Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій
(повна назва)
Кафедра Інфокомунікаційної інженерії імені В.В. Поповського
(повна назва)

**КВАЛІФІКАЦІЙНА РОБОТА**

**Пояснювальна записка**

Рівень вищої освіти другий (магістерський)

Методи, засоби та технології забезпечення стійкості та безпеки критичної інформаційної інфраструктури
(Methods, Tools, and Technologies for Providing the Resilience and Security of Critical Information Infrastructure)
(тема)

Виконав:
студент 2 курсу, групи АМСЗІім-21-1
Юджесой Асіл Йігіт
(прізвище, ініціали)
Спеціальність: 125 Кібербезпека
(код і повна назва спеціальності)
Тип програми: освітньо-наукова
(освітньо-професійна або освітньо-наукова)
Освітня програма: Адміністративний менеджмент у сфері захисту інформації
(повна назва освітньої програми)
Керівник: проф. каф. ІКІ імені В.В. Поповського
Єременко О.С.
(посада, прізвище, ініціали)

Допускається до захисту
Зав. кафедри _____ Лемешко О.В.
(підпис) (прізвище, ініціали)

2023 р.

*Кваліфікаційна робота не містить відомостей, що заборонені до відкритого друку*

Студент 2 курсу
групи АМСЗІім-21-1 _____ Юджесой Асіл Йігіт
(підпис) (ініціали, прізвище)

Керівник _____ О.С. Єременко
(підпис) (ініціали, прізвище)

Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій
(повна назва)
Кафедра Інфокомунікаційної інженерії імені В.В. Поповського
(повна назва)
Рівень вищої освіти другий (магістерський)
Спеціальність 125 Кібербезпека
(код і повна назва)
Тип програми освітньо-наукова
(освітньо-професійна або освітньо-наукова)
Освітня програма Адміністративний менеджмент у сфері захисту інформації
(повна назва)

ЗАТВЕРДЖУЮ
Зав. кафедри _____
(підпис)
«_10_» 02 2023 р.

**ЗАВДАННЯ**
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентові Юджесой Асіл Йігіт
(прізвище, і'мя, по батькові)

1.Тема роботи: Методи, засоби та технології забезпечення стійкості та безпеки критичної інформаційної інфраструктури (Methods, Tools, and Technologies for Providing the Resilience and Security of Critical Information Infrastructure) затверджена наказом по університету від 10.02.2023 р. № 180Ст

2.Термін подання студентом роботи до екзаменаційної комісії: 28.04.2023 р.

3.Вихідні дані до роботи: методи математичного програмування; моделі та методи відмовостійкої та безпечної маршрутизації; засоби моделювання процесів відмовостійкої та безпечної маршрутизації (середовище Python IDLE); вихідні данні для проведення моделювання (структура досліджуваної мережі, параметри безпеки каналів зв'язку, параметри конфіденційних повідомлень, що передаються).

4.Перелік питань, які потрібно опрацювати в роботі:

1) Провести аналіз методів, засобів і технологій забезпечення стійкості та безпеки критичної інформаційної інфраструктури.

2) Визначити вимоги, що висуваються до критичних інформаційних інфраструктур.

3) Обрати математичну модель відмовостійкої та безпечної маршрутизації фрагментованих конфіденційних повідомлень з використанням композитних шляхів у критичних інформаційних інфраструктурах.

4) Провести аналіз результатів аналітичного моделювання з використанням Python, GEKKO Optimization Suite та NumPy.
5.Перелік графічного матеріалу із зазначенням креслень, плакатів, комп'ютерних ілюстрацій: Демонстраційний матеріал у вигляді ppt-презентації (титульний слайд; опис проблеми, об'єкт, предмет і мета дослідження; аналіз методів, засобів і технологій забезпечення стійкості та безпеки критичної інформаційної інфраструктури; математична модель відмовостійкої та безпечної маршрутизації фрагментованих конфіденційних повідомлень з використанням композитних шляхів у критичних інформаційних інфраструктурах; результати моделювання; висновки).

6. Консультанти розділів роботи

| Найменування розділу | Консультант (посада, прізвище, ім'я, по батькові) | Позначка консультанта про виконання розділу | |
|---|---|---|---|
| | | підпис | дата |
| Основна частина | професор Єременко Олександра Сергіївна | | 28.04.2023 |

## КАЛЕНДАРНИЙ ПЛАН

| № | Назва етапів роботи | Термін виконання етапів роботи | Примітка |
|---|---|---|---|
| 1 | Збір матеріалів для дослідження | 05.03.2023 р. | Виконано |
| 2 | Розробка розділу 1 | 15.03.2023 р. | Виконано |
| 3 | Розробка розділу 2 | 22.03.2023 р. | Виконано |
| 4 | Розробка розділу 3 | 03.04.2023 р. | Виконано |
| 5 | Розробка розділу 4 | 20.04.2023 р. | Виконано |
| 6 | Оформлення роботи | 28.04.2023 р. | Виконано |

Дата видачі завдання 01 березня 2023 р.

Студент _____ Юджесой Асіл Йігіт
(підпис) (прізвище та ініціали)

Керівник роботи _____ професор Єременко О.С.
(підпис) (посада, прізвище, ініціали)

# РЕФЕРАТ

Пояснювальна записка: 60 с., 8 рис., 3 табл., 33 джерела.

КРИТИЧНА ІНФРАСТРУКТУРА, БЕЗПЕКА, ВІДМОВОСТІЙКІСТЬ, МАРШРУТИЗАЦІЯ, ЙМОВІРНІСТЬ КОМПРОМЕТАЦІЇ, МОДЕЛЮВАННЯ

Об’єкт дослідження – процес безпечної та відмовостійкої маршрутизації в критичній інформаційній інфраструктурі.

Предмет дослідження – методи, засоби та технології забезпечення стійкості та безпеки критичної інформаційної інфраструктури.

Мета роботи – аналіз моделей і методів безпечної та відмовостійкої маршрутизації в критичній інформаційній інфраструктурі.

Методи досліджень – аналітичне моделювання, симуляція, формалізація та порівняння.

Проведено аналіз методів, засобів і технологій відповідно до забезпечення стійкості та безпеки критичної інформаційної інфраструктури. Визначено основні вимоги безпеки, що висуваються до систем і мереж як об’єктів критичних інформаційних інфраструктур. Відзначено, що для сталого функціонування таких об’єктів необхідно розробка комплексних рішень з урахуванням технологій безпеки, надійності, резервування та живучості. Обрано математичну модель відмовостійкої та безпечної маршрутизації фрагментованих конфіденційних повідомлень з використанням композитних шляхів у мережах критичних інформаційних інфраструктур. Проаналізовано результати моделювання обраної моделі та обгрунтовано її використання.

# ABSTRACT

This thesis contains 60 pages, 8 figures, 3 tables, and 33 sources or references.

CRITICAL INFRASTRUCTURE, SECURITY, FAULT-TOLERANCE, ROUTING, COMPROMISE PROBABILITY, MODELING

The research object is the process of secure and fault-tolerant routing in critical information infrastructure.

The research subject is the methods, tools, and technologies for providing the resilience and security of critical information infrastructure.

The work aims to analyze models and methods of secure and fault-tolerant routing in critical information infrastructure.

Research methods are analytical modeling, simulation, formalization, and comparison.

An analysis of methods, tools, and technologies was carried out to ensure the resilience and security of Critical Information Infrastructure. The main security requirements for systems and networks as objects of Critical Information Infrastructures are defined. It was noted that for the sustainable functioning of such objects, it is necessary to develop complex solutions considering security, reliability, redundancy, and survivability technologies. A mathematical model of fault-tolerant and secure routing of fragmented confidential messages using composite paths in networks of critical information infrastructures is chosen. The simulation results of the selected model were analyzed, and its use was justified.

# CONTENTS

# LIST OF ABBREVIATIONS, SYMBOLS, UNITS, AND TERMS

API – Application Programming Interface
ACIDS – Application Protocol-Based Intrusion Detection System
APT – Advanced Persistent Threat
BCP – Business Continuity Plan
BYOD – Bring Your Own Device
CEA – Cybersecurity Enhancement Act of 20141
CI – Critical Infrastructure
CII – Critical Information Infrastructure
CIO – Chief Information Officer
COBIT – Control Objectives for Information and Related Technology
COOP – Continuity of Operations Plan
DDoS – Distributed Denial-Of-Service
FBI – Federal Bureau of Investigation
GDPR – General Data Protection Regulation of The European Union
HIDS – Host-Based Intrusion Detection System
IAM – Identity and Access Management
IC3 – Internet Crime Complaint Center
ICS – Industrial Control Systems
ICT – Information and Communications Technology
IDS – Intrusion Detection System
IoT – Internet of Things
IPS – Intrusion Prevention System
IRP – Incident Response Plan
ISSO – Information System Security Officer
IT – Information Technology
MFA – Multi-Factor Authentication
MTTR – Mean Time to Resolve
MUA – Mail User Agent
NIDS – Network-Based Intrusion Detection System
NIST – National Institute of Standards and Technology
OT – Operational Technology

PIDS – Protocol-Based Intrusion Detection System
PoLP – Principle of Least Privileged
SAISO – Senior Agency Information Security Officer
SEM – Security Event Management
SIEM – Security Information and Event Management
SIM – Security Information Management
SSO – Single Sign-On
U.S. – United States
UEBA – User and Entity Behavior Analytics
VPN – Virtual Private Network
WFH – Work from Home
ZT – Zero Trust
ZTA – Zero Trust Architecture

# INTRODUCTION

In a cyber-era where innovative tools and advanced technologies are readily available for threat actors to prosper, it is difficult to over emphasize the importance of maintaining secure and resilient operations within critical infrastructures(CI) to provide necessary services to citizens. Every country has its own formal definition for what a CI is, but in its essence critical infrastructure refers to systems, technologies, assets, processes, networks, and services that are essential for proper functioning of a nation's critical sectors such as energy, telecommunications, healthcare, water supply, transportation, food and agriculture, finance, emergency, and defense.

With an increasing number of conflicts and wars around the world, state-sponsored advanced persistent threat (APT) actors also increased their attacks towards critical information infrastructures (CII). Microsoft, an American multinational technology corporation, reported that; during 2022, cyber-attacks targeting critical infrastructure with threat actors focusing on companies in the information technology sector, financial services, transportation systems, healthcare and communications infrastructure jumped from comprising 20% of all nation state attacks Microsoft detected to 40% [1]. Being so vital to a nation, it is no surprise that critical infrastructures have become a prime target for threat actors. These attacks against critical infrastructures are often well-funded, disciplined, well organized and sophisticated. In order to reduce cybersecurity risks and impacts of a cyber-incident, an organization must implement the best security measures available today, while working together with its partners on improving the cybersecurity readiness of critical assets, missions, and operations.

To improve upon the existing practices and ensure critical information infrastructures' security and resilience, the current work aims to provide a mathematical model of fault-tolerant and secure routing of fragmented confidential messages using composite paths, and analyzes methods, tools, and technologies within information and operational technology environments to reduce cybersecurity risks.

For this reason, the First Chapter contains an overview of the NIST Framework for managing critical infrastructures' cybersecurity risks. The Second Chapter is in general devoted to the preventive safeguards for critical infrastructures. Then, the Third Chapter describes network security and incident response related controls to implement and maintain secure, reliable, and resilient networks. Finally, The Fourth Chapter analyzes

the mathematical model using proactive and reactive approaches, and contains the results of the modeling of fault-tolerant and secure routing of fragmented confidential messages within critical infrastructure networks.

# 1 NIST FRAMEWORK FOR MANAGING CRITICAL INFRASTRUCTURES' CYBERSECURITY RISKS

The NIST framework is a voluntary guidance for organizations within critical infrastructures to manage and reduce cybersecurity risks to ensure the reliable functioning of their operations.[2] According to the Cybersecurity Enhancement Act of 20141 (CEA), a United States federal law designed "to provide for a continuous, voluntary public-private partnership to improve cybersecurity, and to strengthen cybersecurity research and development, workforce development, training, and education, and public awareness and preparedness, and for other purposes related to cybersecurity." [3], NIST must identify "a flexible, prioritized, performance-based, repeatable, and cost-effective approach, including information and operational security measures and safeguards that owners and operators of critical infrastructure may voluntarily adopt to help them identify, assess, and manage cybersecurity risks." [3]

Although NIST has developed the Framework for critical infrastructures to improve their cybersecurity risk management, it can be used by organizations in any sector regardless of their size, operational goals, and current cybersecurity postures. Moreover, since cyberspace does not have borders, critical infrastructures outside the United States may also use the Framework to strengthen their cybersecurity efforts.

The Framework's components were developed based on the existing standards, guidelines, and best security practices and consist of three main components: the Framework Core, the Implementation Tiers, and the Framework Profiles.

The Framework Core is ultimately a collection of cybersecurity activities, references to best practices such as ISO/IEC 27001, CIS Critical Security Controls for Effective Cyber Defense, and Control Objectives for Information and Related Technology (COBIT), and guidance that are common across critical infrastructure sectors.

The implementation tier helps prioritize critical infrastructure's cyber security objectives according to the appropriate level for the organization's current cybersecurity posture. The framework profile serves as a roadmap for organizations within critical infrastructures to reduce cybersecurity risks aligned with organizational goals.

## 1.1 Framework Core

The framework core presents key cybersecurity activities and outcomes for critical infrastructures to manage their cybersecurity risks in a way that aligns with the organization’s existing risk management processes and comprises four elements: functions, categories, subcategories, and informative references. Functions are a high-level organization of basic cybersecurity activities. NIST defines these functions as identify, protect, detect, respond, and recover. Functions have further been divided into Categories, Subcategories and include Informative References to specific sections of standards, guidelines, and practices common among critical infrastructure sectors to manage cybersecurity risks.

### 1.1.1 Identify

According to the NIST Framework, the identify function should help critical infrastructures to "develop and maintain an organizational understanding to manage cybersecurity risk to systems, processes, assets, people, data, and capabilities" [2]. Outcome categories within this function include:

- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy

The NIST Framework’s identify function is the foundation for the implementation of the framework. Organizations must identify and categorize systems, assets, and data on a continuous basis.

This will help the organization to prioritize its efforts based on its specific needs, risks, and budget. The identify function is essential for developing critical discovery capabilities to manage cybersecurity risks, because it is difficult to protect something without understanding what it is there to protect.

### 1.1.2 Protect

The purpose of the protect function is to "develop and implement the appropriate security measures and safeguards to ensure delivery of critical infrastructure services" according to NIST [2]. Outcome categories within this function include:

- Identity Management and Access Control
- Awareness and Training
- Data Security
- Information Protection Processes and Procedures
- Maintenance
- Protective Technology

After completing the identify function by understanding the organization's systems, assets, and data, the next step is the protect function. The protect function helps organizations to plan and implement advanced capabilities that harden its security controls to reduce cybersecurity risks before a cyber-attack occurs. This can help organizations limit the cyber attack's impact by implementing appropriate safeguards while ensuring the delivery of critical infrastructure services.

### 1.1.3 Detect

NIST defines the detect function for critical infrastructures as to "develop and implement activities to identify the occurrence of a cybersecurity event" [2]. Outcome categories within this function include:

- Anomalies and Events
- Security Continuous Monitoring
- Detection Processes

Despite the safeguards implemented at the Protect function phase, adversaries may find a way to get into a critical infrastructure organization’s system and cause harm to the organization. Whether it is a social engineering attack, supply-chain attack, or a sophisticated exploit, many cybersecurity incidents go unnoticed for a long time, which is called attacker’s dwell time, which is the time between an attacker’s initial entry to an organization’s system and the point at which the organization notices their presence. In other words, dwell time indicates the entire life span of a security incident. According to Mandiant, an American cybersecurity firm and a subsidiary of Google, cyber attackers

operate undetected within an organization’s network for an average of 21 days [4]. This is a significant amount of time for attackers to explore an organization’s network, locate its assets and resources, and exfiltrate information. With the implementation of the detect function, organizations may reduce dwell time so they can take appropriate corrective actions before damage occurs.

### 1.1.4 Respond

The purpose of the respond function is to "develop and implement activities to take action regarding a detected cybersecurity incident" according to NIST [2]. Outcome categories within this function include:

- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements

Although it may be best not to get attacked, the likelihood of a destructive cyber-attack such as ransomware affecting an organization’s business functions, finance, and reputation is actually high. In the recently released 2022 Internet Crime Report produced by The Federal Bureau of Investigation (FBI)’s Internet Crime Complaint Center (IC3), it is revealed that, "Of the 16 critical infrastructure sectors that are identified by the U.S government, IC3 reporting indicated 14 sectors had at least 1 member sector that fell victim to a ransomware attack in 2022" [5].

Furthermore, an organization may think they have not experienced a cybersecurity incident yet, but cyber-attacks especially the state-sponsored advanced attacks are often designed to stay dormant until it is time to damage its target. Therefore, in any case, it is important to have an action plan for a detected cybersecurity event.

The respond function can help organizations to develop and implement the appropriate activities to take action such as disclosing the breach, containing the attack, and coordinating with stakeholders and law enforcement regarding these cybersecurity events.

### 1.1.5 Recover

According to the NIST Framework, the recover function should help critical infrastructures to "develop and implement related activities to maintain plans for resilience and to restore and recover any capabilities or services that were impaired due to a cybersecurity incident."[2] Outcome categories within this function include:

- Recovery Planning
- Improvements
- Communications

After a cybersecurity incident occurs within a critical infrastructure organization, the recover function can help reduce the impact of the incident, and serve as a roadmap for returning to normal operations. The function also helps organizations to build lessons learned back into their cybersecurity operations and plans, while reducing the risk from future events that share characteristics with the said incident.

## 1.2 Framework Profile

The framework profile is the alignment of the cybersecurity controls within the NIST framework core with the critical infrastructure's organizational goals and objectives. A profile can serve as a roadmap for organizations to reduce cybersecurity risks and meet their business requirements.

Organizations may have more than one profile that is aligned with the complexity of the organization's business environment. NIST framework describes these two profiles as; one for the current state of the organization's cybersecurity posture, and another one for the desired target state to meet the organization's cybersecurity risk management goals. By comparing these two profiles, organizations may identify gaps between the two, prioritize according to their needs and requirements, and develop an action plan to achieve cybersecurity goals in an efficient manner while communicating risks within and between organizations.

## 1.3 Implementation Tiers

NIST framework's implementation tiers provide a benchmarking system and set of directions related to organization's views on cybersecurity risk and the processes in place

to manage that risk. The framework identifies 4 tiers ranging from partial (tier 1) to adaptive (tier 4), with an increasing degree of complexity in cybersecurity risk management practices. Critical infrastructure organizations should determine a tier that meets the organizational goals and reduces cybersecurity risk to an acceptable level. While the NIST framework encourages organizations identified as tier 1 (partial) to consider moving toward a greater tier, it explicitly states that tiers do not represent maturity levels [2].

Each of these implementation tiers are further divided into three main criteria; risk management process, integrated risk management program, and external participation. The risk management process is the methods critical infrastructures use to manage cybersecurity risks, integrated risk management program is about how such a program is implemented at the organizational level, and external participation is the awareness and understanding level of the organization's business environment.

Tier 1: Partial

At the lowest level of the implementation tiers, organizational cybersecurity risk is often managed without a plan in a reactive manner. The organization has minimum awareness of cybersecurity risk, and measures put in place generally provide insufficient defenses. Processes and procedures to manage cybersecurity risk may not be documented, and information sharing throughout the organization may be limited. An organization within this tier also does not understand its role in the larger ecosystem it is operating in, and may not be aware of the cyber supply chain risks.

Tier 2: Risk informed

At this level, the management of the organization may be aware of the cybersecurity risks and approve risk management processes, but there may not be an organizational policy or organization-wide approach to managing cybersecurity risks. Cyber risk assessment of an organization's assets rarely happens, and information related to cybersecurity is shared within the organization on an informal basis. Tier two organizations lack a unified strategy to reduce cybersecurity risks. Organization understands its role within the supply chain and collaborates with other entities but not in a consistent manner.

Tier 3: Repeatable

Tier 3 is the level where the organization has a living, regularly updated policy to manage cybersecurity risks. There is an organization-wide approach, processes, and procedures to respond to changes in risk. Assets are monitored regularly and correctly,

and organizational communication is established. The organization understands its role in the larger ecosystem and can communicate and collaborate with business partners.

Tier 4: Adaptive

This is the highest level of the implementation tiers, at this level, the organization implements advanced cybersecurity technologies and practices, such as machine learning solutions for threat detection. All personnel work together to manage cybersecurity risks according to policies. The organization can quickly align its security objectives with changing business missions. The organization develops a strong cybersecurity posture against sophisticated threads, including supply chain attacks.

# 2 CRITICAL CONTROLS TO PROVIDE SECURITY AND RESILIENCE

Critical infrastructures are a vital part of any nation, hence a prime target for threat actors with skills and resources to perform advanced cyber-attacks. Moreover, legitimate authorized users may violate security policies unintentionally, impacting the organization's security objectives. In the case where malicious actors successfully conduct their attacks, incapacitation or destruction of a critical information infrastructure can have catastrophic effects on people who rely on such systems to function, therefore it is crucial for organizations to understand their weaknesses and maintain a good overall state of cybersecurity readiness.

## 2.1 Developing an Information System Security Plan

To understand its readiness level for these cyber threats against critical infrastructures, organizations must develop, document, and periodically update an information system security plan. This plan provides an overview of the security requirements of the organization and describes the controls and procedures in place or planned for meeting those requirements. Information system security plan defines identification of the system (name, unique identifier, responsible parties), environment (detailed topology of the system boundaries, system interconnections, and key devices), controls, and record of changes. Information system security plan is a living document that requires periodic review, and should evolve along with the organization's security needs. Differences between information technologies and industrial control systems must be carefully identified, and these differences should influence how security controls will be applied to these systems [6].

National Institute of Standards and Technology (NIST) organizes security controls within the information system security plan into 3 classes, but many security controls, however, can be logically associated with more than one class [7].

Management controls focus on the management of the information system and the management of risk for a system, and contains risk assessment, planning, system and services acquisition, certification, accreditation, and security assessments.

Operational controls address security methods focusing on mechanisms primarily implemented and executed by people, and contain personnel security, physical and

environmental protection, contingency planning, configuration management, maintenance, system and information integrity, media protection, incident response, and awareness and training.

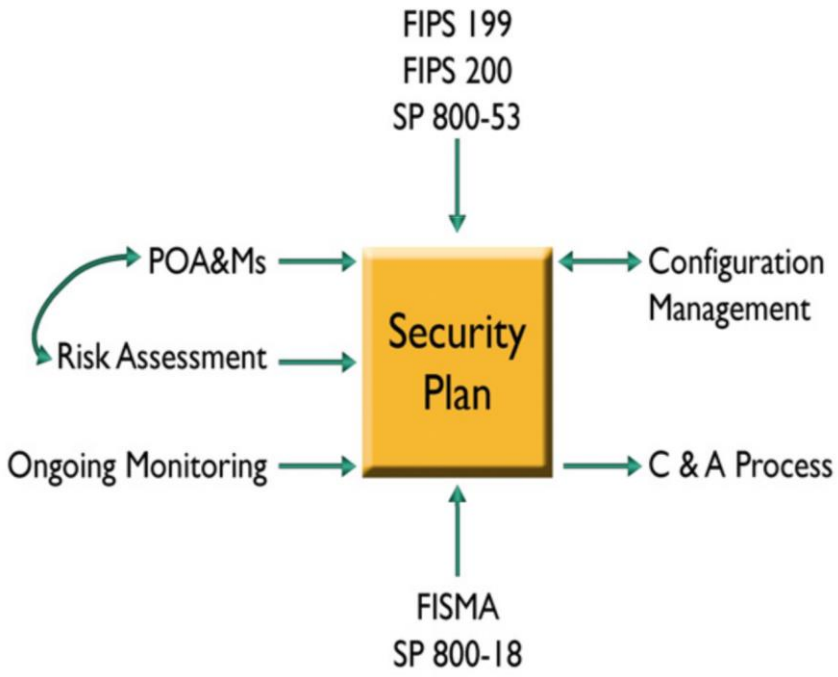


Figure 2.1 – Security Planning Process Inputs/Outputs [7]

Technical controls focus on security controls that the computer system executes, and contain identification and authentication, access control, audit and accountability, and system and communications protection.

Security controls can also be classified by when they act relative to a security breach; before an incident (preventive controls), during an incident (detective controls), and after an incident (corrective controls).

Security controls and procedures outlined within an information system security plan can serve as a road map for organizations to meet their security objectives. Although information system security plan is typically a high-level document it can make use of references to other documents such as contingency plan, incident response plan, or any other additional documents where more detailed information can be obtained.

## 2.2 Preventing Cyber Incidents

A successful cyber-attack may disrupt an organization’s critical operations and business functions, damage the organization’s reputation, and inflict financial losses.

According to IBM Security analysis of research data (gathered from 17 countries and regions and in 17 different industries and compiled by Ponemon Institute), the average cost of a data breach has reached a record high of US$4.35 million in 2022.[8] To reduce the impact, minimize the likelihood of threats, and comply with regulations, it is essential for critical infrastructure organizations to have effective cybersecurity strategies. Preventing these incidents from happening by implementing appropriate preventive safeguards can provide organizations much needed security and resilience against cyberattacks.

### 2.2.1 Risk Assessment and Management

Critical infrastructure organizations operate on complex hardware, software, firmware, systems, and rely on third-party suppliers to provide services. These organizations must protect confidentiality, integrity, availability of information to carry out their business functions by managing information system related security and privacy risks. NIST Risk Management Framework defines risk as "a measure of the extent to which an entity is threatened by a potential event or circumstance, and also a function of the adverse impacts that arise if the said event or circumstance occurs, and the likelihood of occurrence" [9]. Types of risk include:

- Program risk
- Compliance/regulatory risk
- Financial risk
- Legal risk
- Mission/business risk
- Political risk
- Security and privacy risk (including supply chain risk)
- Project risk
- Reputational risk
- Safety risk
- Strategic planning risk

Risk assessment and management is a process that must be carried out as an organization-wide activity. First, an organization must establish the context for risk-based decisions to have a strategy that addresses how organizations intend to assess risk. Secondly, threats to the organization, vulnerabilities within the organization, impacts that

may occur, and the likelihood that impact will occur must be identified to assess risks to the organization. Thirdly, courses of action for responding to risk once identified must be formulated. Lastly, the organization must monitor risk continuously to effectively manage risks within its business environment. For industrial control systems (ICS), safety of the personnel, equipment, property, and environment is a major concern that must be explicitly addressed within a risk assessment and management program. Along with the safety requirements, maintaining maximum availability of for example, water or power systems is also critical for an ICS.

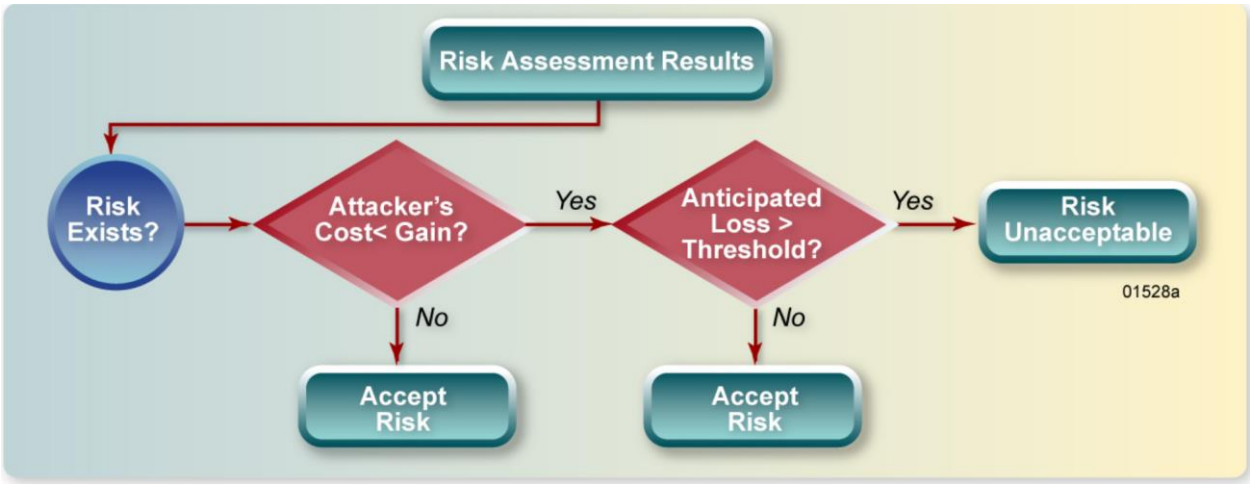


Figure 2.2 – Risk Mitigation Strategy [10]

Given the complexity of threats and the required time and resources to implement safeguards, it is often impractical to eliminate all risks from a system. Therefore, after the initial risk assessment, organizations must develop a prioritization system to categorize risk based on its impact, and whether the risk is acceptable or unacceptable. This system can be used to determine whether risk mitigation actions are necessary. Then, the organization may implement security controls based on its risk mitigation strategy.

### 2.2.2 Identifying Roles and Responsibilities

Organizations must establish security roles and responsibilities in accordance with federal laws and information technology security guidelines that are appropriate for specific operations and functions. Key operations and functions include information security governance, security planning, certification, accreditation, security assessments, and configuration management. Critical infrastructures manage different business

functions as part of their overall organization and these functions has associated risks where the organization's entire workforce must work together to overcome and meet organization’s security objectives.

Managing a workforce for cybersecurity involves different types of organizations including third-party stakeholders, as well as different types of positions some of which are chief information officer (CIO), senior agency information security officer (SAISO), information system security officer (ISSO), chief enterprise architect, authorizing official, certification agent, information system owner, information owner, and user representatives. Before being granted access to critical information systems within IT/OT environments, these individuals must be screened against specific risk designation criteria to reduce potential cybersecurity risks that may arise from the personnel motives or behaviors [6].

### 2.2.3 Inventory of Assets

Attackers are continuously searching for unprotected assets of organizations within critical infrastructures to cause harm to their targets. In order to target these unprotected assets, they need to find and evaluate every asset, whether protected or not, because they cannot attack if they do not know what to attack. Organizations must protect these assets, but like the attackers, they cannot protect what they do not know they have. Thus, it is essential for organizations to identify all their assets to ensure their confidentiality, integrity and availability are well protected.

These assets consist of what is valuable to the organization and also what might be valuable to attackers which is basically any asset that is connected to the infrastructure, and those within cloud environments. Examples include:

- Network devices (router, hub, bridge, access point, switch, gateway)
- End-user devices (desktop or laptop computer, mobile phone, tablet, smartwatch)
- Industrial control systems (supervisory control and data acquisition, Distributed control systems, programmable logic controllers)
- Internet of Things
- Data storage devices (USB flash drive, external or internal hard drive, floppy disk, magnetic tape, paper)
- Servers
- Operating systems and other applications

Along with these assets, organizations must also record metadata, owners of the assets, who can access it, permissions of the asset itself, and how these assets are communicating with each other, and must regularly update their asset inventory. Keeping track of assets is essential for organizations to identify unmanaged and unauthorized assets and it is the basis of an asset management program for monitoring, updating, and removal of these assets.

### 2.2.4 Supply Chain Management

In an increasingly interconnected world, critical infrastructures cross national borders and operate within global supply chains. This introduces a diverse set of vulnerabilities to cyber threats and requires more complex security and resilience practices to reduce the impact of compromising underlying networks and systems. Understanding and mitigating the risk and security gaps associated with each supplier begins with assessing the organization's supply chain and position within the critical infrastructure.

Initial steps for critical infrastructures to determine and control the extent of their environment include:

- Establishing priorities for organizational mission, objectives, and activities.
- Identifying the organization's role in critical infrastructure, industry sector, and supply chain.
- Managing dependencies, critical functions, and resilience requirements for delivery of critical services.

To complete its operational and strategic objectives, organizations rely on the supply chain to provide products and services. Identifying cybersecurity risks and have a collective defense throughout the supply chain is a complicated and costly task, which effectively puts supply chain attacks on the rise. Argon, an Aqua company that specializes in supply chain attacks, conducted a study based on a six-month analysis of customer security assessments to determine the state of enterprise security and readiness to defend against software supply chain attacks and discovered that software supply chain attacks grew by more than 300 percent in 2021 compared to 2020 [11]. The number of supply chain attacks is dramatically increasing because organizations are growing, and so their supply chain. This means a bigger attack surface for attackers, and any supplier that

produces services and products for other organizations can become a potential entry point for the attacker's primary target.

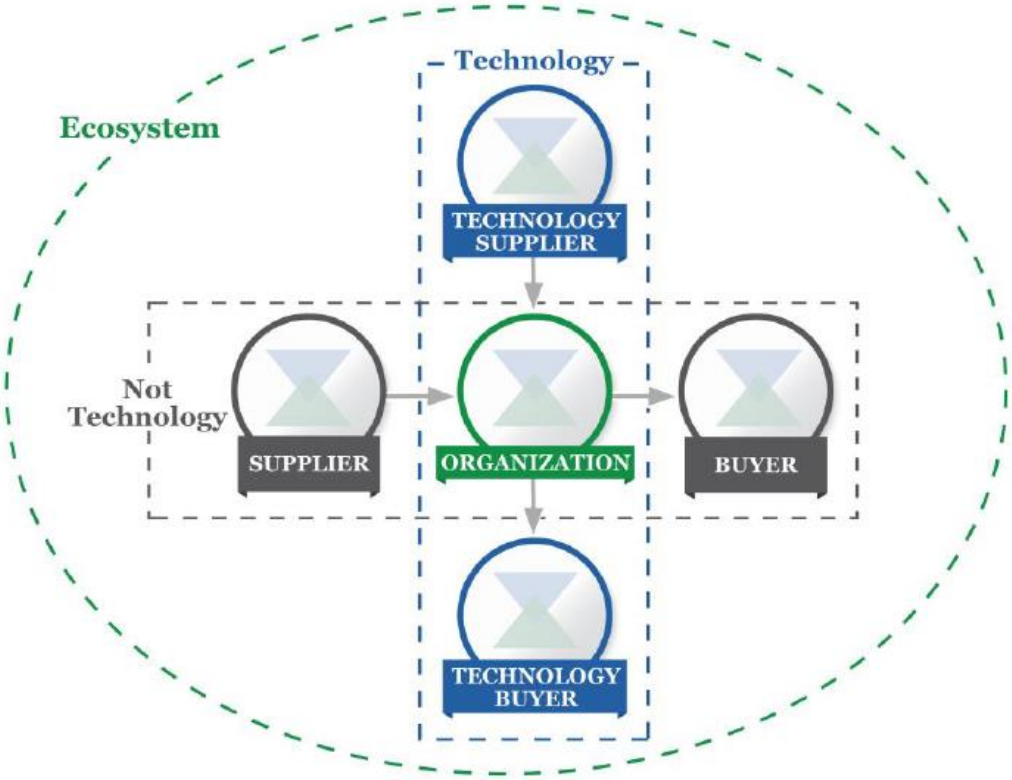


Figure 2.3 – Cyber Supply Chain Relationships [2]

A supply chain attack is a cyber-attack that attempts to cause harm to an organization by exploiting vulnerabilities in its supply chain network. These vulnerabilities are usually linked to suppliers with poor security practices. Supply chain attacks leverage from the trusted relationship between an organization and its suppliers. Any organization including government agencies can suffer a supply chain attack if they work with third-party vendors that lack necessary cybersecurity measures because the information asymmetry that exists between organizations and their suppliers is often difficult to overcome. Origin of these attacks can be difficult to detect because when the attack is discovered, the affected components may have already been widely distributed throughout the supply chain. Types of supply chain attacks include:

- injecting malicious code into software through cyber-attacks, insider threats, and other close access activities
- stealing valid digital signatures from legitimate suppliers and use them to sign malicious code

- compromising hardware or firmware components by injecting specialized code before distribution
- installing malware on devices such as cameras, phones, USB flash drives during manufacturing process

In 2019, Russian Foreign Intelligence Service conducted a campaign of cyber-attacks, and breached the computing networks at SolarWinds, a Texas-based company providing network management software to the United States (U.S) federal government among others. Based on its investigation, SolarWinds found that they have evidence that the vulnerability was inserted within the Orion products and was introduced as a result of a compromise of the Orion software build system and was not present in the source code repository of the Orion products [12]. SolarWinds then released the software updates to its customers not realizing that the updates were compromised allowing attackers to create a backdoor (a program that can give a malicious actor remote access to a compromised system) into the IT environments of its customers. SolarWinds attack compromised the SolarWinds Orion supply chain and according to SolarWinds, up to 18000 customers may have been impacted by the supply chain attack, including government agencies, military offices, major US telecommunications companies, education institutions, and Fortune 500 companies [12].

Supply chain attacks pose a significant risk to all organizations that share data with their supplier network and use third-party products and services. If malicious actors manage to compromise a link in the supply chain, the effects of the breach travels throughout the whole network, affecting everyone involved. Organizations run complex information systems and networks using information and communications technology (ICT) and operational technology (OT) products and components obtained from suppliers. The consequences of a supply chain attack can be severe for critical infrastructures, and protecting against supply chain attacks requires a comprehensive and proactive security strategy. Organizations acquiring services and products from suppliers should evaluate their use, as with other ICT/OT products and services, in the context of a risk management program.

### 2.2.5 Identity and Access Management

Identity and access management (IAM) is a collection of business processes, policies, and supporting technologies and methods such as multi-factor authentication

(MFA), single sign-on (SSO), and principle of least privileged (PoLP) to provide identity, authentication, authorization, and auditing services for managing digital identities. To ensure that users and digital entities only gain access to resources when they have the appropriate credentials, organizations must have an identity and access management program.

Identity and access management programs can be either centralized where all management happens in a single environment, or decentralized where management spreads out across multiple environments. Identity and access management programs can be deployed either on premise, on cloud or through a hybrid model. When implemented, maintained, and monitored correctly, identity and access management can help organizations to comply with regulations related to data security and privacy, strengthen its security posture, reduce costs, and improve employee productivity.

Threat actors often choose credentials as their target because they are easy entry points to an organization's network. According to IBM's Cost of data breach report, stolen or compromised credentials were the primary attack vector of 19% of the data breaches the study highlights in 2022 and also the top attack vector in the 2021 study [8]. Attackers use brute force attacks, spoofing attacks, and social engineering techniques such as phishing, tailgating, whaling and other means to steal credentials and gain unauthorized access to these infrastructures.

In 2021, threat actors used compromised credentials to shut down the Colonial national gas pipeline, an American oil pipeline system that carries gasoline and jet fuel to the United States (U.S). The head of Colonial Pipeline told U.S senators that hackers who launched the cyber-attack against the company and disrupted fuel supplies to the U.S. were able to get into the system by stealing a single password. Colonial Pipeline Chief Executive Joseph Blount told a United States Senate committee that the attack occurred because of a legacy virtual private network (VPN) system that did not have multi-factor authentication in place, and admitted that they did not have a plan such as information system security, identity and access management to prevent this attack.[13] This password compromise essentially led to a ransomware attack (a malicious attack where attackers encrypt an organization's data and demand payment to restore access), and Colonial Pipeline had to pay the attackers $4.4 million to regain access to their systems. The U.S president Joe Biden declared a state of emergency, and Colonial Pipeline had to shut down its operations for six days. In order to prevent this type of attacks disrupting

their business functions, it is imperative for critical infrastructure organizations to implement, maintain, and monitor secure identity and access management solutions.

People tend to use the same password for multiple accounts or choose easy to remember passwords for their accounts. Using strong and unique passwords for each account along with multi-factor authentication can drastically strengthen security of such accounts at authentication level. Multi-factor authentication is an authentication method where users are required to provide two or more pieces of factors to the authentication mechanism to access their accounts. Factors can be something the user knows (password, answer to security questions), something the user has (key, id badge, security token), something the user is (biometrics), or location of the user (different levels of authentication might apply outside of the organization's network). For industrial control systems (ICS), using a long and complex password along with another factor of authentication may not be feasible, because during a crisis, an operator under stress may not be able to remember a complex password or may not have the time to enter the long password into the console.[6] This could lead to a disaster, therefore, it is essential for industrial control systems to maintain a balance between security and operational ease. An alternative to a traditional password authentication, a physical token or smart card combined with a biometric authentication mechanism may be used within these environments.

Organizations using multiple applications may incorporate single sign-on (SSO) technology to their infrastructure to help reduce the number of passwords a user must manage and prevent security fatigue. Being able to remember and manage a single password could encourage users to choose stronger passwords. However, single sign-on requires strong security measures to protect user credentials because once stolen, attackers can gain access to all applications unified under the SSO. Within critical infrastructures where availability of systems is crucial, organizations must have failover mechanisms for single sign-on authentication services against denial of service attacks.

Another important concept that can help reduce an organization's attack surface and risk of malware spread is the principle of least privileged where users, systems, and processes have access to information and resources only when it is absolutely necessary to function.

### 2.2.6 Data Protection

Managing data is paramount. A successful attack, hardware failure, or accidental or intentional data destruction can have catastrophic effects on organizations within critical infrastructures. Exposing personal data is often subject to regulations the infrastructure must comply with. General Data Protection Regulation of the European Union (GDPR) can fine violators up to €20 million, or up to 4% of the annual worldwide turnover of the preceding financial year, whichever is greater [14]. It is crucial for critical infrastructure organizations to have a data management plan for data protection, monitoring, recovery, and disposition.

Data can be on premise but can also be on cloud environments, shared with multiple vendors, or with users who work from home (WFH). Data can be at rest or in transit and must be managed through its entire life cycle.

In order to avoid data loss, organizations should make isolated backups of data regularly to facilitate recovery when necessary. A data backup plan or policy should be established prior to deployment and should include testing and restoration of said data.

Critical infrastructures must protect data, while allowing authorized users to perform their job functions. Organizations can utilize encryption as a technology that scrambles data in a way that only authorized personnel can understand them. This protection should also provide robust encryption key management, access control, and audit logging capabilities. For time critical operations such as those within industrial control systems, communications latency due to the additional time and computing resources required for encryption technologies must be explicitly calculated and it is usefulness for cybersecurity should not lower the organization’s operational capabilities [6]. Organizations that are working together should develop shared encryption policies and procedures to not disrupt interoperability [15].

Data disposal is another important aspect of the data management process. Most regulations state that organizations must dispose of data that are no longer in use or if it is personal data and the person who is the subject of the said data withdraws their consent. It is important for critical infrastructures to have a policy that covers what happens to data at the end of the retention period.

### 2.2.7 Security Awareness and Training

Threat actors thrive from weaknesses they find in their target organizations. These weaknesses can occur either in cyber space at any form or more prominently in humans as cognitive bias. According to IBM Cyber Security Intelligence Index Report, human error was the major cause in %95 of all successful breaches [16]. Threat actors prefer to search for human weaknesses first, because exploiting cognitive bias is usually easier than searching through entire cyberspace which is both complex and prone to have at least basic cyber security measures. Because of this, threat actors have developed tactics, techniques and procedures to exploit human weaknesses.

Although sophisticated attacks exist, these attacks can also be as simple as sending a malicious email to a specific employee of the target organization, hoping the employee is not aware of the consequences of treating such an email harmless. This type of an attack is an example of spear phishing attack and most attacks start with a phishing email to an unsuspecting victim. Some of these attacks would not be successful if the victims are aware of the technique attackers use, and the impact it might cause to the organization.

If organizations within a critical infrastructure must comply with regulations, such as FISMA, PCI, or HIPAA, they must provide security awareness training to employees to meet regulatory requirements. The training can be as straightforward as locking a desk drawer, recognizing a guest without a badge, erasing a whiteboard after a meeting, or reporting an incident. It might also be technical but this can quickly become a burden to employees. For industrial control systems (ICS), an awareness and training program must include physical processes, and system specific information.[6] Security awareness and skills training program needs regular updates and all employees should join to the program. There is no way to effectively measure how willing employees may be, thus, organizations should consider every employee as a potential security weakness.

### 2.2.8 Software Protections

Software (operating systems and applications) acquired from third-party providers usually come with default configurations such as default administrator accounts or passwords, open services and ports, and pre-configured settings to provide easy deployment and use for organizations. Although convenient, this is not the most secure

approach. If left with the default configurations, these software can become easy targets for malicious actors.

It is organizations' responsibility rather than the software provider to update the initial configurations of these software according to their own security policy. Organizations may deploy a configuration management tool to look for differences between the settings of software of managed machines and the default configurations. Software configuration management is a continuous process, because providers may release software updates and patches, new vulnerabilities may be reported, or organization's security policy may be updated. After initial configurations, organizations must maintain and manage software through its entire life cycle.

New vulnerabilities arise every day. Cyber defenders within critical infrastructures must monitor public and private industry sources such as security advisories, threat bulletins to identify new vulnerabilities before the malicious actors do. Vulnerability scanning tools can be useful for evaluating security configuration of an organization's assets and software. Organizations then use the result of these tools to remediate detected vulnerabilities in their software. A ticket system might also be deployed along with the vulnerability scanning tool to track and prioritize vulnerabilities for fixing.

Email represents one the most common part of organizational communication and also the organization's largest attack surface. With email, users interact with external users on a daily basis, without the knowledge of whether these external users are trustworthy or not. To manage their email, users use a computer program called mail user agent (MUA), which is also known as an email client. Because of its ease of use; web based email clients, and mobile email clients has become popular amongst users, but these clients may lack embedded security controls, encryption, authentication, Something Posing as Mail (SPAM) filter, and multi-factor authentication (MFA), any of which an attacker can take advantage of using techniques such as phishing, spoofing, and snooping among others [17]. It is organization's responsibility to ensure only secure, fully supported, and latest version of email clients are allowed, and users are trained against common attack vectors against email.

In addition to email clients, attackers can exploit web browsers in multiple ways leveraging trust between users and the application. A web browser that is not secure, outdated, and unpatched can become an easy entry point for attackers. Third party extensions that are not vetted properly can run malicious code within the context of the web browser, or even directly the operation system itself [17]. Like the email clients,

organizations must ensure that web browsers are only used when they are known to be secure, updated, and its extensions have restricted access.

### 2.2.9 Malware Defense

Malware (a portmanteau for malicious software) is a type of computer program designed to infect computers with the intention of causing harm to them in multiple ways. There are many types of malware, including: virus, worm, trojan horse, rootkit, fileless malware, coin miner, spyware, adware, malicious mobile code, keystroke logger, and ransomware. Malware is one of the key elements of almost every type of cyber attack, and according to Sonicwall, an American cybersecurity company that sells network security appliances, During 2022, the worldwide number of malware attacks reached 5.5 billion, an increase of two percent compared to 2021.[18] There are numerous methods attackers can deliver malware such as, injecting malware into vulnerable software or hardware, using social engineering techniques, brute-force credential attack. Threat actors use malware to:

- Take control of legitimate users' computers to run botnets, send spam emails
- Extort payment by disrupting business functions and operations
- Destruct networks and computer systems
- Steal sensitive information such as passwords, e-mails, trade secrets, patent documentations, acquisition plans

Keeping software up-to-date, deploying malware detection and protection suites, and increasing user awareness about password hygiene, phishing emails, dangers of plugging unfamiliar removable drives, and other possible malware attack vectors can help organizations to stay protected from malware attacks and minimize the cybersecurity risks.

### 2.2.10 Penetration Testing

State-sponsored advanced persistent threat actors use sophisticated attacks to target critical infrastructures. It is a difficult task for cyber defenders to predict what these attackers might do, and what weaknesses are there for the attackers to find. In order to make this task easier, an organization may conduct simulated cyber-attacks against its own systems and networks to discover its weaknesses before the threat actors do. This

kind of activity is called penetration testing and can help the organization to reduce cybersecurity risks and improve security posture.

In these simulated attacks, penetration testers use a variety of tactics, techniques, and procedures that are similar to real world attack patterns used by threat actors. Along with the weakness discovery opportunities before the attackers, penetration tests can also help measure compliance with security policies and regulations. There are different types of penetration testing categorized by where penetration testers search for the weaknesses; application, network, hardware, and personnel. Personnel penetration testing uses social engineering methods and can provide the organization insights about the level of awareness and training its employees have. Conducting regular penetration tests, critical infrastructure organizations can gain in-depth understanding about effectiveness of their cybersecurity methods and resiliency of their assets.

# 3 NETWORK SECURITY AND INCIDENT DETECTION

## 3.1 Network Security

Critical infrastructure organizations rely on their network to run critical missions and business operations. Therefore, it is essential for these organizations to have secure networks. Network security is the collection of policies, technologies, processes and practices that protects the organization's data and resources against potential threats by preventing entry and proliferation within a network.

In addition to securing the network itself, organizations must also deploy preventative measures to protect the underlying networking infrastructure. Network infrastructure is a collection of hardware devices, software applications, and network services that work together to run an organization's network. When acquired from third-party suppliers, network infrastructure devices often come with default configurations and features such as open ports, administrator account and password, and support for older protocols to ease deployment and use. Designing and maintaining a reliable, safe, robust and scalable network infrastructure is essential to an organization's ability to provide product and services. Although every organization has different needs and objectives when it comes to cybersecurity, combination of following tools and technologies may be utilized to build a network security system.

### 3.1.1 Firewalls

A firewall is software or hardware that controls the flow of traffic between networks. Firewalls act as gatekeepers to stop undesired traffic and unrecognized sources from entering the network while letting legitimate traffic through. Organizations often deploy firewalls at the edges of a network, but firewalls can also be used internally to segment a larger network into smaller subnetworks, because if one subnetwork is compromised by an attack, the organization can quarantine the subnetwork and deny attackers to have free reign inside the whole network. There are three general classes of firewalls:

1. Packet filtering firewall also known as stateless inspection firewall is the most basic type of firewall that operates at the network layer to employ access control lists

based on the information contained in a packet such as the packet's source and destination IP addresses, network protocol, session source and destination ports, and the direction of the packets without keeping track of the state of the traffic that passes through, hence stateless.

2. Stateful inspection firewall, as with packet filtering firewall, intercepts packets at the network layer and inspects them to see if they are permitted by an existing rule, but unlike packet filtering, stateful inspection firewalls keep track of each connection to determine if the packet's state contradicts its expected state, and decide whether allow the packet pass through or not.[19]
3. Application-proxy gateway firewall examines packets at the application layer and filters traffic based on specific application rules to perform stateful and deep packet inspections.

### 3.1.2 Intrusion Prevention Systems

An intrusion prevention system (IPS) is either a hardware or software that is developed to prevent incidents from happening. IPSs can prevent both known and unknown threats, and can take appropriate measures automatically, such as configuring a firewall to deny access on port 22, or applying patch to a vulnerable software, or removing the infected part of an e-mail. [20] A typical IPS can perform the following activities; continuously monitor events within computer systems and networks, log information about the events, analyze the events, discover intrusion attempts by performing signature or anomaly based detection techniques, try to stop these attempts if found, and report the findings.

### 3.1.3 Virtual Private Networks

A virtual private network (VPN) can provide user authentication and integrity checking while extending a private internal network over a public network, such as the Internet by encrypting connections between them. VPNs can be used to improve industrial control systems' security by controlling access between control system host computers/controllers and untrusted networks [6]. A VPN often uses IPsec or SSL/TLS encryption protocols to establish encrypted connections over network and devices. The two most common VPN architectures are gateway-to-gateway which connects multiple

fixed sites over public lines and host-to-gateway which provides a secure connection to the network for individual remote users who are located outside of the network [19].

### 3.1.4 Zero Trust Architecture

Traditionally, critical infrastructure organizations have relied on perimeter based network security to monitor and control traffic going into and out the network to protect their assets and resources. However, digital transformation, cloud migration, bring your own device (BYOD), and the Internet of Things (IoT) are changing the way these organizations operate. Furthermore, when the COVID-19 pandemic started to spread throughout the world, many organizations shifted towards work from home (WFH) policies while allowing individuals to connect to the network from home computers outside an organization’s control. As a result, it has become nearly impossible to secure a network using traditional perimeter-based network security methods such as deploying a firewall when an organization's employees, data, and resources are spread across the globe.

This network expansion requires more firewalls to be deployed and all these firewalls need even more complex configurations than before. The initial deployment might also be not enough, because every time the network boundaries change or attackers find an innovative way to get into the network, these firewalls must be adjusted to control the traffic going into an out the network. This requires extensive resources to be devoted to the firewall maintenance, and can become extremely costly for the organizations and burdensome to the security teams.

Complicating network security further, with the convergence of information technology (IT) and operational technology (OT), OT systems that were previously isolated have become more accessible while expanding the network boundaries along with the attack surface. Adoption of automation requires third-party suppliers to supply even more IoT devices, adding reliance to the supply chain and the risks that come with it. Also, perimeter-based network security guards the entry and exit points to the network, but there is an implicit trust within the network, meaning once attackers breach the perimeter they can move laterally within the network uninterrupted.

The increased inefficiency of traditional perimeter-based network security has led to development of a new model for cybersecurity known as “zero trust” (ZT) and along with it "zero trust architecture" (ZTA) which is a cybersecurity architecture that is based

on zero trust principles [21]. According to NIST, an operative definition of zero trust and zero trust architecture is as follows: "Zero trust (ZT) aims to provide a collection of ideas and concepts designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised. Zero trust architecture (ZTA) is an organization's cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, access policies, and workflow planning. Therefore, a zero trust organization is the network infrastructure (physical and virtual) and operational policies that are in place for an organization as a product of a zero trust architecture plan" [21]. In 2010, while a principal analyst at Forrester Research, a United States based company that provides independent research, data, and advisory services, John Kindervag developed the zero trust architecture and it works by assuming everything (enterprise assets, users, software, hardware, non-human entities) is considered a threat regardless of their position within or outside the network.

To implement a Zero Trust Architecture within an enterprise, NIST recommends adherence to the following zero trust basic tenets [21]:

- All data sources and computing services are considered resources.
- All communication is secured regardless of network location.
- Access to individual enterprise resources is granted on a per-session basis.
- Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes.
- The enterprise monitors and measures the integrity and security posture of all owned and associated assets.
- All resource authentication and authorization are dynamic and strictly enforced before access is allowed.
- The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.

## 3.2 Detecting Incidents: When Prevention Fails

Even the best cyber defense is not immune to all cyber-attacks all the time. Cyber incidents will occur. Whether through ransomware, social engineering, distributed denial-

of-service (DDoS), supply chain, or through a malicious insider, adversaries will find a way that works. These types of incidents happen because of an intentional attack, there are also unintentional threats where a legitimate authorized user violates security policies unintentionally, impacting the organization's security objectives, and causing harm to the organization's information systems or sensitive data. For the times attackers bypass the preventive safeguards, it is essential for organizations to have detective controls in place. Detective controls are an organization's second line of defense, and must be designed to monitor, detect, log, and alert the security teams after an event has occurred.

### 3.2.1 Logging and Continuous Monitoring

It is crucial for an organization to lower its mean time to resolve (MTTR) metric by detecting and responding to malicious activities quickly. Because the longer the intruders linger within the organization's systems and networks, the more damage they can cause. System and audit logs collection and continuous monitoring can help organizations to detect the threats and reduce the impact when incidents occur.

#### 3.2.1.1 Security Information and Event Management

Security information and Event Management (SIEM) is an "application that aims to provide the ability to gather numerous data from information system components and present that data as practical information via a single interface" according to NIST [22]. For compliance and auditing purposes, critical infrastructure organizations may use SIEM software products or services as a combination of security information management (SIM) and security event management (SEM) to monitor, analyze, and correlate events from system logs to detect intrusion attempts. SIEM solutions can; aggregate data, link events and attributes together, search through logs based on specified criteria, display alerts and informational charts, perform advanced user and entity behavior analytics (UEBA) using machine learning, and report results for organizations to detect threats before they have a chance to disrupt business operations.

#### 3.2.1.2 Intrusion Detection Systems

A critical infrastructure organization must continuously scan its systems for possible incidents to take appropriate security measures before the eventual impact occurs. Intrusion detection is "the process of monitoring the events occurring in an information system or a computer network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, standard security practices, or acceptable use policies" [20]. Organizations can automate this process using an intrusion detection system (IDS). An IDS is a network security tool (which can be a hardware device or software) that sits out of band on the organization’s network infrastructure and consists of network security technologies to help organizations identify potential threats. Along with monitoring, analyzing, and reporting, IDSs also provide extensive logs, which then can be further analyzed by the security personnel.

Most commonly, intrusion detection systems perform detection by either using signature based or anomaly based analysis. Signature based detection is a simple process that takes place by comparing current activities with characteristics of known threats using string operation methods such as regular expressions. Signature based detection cannot detect previously unknown threats, and attackers can easily avoid this type of detection by using fragmentation or obfuscation techniques. Anomaly based detection looks for deviations between normal behaviors and observed events. Security personnel may define the "normal" behaviors manually, or more often than not, a computer program with machine learning capabilities may also do it. Anomaly based detection can detect previously unknown threats, but depending on the quality of the normal behavior definitions, it can also generate extensive amounts of false-positives.

IDS types range in scope, a network-based intrusion detection system (NIDS) can be deployed at strategic locations within the organization’s network infrastructure to monitor the whole network, host-based intrusion detection system (HIDS) can be deployed on specific endpoints, protocol-based intrusion detection system (PIDS) analyzes the communication protocol used by computer systems, application protocol-based intrusion detection system (ACIDS) works at the application level to monitor specific application protocols, or an IDS can be the combination of these systems.

## 3.3 Corrective Measures to Provide Cyber Resilience

Threat actors have the advantage of an element of surprise. They also have access to advanced technologies, and innovative tools to conduct their attacks. It is difficult to anticipate every cyberattack, but being resilient to them is essential for critical infrastructures. Cyber resiliency refers to "the capacity to anticipate, withstand, recover from, and adapt to adverse conditions, attacks, stresses, or compromises on systems that use or are enabled by cyber resources."[23]

Although cybersecurity and cyber resilience pursue the same objective towards protecting against cyber threats, cyber resilience is considered more focused on reducing risks of potentially compromised cyber resources. To be cyber resilient, organizations should aim to achieve following objectives; avoid cyber incidents, prepare specific actions for anticipated adversities, continue critical business functions during adversity, limit impact from incidents and restore functionality as quickly as possible, identify organization’s weaker points and adapt security controls accordingly to be better prepared for the next incident [24].

Detecting incidents is a prerequisite for cyber resiliency, because it provides opportunity to respond. Once an incident has been detected, corrective controls must be quickly activated to reduce or eliminate the potential impact, and be able to return to the previously working state of operations as soon as possible.

### 3.3.1 Contingency Planning

Information security stands on three pillars; confidentiality, integrity, and availability. Contingency planning strategies address the impact level of the availability (which is timely and reliable access to and use of information) security objective of information systems.[25] All critical infrastructure organizations must develop and maintain information system contingency plans for "backup operations, disaster response, and post-disaster recovery to ensure the availability of critical resources and services, and to facilitate the continuity of operations in an emergency situation."[26] Contingency plans combine efforts with continuity of operations plans (COOP) along with other recovery and resilience plans to provide an organization steps to restore its business functions possibly at an alternate location while preventing major disruptions to operations.

#### 3.3.1.1 Business Continuity Plan

Business continuity plan (BCP) contains a set of instructions that address an organization's short or long term recovery strategies in conjunction with a continuity of operations plan (COOP) to sustain the organization's mission/business essential functions in the event of a disruption. Achieving mission/business continuity during and after a disruption is crucial for critical infrastructures especially those operating with industrial control systems to ensure essential services are available for citizens.

#### 3.3.1.2 Disaster Recovery Plan

Without a disaster recovery plan many organizations cannot withstand major disruptions and recover from the losses. ITIC 2022 Global Reliability survey polled 1,550 corporations across 30 vertical market segments worldwide and discovered that 44% of firms said a single hour of downtime in 2022 costs their businesses $1 Million [27]. When disaster strikes, disaster recovery plans can help an organization to reduce risks and impacts dramatically. DRP is "formally documented procedures to recover and protect a critical information technology or operational technology infrastructure in the event of a major hardware or software failure or destruction of facilities" [6]. An organization must identify and train its response teams for disaster recovery process, and maintain backup of its mission critical data and also extra available storage and computing power to fail over in the case of disruption resulting from catastrophic events.

### 3.3.2 Incident Response

To minimize the likelihood of an impact and return to the operational state in a timely manner, organizations must have formally documented processes for responding to these incidents when they occur. This document is called an incident response plan (IRP) and must cover organization's response processes along with training requirements for personnel and testing the incident response capabilities of the information assets [6]. As shown in Figure 3.1, there are four major phases of the incident response process for organizations to follow [28]:

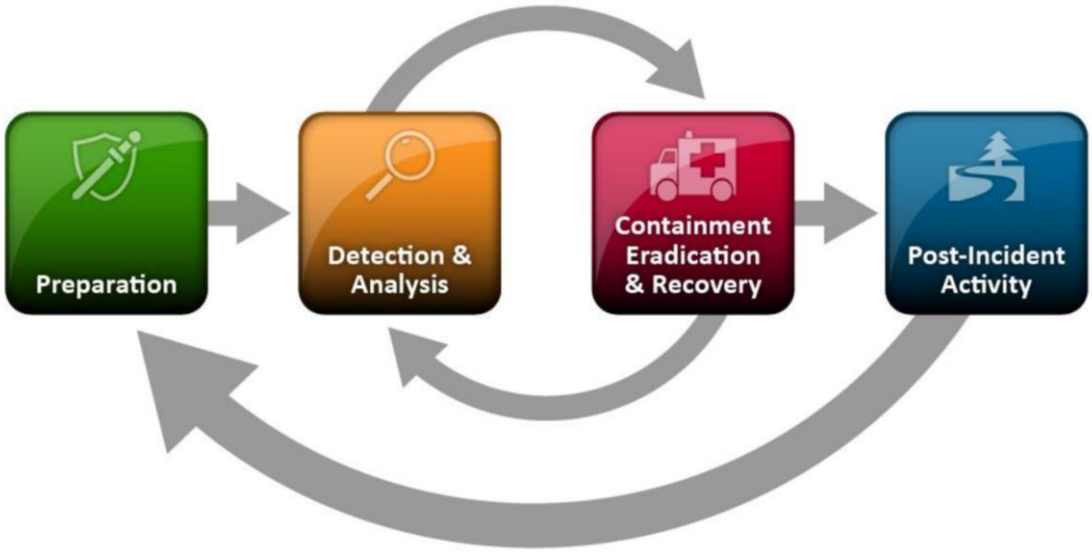


Figure 3.1 – Incident Response Life Cycle [28]

1. In the preparation phase, the organization aims to prevent incidents from happening in the first place by implementing appropriate safeguards according to its risk management criteria. An incident response team (a team manager, a technical lead, and other technical personnel with diverse technical skill sets) must be established, trained, and provided with necessary tools and resources.
2. With enough determination and persistence, even the best defense can be penetrated. There may also be accidental violations of security policies caused by the personnel. In the detection and analysis phase, accurately detecting and assessing possible incidents is essential to alert security teams, so that they can proceed to the next step within the incident response process.
3. Containment, eradication, and recovery phase involves processes to mitigate the impact of the incident. For example, if a malware infects an application server within a corporate network, first, the application server must be separated from the rest of the network such as workstations, printers, and control network to contain the infection. Secondly, all connected networks prior to the incident must be analyzed to see if additional hosts are infected by the malware while eradicating detected malware instances from the infected systems. Finally, the organization can identify the extent and magnitude of the impact and recover from it.
4. In the post-incident activity phase, the organization identifies the cost of the incident, and builds lessons learned back into its cybersecurity plan to prevent future incidents.

# 4 ROUTING MEANS FOR IMPROVEMENT OF CRITICAL INFORMATION INFRASTRUCTURE RESILIENCE AND SECURITY

## 4.1 Critical ICT Services

Telecommunications, or telecom, transmit information such as video, voice, and data over radio, wire, optical, or other electromagnetic systems utilizing numerous information and communication technologies (ICT) and underlying infrastructures. In recent years, with the rapid growth of communication networks, the telecommunications sector has evolved from a provider of voice services into an interconnected industry encompassing satellite, wireless, and wireline systems and technologies that allow entities to share information throughout the globe.

The telecommunication sector is critical on its own and an integral component of any nation, supporting the operations of all other critical infrastructure sectors. Emergency services rely on communications to receive emergency calls from citizens, dispatch responders, and coordinate operations. Financial services transmit transactions over underlying communication infrastructure. The energy sector monitors and controls the delivery of electricity with the aid of communications technologies and systems. Transportation systems depend on communications to direct and control the flow of traffic. Telecommunications infrastructure is essential for delivering critical services, and its operational denial or disruption may have a cascading effect on people and critical sectors that depend on interoperability.

## 4.2 Network Security and Secure Routing Means

A group of interconnected nodes transmits data or messages over a communication channel, ultimately building a computer network. Links between these nodes may sometimes be disrupted by an unintentional security policy violation, configuration mistake, hardware failure, cyber incident, or other means. When a link within this computer network fails, unless there is a failsafe, the said data cannot traverse through the nodes causing all sorts of problems depending on the criticality of the data and who owns it. Although securing the primary communication point for critical infrastructure is crucial, a single point of failure like this is not an acceptable approach. Instead, a

distributed routing algorithm computes new routes in case of a failure while providing the much-needed redundancy for the mission-critical networks. Even though it is a failsafe, this approach is also not without its caveats. The connectivity between nodes stays impaired when the algorithm calculates the new routes. Although this routing transition is generally handled in a fraction of a second, it may not be fast enough for time-sensitive operations and need improvements.

The analysis demonstrates that modern network construction standards prioritize the implementation of information security measures. The International Telecommunication Union (ITU) standards require three levels of security: infrastructure, services, and applications [29]. The efficiency of the top two levels relies heavily on the effectiveness of the infrastructure-level security measures. These measures aim to ensure the security of network elements (such as switches, routers, and servers), links, and routes composed of links in general.

Typically, the security level of network elements is assessed through the probability of compromise, which refers to unauthorized access to protected information and any indication of such access. The relevant layers of the OSI model protocols should provide security services [29-32]. On the other hand, the security at the network layer should be ensured and maintained by routing protocols. As demonstrated in several studies [29], routing tools enable the secure transmission of confidential information, such as session keys, authentication information, and critical user data.

In practice, a combination of proactive and reactive measures, including those related to routing solutions, is necessary to ensure the desired level of information security. Proactive measures are primarily used to prevent message compromise or reduce the likelihood of such an event [29]. Reactive measures, conversely, come into play when the security of transmitted data is breached. In such cases, routing solutions are essential to restore the necessary level of security quickly.

A proactive approach to information security could involve implementing a solution that provides a specific level of security. For instance, one approach could involve transmitting messages in parts using Shamir's scheme over multipath routing, where the number of parts is balanced over non-overlapping paths [29]. It is essential to determine the order of changing the paths used to transfer parts of confidential messages in response to changes in the network state that could compromise message security to maintain the security of the transmitted messages. In this case, fast rerouting solutions can be considered reactive in ensuring secure routing.

## 4.3 Method of Secure Fast Rerouting of Messages over Composite Paths: Proactive and Reactive Approaches

Extending the functionality of secure routing means is vital to implement the principles of both the proactive and reactive approaches. In other words, in the structure of the method of secure routing, it is essential to provide procedures for prompt response to possible violations of the information security level [29-31]. Currently, routing protocols react to potential changes in the network state in the time scale of tens of seconds, which is not always acceptable in terms of the required quality of service and information security.

Therefore, methods and protocols of fast rerouting are increasingly used in practice, during which two types of paths are precomputed: primary and backup. The use of each type separately should lead to the satisfaction of the requirements regarding the level of information security. Then, if the primary path fails, the transmitted data will be routed almost instantaneously (with a delay of tens of milliseconds) using backup routes. Of course, the primary and backup routes should not overlap on the failed network elements (routers, communication links, or paths in general) [29]. The causes of denial of service can be both overload and breakdown of network equipment, the consequences of network attacks, and the impact of malicious software.

Then, within the framework of Secure Fast Rerouting (S-FRR), the use of multiple primary paths refers to Proactive Approach solutions for providing a given level of information security, and the application of backup paths meets the requirements of a Reactive Approach. At the same time, in the framework of the proposed method, the calculation of the set of primary and backup paths should be carried out as consistently as possible to improve the efficiency of the final solutions.

Division of paths into primary and backup means that parts of the message will not be transmitted over all accessible composite and simple paths, only in their limited number, but with the fulfillment of the requirements for the compromise probability [29].

Considering that it is necessary to implement multipath routing of message parts to increase information security, primary and backup paths will be represented by not individual composite or simple paths but by their multipath. In this case, the primary and backup multipath composition can include several composite and (or) simple paths.

In the calculation of the backup multipath, it is proposed to implement the following two protection schemes for the primary multipath:

- protection scheme for the primary multipath as a whole, in which the primary and backup multipaths do not overlap either by nodes or links;
- protection scheme for a single path (composite or simple) of the primary multipath where the backup multipath should not contain the protected path of the primary multipath.

The implementation of each protection scheme aims to restore a given level of information security by eliminating the primary multipath and moving to a backup multipath. In this regard, we use the following notations according to [29].

Table 4.1 – S-FRR Model Notations [29]

| | |
|---|---|
| **Constants** | |
| $S_{msg}$ and $D_{msg}$ | source and destination nodes for the transmitted message |
| $\tilde{M}$ | Number of the non-overlapping composite paths that could be used during the routing of message parts |
| $\tilde{M}_i$ | Number of fragments in the *i*th composite path which can be compromised ($i = \overline{1,\tilde{M}}$) |
| $M_i$ | Number of links in the *i*th composite path which can be compromised ($i = \overline{1,\tilde{M}}$) |
| $p_i^j$ | Probability of compromising the *j*th link of the *i*th composite path ($i = \overline{1,\tilde{M}}$, $j = \overline{1,M_i}$) |
| $(T,N)$ | Shamir's scheme parameters, where $N$ is the total number of message parts, obtained by applying Shamir's scheme; $T$ is the minimum number of parts ($T \le N$) needed for the message reconstruction |
| $\gamma_P$ | Allowable probability of message compromise in the network |
| **Indices** | |
| $\tilde{p}_i^j$ | Probability of compromising the *j*th fragment of the *i*th composite path ($i = \overline{1,\tilde{M}}$, $j = \overline{1,\tilde{M}_i}$) |
| $\tilde{p}_i^{pr}$ | Probability of compromising the *i*th composite or simple path of primary multipath ($i = \overline{1,\tilde{M}}$) |

| | |
|---|---|
| $\tilde{p}_i^b$ | Probability of compromising the *i*th composite or simple path of backup multipath ($i = \overline{1, \tilde{M}}$) |
| $\tilde{P}_{msg}^{pr}$ | Probability of compromise for the whole message during its transmission in parts over composite or simple paths of primary multipath |
| $\tilde{P}_{msg}^b$ | Probability of compromise for the whole message during its transmission in parts over composite or simple paths of backup multipath |
| **Variables** | |
| $n_i$ | Integer variable, which is the number of message parts transmitted over the *i*th composite or simple path, included into the primary multipath, ($i = \overline{1, \tilde{M}}$) |
| $\bar{n}_i$ | Integer variable, which is the number of message parts transmitted over the *i*th composite or simple path, included into the backup multipath, ($i = \overline{1, \tilde{M}}$) |

The probability of compromising the *i*th composite path consisting of $\tilde{M}_i$ fragments can be calculated according to the following expression:

$$\tilde{p}_i = 1 - \prod_{j=1}^{\tilde{M}_i} (1 - \tilde{p}_i^j). \quad (4.1)$$

While the probability of compromising the *i*th simple path consisting of $M_i$ elements can be calculated using the expression

$$p_i = 1 - (1 - p_i^1)(1 - p_i^2)\ldots(1 - p_i^{M_i}) = 1 - \prod_{j=1}^{M_i} (1 - p_i^j). \quad (4.2)$$

In the general case, one composite path may comprise several series-connected fragments with parallel connections of links. Let us denote the maximum number of parallel connected links $h_i$ over all fragments of the *i*th composite path. Then following conditions take place [29]

$$h_i \le n_i \le T-1,\ (i=\overline{1,\tilde{M}}), \tag{4.3}$$

and its fulfillment will allow the distribution of message parts over parallel links of network fragments of composite paths so that a nonzero number of such message parts is transmitted in each of them.

In addition, condition (4), taking into account the composite nature of the used paths, will take the form:

$$N - n_i < T,\ (i=\overline{1,\tilde{M}}). \tag{4.4}$$

The constraints (4.1), (4.3), or (4.4) are imposed on the control variables depending on Shamir's scheme used, and the equality []

$$\sum_{i=1}^{\tilde{M}} n_i = N. \tag{4.5}$$

Following the above notations, to calculate the probability of compromising the message transmitted in parts over a set of composite paths, it is necessary to use expressions [29]

$$\tilde{P}_{msg}^{pr} = \prod_{i=1}^{\tilde{M}} \tilde{p}_i^{pr} \quad \text{and} \quad \tilde{P}_{msg}^{b} = \prod_{i=1}^{\tilde{M}} \tilde{p}_i^{b}. \tag{4.6}$$

It should be noted that the compromise probabilities of network fragments $\tilde{p}_i^{pr}$ and $\tilde{p}_i^{b}$ are the function of the message parts number transmitted in them, i.e., from $n_i$ and $\bar{n}_i$. Then, taking into account (8), we have the conditions

$$\tilde{p}_i^{pr} = \begin{cases} 1 - \prod_{j=1}^{\tilde{M}_i} (1-\tilde{p}_i^{j}),\ n_i > 0; \\ 1,\ n_i = 0, \end{cases} \text{ and } \tilde{p}_i^{b} = \begin{cases} 1 - \prod_{j=1}^{\tilde{M}_i} (1-\tilde{p}_i^{j}),\ \bar{n}_i > 0; \\ 1,\ \bar{n}_i = 0. \end{cases} \tag{4.7}$$

The systems (4.7) can be rewritten as follows:

$$\tilde{p}_i^{pr} = 1 - H_0(n_i) \prod_{j=1}^{\tilde{M}_i} (1 - \tilde{p}_i^j) \;\; \text{i} \;\; \tilde{p}_i^b = 1 - H_0(\bar{n}_i) \prod_{j=1}^{\tilde{M}_i} (1 - \tilde{p}_i^j) \;, \tag{4.8}$$

where $H_0$ is the Heaviside function, which, taking into account expression (4.8), is calculated as follows

$$H_0(n) = \begin{cases} 0, \, n = 0; \\ 1, \, n > 0. \end{cases}$$

The expression adds the existing conditions from [29] due to the S-FRR implementation

$$\sum_{i=1}^{\tilde{M}} \bar{n}_i = N \tag{4.9}$$

In turn, to protect the main multipath, by analogy with [29], it is necessary to ensure the following condition:

$$\sum_{i=1}^{\tilde{M}} n_i \, \bar{n}_i = 0 . \tag{4.10}$$

If it is necessary to protect the *i*th composite path, it is essential to ensure fulfillment of the bilinear condition

$$n_i \, \bar{n}_i = 0 . \tag{4.11}$$

The following conditions are introduced to meet the requirements regarding the probability of compromising the messages transmitted using both the primary and backup multipath:

$$P_{msg}^{pr} \le P_{msg}^{b} \le \gamma_P \,. \tag{4.12}$$

Therefore, the basis of the developed S-FRR method can be the solution to the optimization problem of Nonlinear Integer Programming with the optimality criterion [29]

$$J = \sum_{i=1}^{\tilde{M}} \tilde{p}_i n_i + \sum_{i=1}^{\tilde{M}} \tilde{p}_i \bar{n}_i \,. \tag{4.13}$$

and the constraints represented by the conditions (4.1) – (4.12). In this case, the constraints (4.12), (4.13) are nonlinear, and the calculated variables $n_i$ and $\bar{n}_i$ are integers. In criterion (4.13), the values $\tilde{p}_i$ calculated under expressions (8) are the cost weight coefficients. This ensures secure routing over the network when the maximum number of message parts will be sent over the path with the minimum compromise probability. Conversely, the minimum number of message parts will be transmitted over the path with the highest compromise probability, or no message parts will be transferred.

## 4.4 Numerical Study of Secure Fast Rerouting

Let us demonstrate the features of the proposed mechanism of Secure Fast Rerouting. CII topology for Turk Telekom International has been selected for the numerical example (Fig. 4.1). The initial structure of the network is shown in Fig. 4.2, and the corresponding probabilities of compromising the communication links are indicated in Table. 4.2.

The message's source is the first node, and the destination is the fifteenth node. In Figure 4.3, the solid lines show the communication links to form the primary and backup multipath (composite paths) for message transmission.

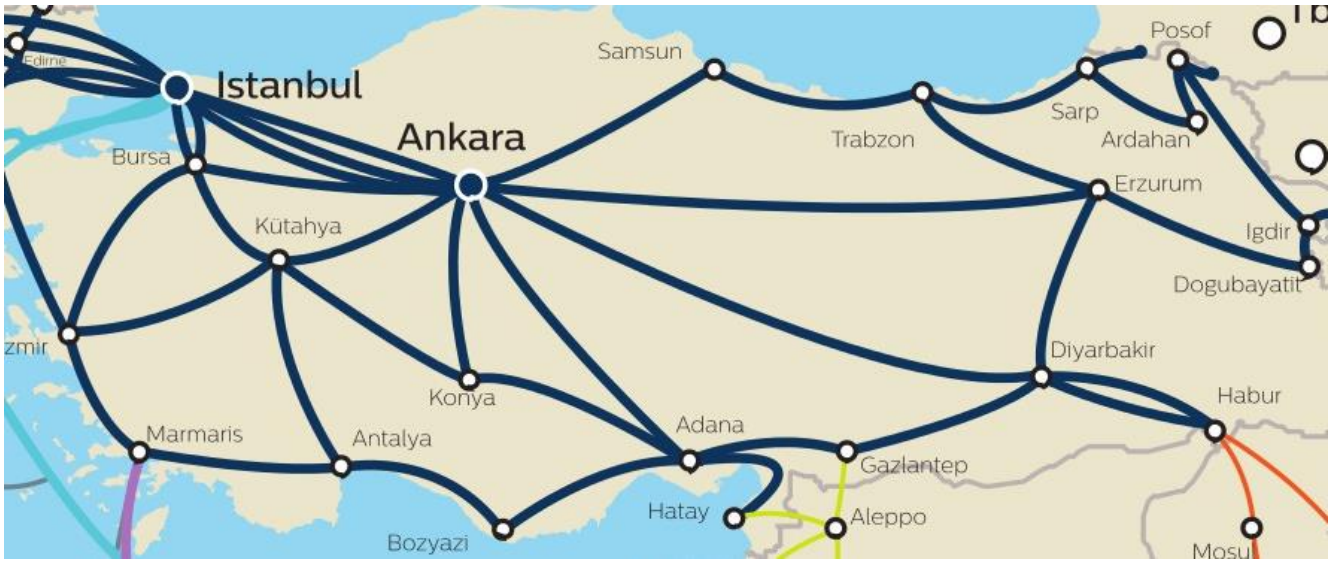


Figure 4.1 – Turk Telekom International network map fragment [33]

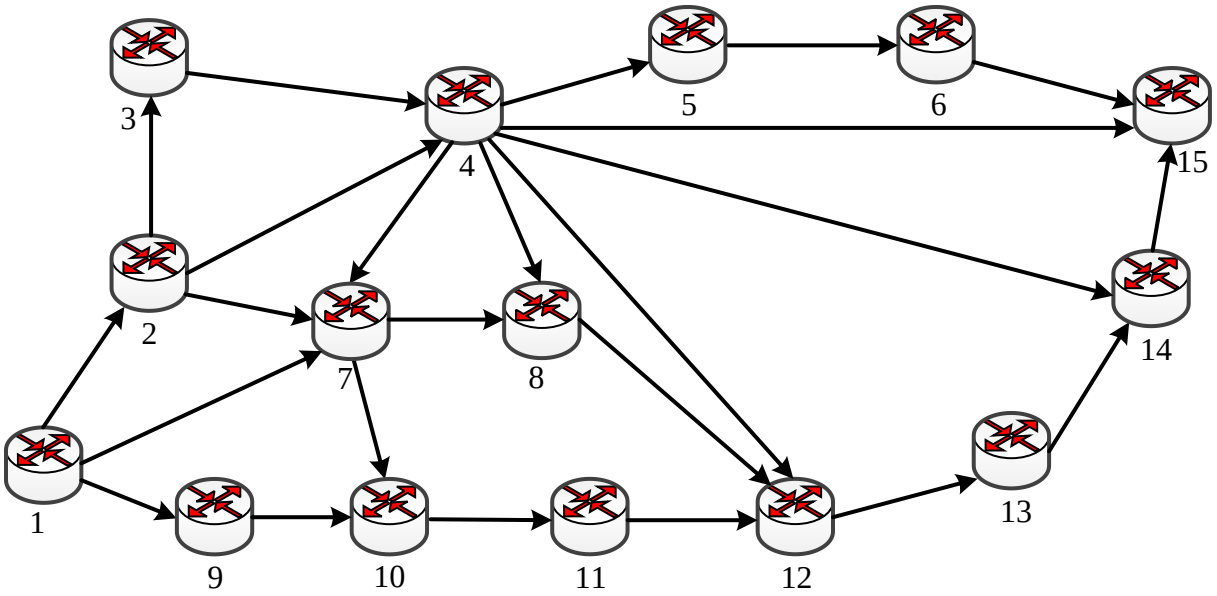


Figure 4.2 – Initial network structure for numerical research

Suppose that with the Secure Fast ReRouting, Shamir's scheme (10, 10) is implemented. According to the structure of the paths from Figure 4.3, $h_1 = 2$ and $h_2 = 2$ . Also, the allowable value of the probability of compromising the transmitted message, determined by the parameter $\gamma_P$, is 0.4. Then, during the numerical research, the following cases were considered demonstrating the features of implementing the protection scheme described in Section 4.3.

It should be noted that the composite paths shown in Figure 4.3 by the red and blue solid lines on the network structure under study are chosen to satisfy the requirements for

$\gamma_P = 0.4$, and are also formed by the maximum number of communication links. Therefore, network resources are used more efficiently without compromising the level of network security in terms of message compromise probability.

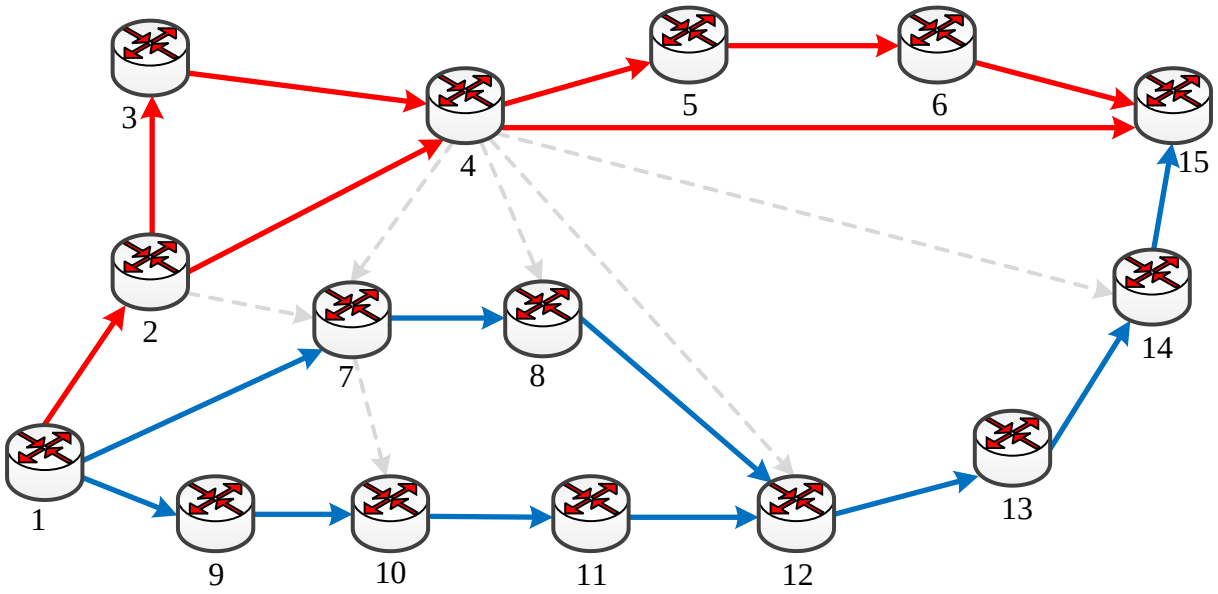


Figure 4.3 – Composite paths selected

Table 4.2 Initial research data for the Secure Fast Rerouting (composite paths)

| Path # | 1 (Composite) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Link | 1→2 | 2→3 | 3→4 | 2→4 | 4→5 | 5→6 | 6→15 | 4→15 |
| Link # | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| $p_i^j$ | 0.2 | 0.2 | 0.1 | 0.2 | 0.2 | 0.15 | 0.2 | 0.1 |
| Path # | 2 (Composite) | | | | | | | |
| Link | 1→7 | 7→8 | 8→12 | 1→9 | 9→10 | 10→11 | 11→12 | 12→13 | 13→14 | 14→15 |
| Link # | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
| $p_i^j$ | 0.1 | 0.1 | 0.1 | 0.1 | 0.15 | 0.1 | 0.1 | 0.1 | 0.15 | 0.1 |

Since only two disjoint composite paths can be chosen on the structure under study, the composite path protection scheme (4.11) is preferred. At the same time, condition

(4.12) allows for determining which route will be the primary and which will be the backup. Table 4.3 shows the results of calculating the parameters for the primary and backup routes, namely the probability of path compromise and the order of balancing message parts by fragments of composite paths.

Table 4.3 Parameters of the primary and backup composite paths

| Primary Composite Path | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Path compromise probability | 0.2792 | | | | | | | |
| Number of message parts in the path | 10 | | | | | | | |
| Link | 1→2 | 2→3 | 3→4 | 2→4 | 4→5 | 5→6 | 6→15 | 4→15 |
| Link # | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| Number of message parts in the link | 10 | 1 | 1 | 9 | 1 | 1 | 1 | 9 |
| Backup Composite Path | | | | | | | | |
| Path compromise probability | 0.3825 | | | | | | | |
| Number of message parts in the path | 10 | | | | | | | |
| Link | 1→7 | 7→8 | 8→12 | 1→9 | 9→10 | | | |
| Link # | 1 | 2 | 3 | 4 | 5 | | | |
| Number of message parts in the link | 9 | 9 | 9 | 1 | 1 | | | |
| Link | 10→11 | 11→12 | 12→13 | 13→14 | 14→15 | | | |
| Link # | 6 | 7 | 8 | 9 | 10 | | | |
| Number of message parts in the link | 1 | 1 | 10 | 10 | 10 | | | |

Next, consider the use of simple disjoint paths. The selected set is shown in Figure 4.4. It should be noted that they are the shortest in terms of the number of hops and partially contain the communication links that made up the composite routes, which will allow a comparison between these two cases.

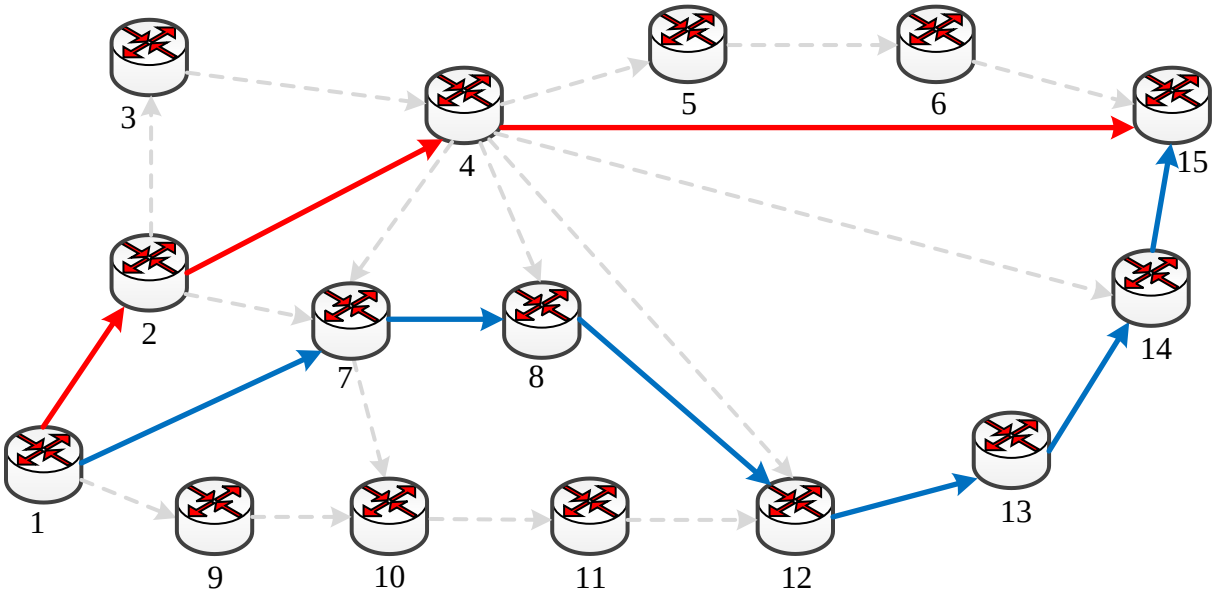


Figure 4.4 – Simple primary and backup paths

First, it must be said that the maximum number of disjoint paths on the structure under study is two. This means it is possible to implement either a secure routing strategy balancing confidential message parts along these two routes or a fault-tolerant routing strategy with one primary and one backup route. Implementing a complex solution to the problem of secure fast rerouting is impossible by using simple paths on the structure under study. In addition, the calculation of the path compromise probabilities showed that they do not meet the requirements for the probability of compromise of the transmitted message since, in this case, it is determined by the path compromise probability:

- for the path 1→2→4→15 the compromise probability is 0.4240;
- for the path 1→7→8→12→13→14→15 the compromise probability is 0.4981.

Consequently, the only option for implementing Secure Fast Rerouting (S-FRR) for the structure under study is to use composite paths. Here, including series-parallel fragments in the route allows for balancing the parts of the message within the fragments, thus reducing the probability of compromising the composite path and the message being transmitted. The calculations confirmed this conclusion. In addition, the generated paths satisfy the introduced requirements $\gamma_P = 0.4$ for the primary and backup composite routes, while the simple paths do not.

# CONCLUSION

This work is devoted to researching methods, tools, and technologies for providing the resilience and security of Critical Information Infrastructure. An analysis of methods, tools, and technologies was carried out to ensure the resilience and security of Critical Information Infrastructure. The main security requirements for systems and networks as objects of Critical Information Infrastructures are defined. It was noted that for the sustainable functioning of such objects, it is necessary to develop complex solutions considering security, reliability, redundancy, and survivability technologies, as well as recognized technical standards and means, namely:

- NIST framework for managing critical infrastructures' cybersecurity risks;
- critical controls to provide security and resilience;
- network security and incident detection;
- routing means for the improvement of Critical Information Infrastructure resilience and security.

A mathematical model of fault-tolerant and secure routing of fragmented confidential messages using composite paths in networks of critical information infrastructures is chosen. The simulation results of the selected model were analyzed, and its use was justified. An analysis of analytical modeling results using Python, GEKKO Optimization Suite, and NumPy has been conducted.

Hence, the technical task of Secure Fast Rerouting was formulated as an optimization problem with constraints (4.1)-(4.12) and optimality criterion (4.13). The simulation results proved the adequacy and workability of the used method. Including series-parallel fragments in the route allows for balancing the parts of the confidential message within the fragments, thus reducing the probability of compromising the composite path and the message being transmitted.

Some work results were reported at international scientific and practical conferences [30-32].

# REFERENCES


1. Microsoft, “Microsoft Digital Defense Report.” https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv; Microsoft, 2022.
2. NIST, “Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1,” National Institute of Standards; Technology, Gaithersburg, MD, Apr. 2018. doi: 10.6028/NIST.CSWP.04162018.
3. “Public Law 113–274.” https://www.congress.gov/bill/113th-congress/senate-bill/1353/text; The United States Government Publishing Office, 2014.
4. “M-trends Mandiant Special Report.” https://www.mandiant.com/media/15671; Mandiant, Inc, 2022.
5. “Internet Crime Report.” https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf; Internet Crime Complaint Center, 2022.
6. K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, “Guide to Industrial Control Systems (ICS) Security,” National Institute of Standards; Technology, NIST SP 800-82r2, 2015. doi: 10.6028/NIST.SP.800-82r2.
7. M. Swanson, J. Hash, and P. Bowen, “Guide For Developing Security Plans For Federal Information Systems,” National Institute of Standards; Technology, NIST SP 800-18r1, 2006. doi: 10.6028/NIST.SP.800-18r1.
8. IBM, “Cost of Data Breach Report 2022.” https://www.ibm.com/downloads/cas/3R8N1DZJ; IBM Security, 2022.
9. Joint Task Force Transformation Initiative, “Risk Management Framework For Information Systems and Organizations,” National Institute of Standards; Technology, NIST SP 800-37r2, 2018. doi: 10.6028/NIST.SP.800-37r2.
10. P. Bowen, J. Hash, and M. Wilson, “Information Security Handbook: A Guide for Managers.”
11. E. Orzel, “Software Supply Chain Security Report.” https://info.aquasec.com/argon-supply-chain-attacks-study; Argon Security, 2021.
12. S. Ramakrishna, “An Investigative Update of the Cyberattack.” https://orangematter.solarwinds.com/2021/05/07/an-investigative-update-of-the-cyberattack/, 2021.

13. W. Turton and K. Mehrotra, “Hackers Breached Colonial Pipeline Using Compromised Password.” https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password; Bloomberg, 2021.
14. GDPR, “REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL,” 2016.
15. CISA, “Public safety land mobile radio communications security,” 2022.
16. IBM, “IBM Cyber Security Intelligence Index Report.” IBM Security, 2014.
17. “CIS controls version 8.” https://learn.cisecurity.org/cis-controls-download; Cybersecurity; Infrastructure Security Agency, 2021.
18. B. Conner, “2023 SonicWall Cyber Threat Report.” https://www.sonicwall.com/2023-cyber-threat-report, 2023.
19. K. Scarfone and P. Hoffman, “Guidelines on Firewalls and Firewall Policy,” 2009.
20. K. A. Scarfone and P. M. Mell, “Guide to Intrusion Detection and Prevention Systems (IDPS),” National Institute of Standards; Technology, NIST SP 800-94, 2007. doi: 10.6028/NIST.SP.800-94.
21. S. Rose, O. Borchert, S. Mitchell, and S. Connelly, “Zero Trust Architecture,” National Institute of Standards; Technology, 2020. doi: 10.6028/NIST.SP.800-207.
22. A. Johnson, K. Dempsey, R. Ross, S. Gupta, and D. Bailey, “Guide For Security-focused Configuration Management of Information Systems,” National Institute of Standards; Technology, NIST SP 800-128, 2019. doi: 10.6028/NIST.SP.800-128.
23. R. Ross, V. Pillitteri, K. Dempsey, M. Riddle, and G. Guissanie, “Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations,” National Institute of Standards; Technology, Gaithersburg, MD, NIST SP 800-171r2, 2020. doi: 10.6028/NIST.SP.800-171r2.
24. R. Ross, V. Pillitteri, R. Graubart, D. Bodeau, and R. McQuaid, “Developing Cyber-Resilient Systems,” National Institute of Standards; Technology, NIST SP 800-160v2r1, 2021. doi: 10.6028/NIST.SP.800-160v2r1.
25. “44 USC 3542: Definitions.” https://uscode.house.gov/view.xhtml?req=granuleid:USC-2010-title44-section3542&num=0&edition=2010; The U.S. Government Publishing Office, 2011.
26. E. Barker, “Recommendation for Key Management Part 1: General,” National Institute of Standards; Technology, NIST SP 800-57pt1r4, 2016. doi: 10.6028/NIST.SP.800-57pt1r4.

27. L. Didio, “ITIC Global Server Hardware, Server OS Reliability Report,” Information Technology Intelligence Consulting Corp, 2022.
28. P. Cichonski, T. Millar, T. Grance, and K. Scarfone, “Computer Security Incident Handling Guide : Recommendations of the National Institute of Standards and Technology,” National Institute of Standards; Technology, NIST SP 800-61r2, 2012. doi: 10.6028/NIST.SP.800-61r2.
29. Yeremenko, O., Lemeshko, O., Persikov, A.: Secure routing in reliable networks: proactive and reactive approach. In: Shakhovska, N., Stepashko, V. (eds.) CSIT 2017. AISC, vol. 689, pp. 631–655. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-70581-1_44
30. A.Y. Yucesoy, F.R. Negre De Bofarull. Providing the Resilience and Security of Critical Information Infrastructure. Fifteenth International Scientific Conference of undergraduate and graduate students "Prospects for Development of Information-Telecommunication Technologies and Systems" PDTIS 2023: Conference Proceedings. Kyiv, NTUU "KPI", 2023. P. 361.
31. F.R. Negre De Bofarull, A.Y. Yucesoy. Analysis and Research of Ensuring Network Security Methods Under Load Balancing. Fifteenth International Scientific Conference of undergraduate and graduate students "Prospects for Development of Information-Telecommunication Technologies and Systems" PDTIS 2023: Conference Proceedings. Kyiv, NTUU "KPI", 2023. P. 360.
32. J. Kashaija, A.Y. Yucesoy, F.R. Negre De Bofarull. Investigation of "MAN-ON-THE-SIDE" Attack by Wireshark Simulation. Fifteenth International Scientific Conference of undergraduate and graduate students "Prospects for Development of Information-Telecommunication Technologies and Systems" PDTIS 2023: Conference Proceedings. Kyiv, NTUU "KPI", 2023. P. 363.
33. Turk Telekom International network map. URL: https://turktelekomint.com/network-map/