თავდასხმები
მოდული 03: ქსელის უსაფრთხოების საფუძვლები
მოდული 04: იდენტიფიკაცია, ავთენტიფიკაცია და ავტორიზაცია
მოდული 05: ქსელის უსაფრთხოების კონტროლი - ადმინისტრაციული კონტროლი
მოდული 06: ქსელის უსაფრთხოების კონტროლი - ფიზიკური კონტროლი
მოდული 07: ქსელის უსაფრთხოების კონტროლი - ტექნიკური კონტროლი
მოდული 08: ქსელის უსაფრთხოების შეფასების ტექნიკა და ინსტრუმენტები
მოდული 09: აპლიკაციის უსაფრთხოება
მოდული 10: ვირტუალიზაცია და ღრუბლოვანი ინფრასტრუქტურა
მოდული 11: უსადენო ქსელის უსაფრთხოება
მოდული 12: მობილური მოწყობილობის უსაფრთხოება
მოდული 13: „IoT" (IBM, https://www.ibm.com n.d.) და „OT" ტიპის მოწყობილობების (NIST n.d.)უსაფრთხოება
მოდული 14: კრიპტოგრაფია
მოდული 15: მონაცემთა უსაფრთხოება
მოდული 16: ქსელის პრობლემების მოგვარება
მოდული 17: ქსელური ნაკადის მონიტორინგი
მოდული 18: ქსელის ჟურნალების მონიტორინგი და ანალიზი
მოდული 19: ინციდენტზე რეაგირება
მოდული 20: კიბერ ექსპერტიზა
მოდული 21: ბიზნესის უწყვეტობა და კატასტროფის აღდგენა (cisco თ. გ.)
მოდული 22: რისკების მართვა
(eccouncil 2024)

"Chief Certified Information Security Officer" (C|CISO)
ქართულად - „ინფორმაციული უსაფრთხოების სერთიფიცირებული უფროსი ოფიცერი"
სასწავლო მასალაში შემავალი საკითხები:
დომენი 1: მმართველობა, რისკი, შესაბამისობა
დომენი 2: ინფორმაციის უსაფრთხოების კონტროლი და აუდიტის მართვა
დომენი 3: უსაფრთხოების პროგრამის მართვა და ოპერაციები
დომენი 4: ინფორმაციის უსაფრთხოების ძირითადი კომპეტენციები
დომენი 5: სტრატეგიული დაგეგმვა, ფინანსები, შესყიდვები და მესამე მხარის მართვა
(https://www.eccouncil.org 2024)
აშკარაა, რომ როგორც მოცემული სასერტიფიკატო კურსის დასახელებები, ასევე სასწავლო მასალებში შემავალი საკითხების აბსოლუტური უმრავლესობა მკვეთრად

განსხვავებულია და ორივე შემთხვევაში მკაფიოდაა გამოკვეთილი შესაბამისი დარგისა თუ მეცნიერებისთვის საჭირო და მნიშვნელოვანი პროფესიული სპეციფიკა და აქცენტები.
6. თუ გადავხედავთ საერთაშორისოდ აღიარებულ სტანდარტებთან შესაბამისობაში მყოფ და მსოფლიოს წამყვანი ორგანიზაციებისა თუ ქვეყნების სახელმწიფო სტრუქტურული ერთეულების მიერ გამოქვეყნებულ ვაკანსიებს, - შევამჩნევთ, რომ აქაც მკაფიოდაა გამოკვეთილი ინფორმაციული უსაფრთხოების დარგის ან/და კიბერუსაფრთხოების მეცნიერების სპეციალისტების წინაშე წაყენებული, სპეციფიური ცოდნისა და გამოცდილების შესაბამისი მოთხოვნები და პასუხისმგებლობები.
ასე მაგალითად, შეგვიძლია განვიხილოთ დასაქმების საერთაშორისო ონლაინ პლატფორმაზე “Indeed”-ზე გამოქვეყნებული ორი დამოუკიდებელი ვაკანსია, - ინფორმაციული უსაფრთხოების დარგის სპეციალისტისა და კიბერუსაფრთხოების მეცნიერების სპეციალისტის პოზიციაზე და შევადაროთ ერთმანეთს მათ წინაშე წაყენებული სპეციფიური მოთხოვნები და პასუხისმგებლობები:



INFORMATION SECURITY SPECIALIST

The State of Florida | 250 Marriott Dr, Tallahassee, FL 32301 | $55,000 a year

Apply now

Full job description

Requisition No: 828027

Agency: Department of Law Enforcement

Working Title: INFORMATION SECURITY SPECIALIST- 71001685

Pay Plan: Career Service

Position Number: 71001685

Salary: $55,000.00

Posting Closing Date: 06/26/2024

Total Compensation Estimator Tool

INFORMATION SECURITY SPECIALIST

INFORMATION TECHNOLOGY SERVICES

NETWORK AND INFORMATION SECURITY - RISK

****Open-Competitive Opportunity****

POSITION SUMMARY:

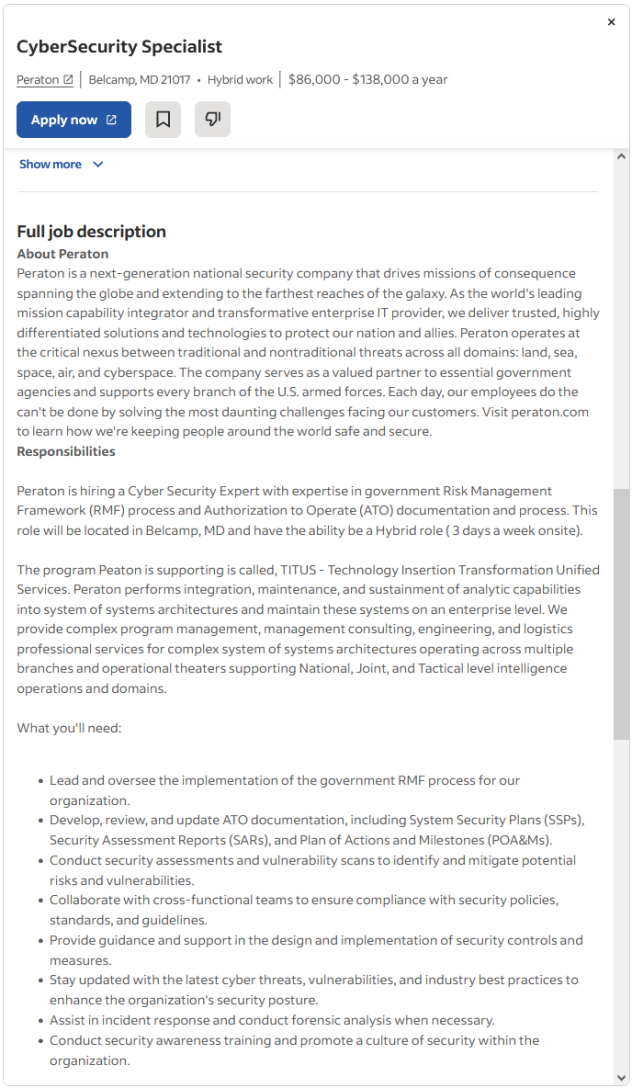
This position is responsible for assisting in the ongoing support and administration of the Department's information security program. The incumbent in this position will focus on areas relating to risk management, continuity of operations, and disaster recovery in support of the information security program. This individual will also have a secondary focus in areas of governance and compliance for information security regulations. The incumbent will also assist in formulation and maintenance of information security policies in conjunction with the FDLE Information Security Manager relating to these areas.

DUTIES & RESPONSIBILITIES:

Specific duties include:

- Establishing and continuously enhancing the Continuity of Operations (COOP) programs, plans and processes for FDLE in conjunction with the Information Security Manager;
- Establishing and continuously enhancing the Disaster programs (DR), plans and processes for FDLE in conjunction with the Information Security Manager;
- Establishing and continuously enhancing the Risk Management programs, plans, and processes in conjunction with the Information Security Manager;
- Researching mandates, regulations and rules for Information Security requirements for the agency;
- Conducting interviews and information gathering meetings;
- Leading tabletop exercises relating to COOP, Risk Management and DR in conjunction with the Information Security Manager; and
- Establishing applicable security policies and best practices.

Fig.1 *ინფორმაციული უსაფრთხოების დარგის სპეციალისტის ვაკანსია,* (https://www.indeed.com n.d.) *დამსაქმებელი: ფლორიდის შტატის სამართალდამცავი დეპარტამენტი*



CyberSecurity Specialist

Peraton | Belcamp, MD 21017 • Hybrid work | $86,000 - $138,000 a year

Apply now

Show more

Full job description

About Peraton

Peraton is a next-generation national security company that drives missions of consequence spanning the globe and extending to the farthest reaches of the galaxy. As the world's leading mission capability integrator and transformative enterprise IT provider, we deliver trusted, highly differentiated solutions and technologies to protect our nation and allies. Peraton operates at the critical nexus between traditional and nontraditional threats across all domains: land, sea, space, air, and cyberspace. The company serves as a valued partner to essential government agencies and supports every branch of the U.S. armed forces. Each day, our employees do the can't be done by solving the most daunting challenges facing our customers. Visit peraton.com to learn how we're keeping people around the world safe and secure.

Responsibilities

Peraton is hiring a Cyber Security Expert with expertise in government Risk Management Framework (RMF) process and Authorization to Operate (ATO) documentation and process. This role will be located in Belcamp, MD and have the ability be a Hybrid role (3 days a week onsite).

The program Peaton is supporting is called, TITUS - Technology Insertion Transformation Unified Services. Peraton performs integration, maintenance, and sustainment of analytic capabilities into system of systems architectures and maintain these systems on an enterprise level. We provide complex program management, management consulting, engineering, and logistics professional services for complex system of systems architectures operating across multiple branches and operational theaters supporting National, Joint, and Tactical level intelligence operations and domains.

What you'll need:

- Lead and oversee the implementation of the government RMF process for our organization.
- Develop, review, and update ATO documentation, including System Security Plans (SSPs), Security Assessment Reports (SARs), and Plan of Actions and Milestones (POA&Ms).
- Conduct security assessments and vulnerability scans to identify and mitigate potential risks and vulnerabilities.
- Collaborate with cross-functional teams to ensure compliance with security policies, standards, and guidelines.
- Provide guidance and support in the design and implementation of security controls and measures.
- Stay updated with the latest cyber threats, vulnerabilities, and industry best practices to enhance the organization's security posture.
- Assist in incident response and conduct forensic analysis when necessary.
- Conduct security awareness training and promote a culture of security within the organization.

Fig.2 *კიბერუსაფრთხოების მეცნიერების სპეციალისტის ვაკანსია დამსაქმებელი: კომპანია „Peraton", გახლავთ აშშ-ს სამთავრობო სააგენტოებისა და აშშ-ს შეიარაღებული ძალების მომსახურე კომპანია.* (https://www.indeed.com n.d.)

აშკარაა, რომ ინფორმაციული უსაფრთხოების სფეროს ადმინისტრაციული და პრაქტიკული მიმართულებების, ანუ ინფორმაციული უსაფრთხოების დარგის სპეციალისტისა და კიბერუსაფრთხოების მეცნიერების სპეციალისტის წინაშე წაყენებული მოთხოვნები და პასუხისმგებლობები სპეციფიურად აქცენტირებულია,

კონკრეტული მიმართულებისთვის დამახასიათებელი, შესაბამისი ცოდნისა და გამოცდილების ჭრილში.

აქვე, შემაჯამებელი სახით, გთავაზობთ მოკლე განმარტებას ინფორმაციული უსაფრთხოების სფეროს ზემოთხსენებული ორი მიმართულების ძირითად ფუნქცია - მოვალეობებზე.

ინფორმაციული უსაფრთხოების დარგის პროფესიონალების ძირითადი ამოცანებია, რომ, პირობითად, კომპანიაში დოკუმენტირებული და დანერგილი იყოს სხვადასხვა პოლიტიკები და პროცედურები, რომლებიც შესაბამისობაში იქნება სახელმწიფო კანონებთან და საერთაშორისოდ აღიარებულ სტანდარტებთან. ასევე, პრაქტიკულ ნაწილში, პირობითად, ხდებოდეს ბიზნეს უწყვეტობის პროცედურის პერიოდული ტესტირება, ბიზნეს პროცესების კომპანიაში დანერგილ პოლიტიკებთან თავსებადობის აუდიტი და ასევე სხვა, ინფორმაციული უსაფრთხოების სფეროს ადმინისტრაციული მიმართულების აქცენტის მქონე ფუნქცია-მოვალეობები, რაც თავისთავად არ გამორიცხავს ტექნიკურ ცოდნასა და ტექნიკური კონტროლების დანერგვა / კონფიგურაციაში ჩართულობას.

მეორეს მხრივ, კიბერუსაფრთხოების მეცნიერების პროფესიონალების ძირითადი ამოცანებია, რომ, პირობითად, რეგულარულად ხდებოდეს კომპანიის ინფორმაციული სისტემებსა და მათ შემადგენელ კომპონენტებში არსებული პოტენციური უსაფრთხოების სისუსტეების იდენტიფიცირება, ვალიდაცია და მიტიგაცია - უსაფრთხოების სისუსტეების სკანირებისა (Center, https://csrc.nist.gov თ. გ.) და შეღწევადობის ტესტირების გზით (Center, https://csrc.nist.gov თ. გ.).რეგულარულად მოწმდებოდეს თანამშრომლების კიბერუსაფრთხოების ცნობიერების დონისა და კომპანიის თანამშრომლების მედეგობის განსაზღვა ე.წ. „ფიშინგ სიმულაციის“ (Phishing Simulation) გზით (IBM, https://www.ibm.com n.d.). გარდა ამისა, პირობითად, დოკუმენტირებული იყოს სხვადასხვა ტიპის კიბერ საფრთხეების წინააღმდეგ რეაგირების გეგმები. ეს ყველაფერი თავისთავად არ გამორიცხავს სახელმწიფო კანონებისა და საერთაშორისოდ აღიარებული სტანდარტების ან/და საუკეთესო პრაქტიკების ცოდნას, კომპანიაში დანერგილ უსაფრთხოების პოლიტიკებთან შესაბამისობას და ა.შ.

შემაჯამებელი სახით უნდა აღინიშნოს, რომ ინფორმაციული უსაფრთხოების დარგსა და კიბერუსაფრთხოების მეცნიერებას შორის არსებითი განსხვავება ის გახლავთ, რომ ინფორმაციული უსაფრთხოების დარგი იცავს ინფორმაციასა და მის ატრიბუტებს, ხოლო კიბერუსაფრთხოების მეცნიერება კი ორიენტირებულია ინფორმაციისა და ინფორმაციული აქტივების სხვადასხვა ტიპის კიბერ საფრთხეებისგან დაცვის პრაქტიკაზე.

საბოლოოდ, აშკარად იკვეთება, რომ ინფორმაციული უსაფრთხოების სფეროს როგორც ადმინისტრაციული, ასევე პრაქტიკული მიმართულების პროფესიონალს სჭირდება მედლის მეორე მხარეს მდგომი მეცნიერებისა თუ დარგისათვის დამახასიათებელი სპეციფიკის საფუძვლების ცოდნა, თუმცა ცალკეულად აღებულ მიმართულებათა ჭრილში, მათთვის დამახასიათებელი სპეციფიკა მკვეთრად განსხვავებულია და საჭიროებს შესაბამის სიღრმისეულ ცოდნასა და გამოცდილებას იმისათვის, რომ საერთო ჯამში, ორივე ზემოთხსენებული პროფილის მქონე პროფესიონალების გაერთიანებით შეიკრას ის ძალა, რომელიც ცნობილია ინფორმაციული უსაფრთხოების სფეროს სახელით და რომელიც დღემდე წინ უდგათ კიბერ კრიმინალებს.

Bibliography

Center, Computer Security Resource. n.d. *https://csrc.nist.gov.* https://csrc.nist.gov/glossary/term/vulnerability_assessment.

—. n.d. *https://csrc.nist.gov.* https://csrc.nist.gov/glossary/term/penetration_testing.

cisa. 2021. *https://www.cisa.gov.* February 1. Accessed February. https://www.cisa.gov/news-events/news/what-cybersecurity .

cisco. n.d. *https://www.cisco.com.* https://www.cisco.com/c/en/us/solutions/hybrid-work/what-is-business-continuity.html.

eccouncil. 2024. *https://www.eccouncil.org.* https://www.eccouncil.org/train-certify/certified-cybersecurity-technician-certification/.

Gill, Ritu. 2023. "https://www.sans.org/blog/what-is-open-source-intelligence/." *https://www.sans.org.* February 23. https://www.sans.org/blog/what-is-open-source-intelligence/.

2024. *https://www.eccouncil.org.* https://www.eccouncil.org/train-certify/certified-chief-information-security-officer-cciso/ .

n.d. "https://www.indeed.com." *https://www.indeed.com/jobs.* https://www.indeed.com/jobs?q=information+security+specialist&sc=0bf%3Aexrec%28%29%3B&start=30&vjk=0355d1840893a397.

n.d. "https://www.indeed.com." *https://www.indeed.com/jobs.* https://www.indeed.com/jobs?q=cybersecurity+specialist&start=C30&vjk=66a83adb9abe8030.

IBM. n.d. "https://www.ibm.com." *https://www.ibm.com/topics/threat-intelligence.* https://www.ibm.com/topics/threat-intelligence.

—. n.d. *https://www.ibm.com.* https://www.ibm.com/think/topics/phishing-simulation.

—. n.d. *https://www.ibm.com.* https://www.ibm.com/topics/internet-of-things.

ISO. n.d. *https://www.iso.org.* https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-2:v1:en .

ISO/IEC. 2022. "Information security, cybersecurity and privacy protection — Information security management systems — Requirements”." *https://www.iso.org.* https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27001:ed-3:v1:en.

nist. n.d. *https://csrc.nist.gov.* https://csrc.nist.gov/glossary/term/information_security .

NIST. n.d. *https://csrc.nist.gov.* https://csrc.nist.gov/glossary/term/operational_technology.