symmetry

MDPI

Article

Models and Methods for Assessing Intruder's Awareness of Attacked Objects

Vladimir V. Baranov [1,*] and Alexander A. Shelupanov [2]

[1] Department of "Information Security", M.I. Platov South Russian State Polytechnic University, 346428 Novocherkassk, Russia
[2] Department of "Integrated Information Security of Electronic Computing Systems", Tomsk State University of Control Systems and Radioelectronics (TUSUR), 634050 Tomsk, Russia; saa@tusur.ru
* Correspondence: kaf-ib@npi-tu.ru; Tel.: +7-9281-00-05-98

Abstract

The formation of strategies and tactics of destructive impact (DI) at the stages of complex computer attacks (CCAs) largely depends on the content of intelligence data obtained by the intruder about the attacked elements of distributed information systems (DISs). This study analyzes scientific papers, methodologies and standards in the field of assessing the indicators of awareness of the intruder about the objects of DI and symmetrical indicators of intelligence security of the elements of the DIS. It was revealed that the aspects of changing the quantitative and qualitative characteristics of intelligence data (ID) at the stages of CCA, as well as their impact on the possibilities of using certain types of simple computer attacks (SKAs), are poorly studied and insufficiently systematized. This paper uses technologies for modeling the process of an intruder obtaining ID based on the application of the methodology of black, grey and white boxes and the theory of fuzzy sets. This allowed us to identify the relationship between certain arrays of ID and the possibilities of applying certain types of SCA end-structure arrays of ID according to the levels of identifying objects of DI, and to create a scale of intruder awareness symmetrical to the scale of intelligence protection of the elements of the DIS. Experiments were conducted to verify the practical applicability of the developed models and techniques, showing positive results that make it possible to identify vulnerable objects, tactics and techniques of the intruder in advance. The result of this study is the development of an intruder awareness scale, which includes five levels of his knowledge about the attacked system, estimated by numerical intervals and characterized by linguistic terms. Each awareness level corresponds to one CCA stage: primary ID collection, penetration and legalization, privilege escalation, distribution and DI. Awareness levels have corresponding typical ID lists that can be potentially available after conducting the corresponding type of SCA. Typical ID lists are classified according to the following DI levels: network, hardware, system, application and user level. For each awareness level, the method of obtaining the ID by the intruder is specified. These research results represent a scientific contribution. The practical contribution is the application of the developed scale for information security (IS) incident management. It allows for a proactive assessment of DIS security against CCAs—modeling the real DIS structure and various CCA scenarios. During an incident, upon detection of a certain CCA stage, it allows for identifying data on DIS elements potentially known by the intruder and eliminating further development of the incident. The results of this study can also be used for training IS specialists in network security, risk assessment and IS incident management.

Academic Editor: Sergei Odintsov

Received: 23 July 2025
Revised: 25 August 2025
Accepted: 4 September 2025
Published: 27 September 2025

Citation: Baranov, V.V.; Shelupanov, A.A. Models and Methods for Assessing Intruder's Awareness of Attacked Objects. *Symmetry* **2025**, *17*, 1604. https://doi.org/10.3390/sym17101604

Keywords: the symmetry of indicators of awareness of the intruder and indicators of intelligence security; arrays of intelligence data; levels of identification of objects of destructive influence

1. Introduction

The main channel for receiving data about the attacked object for the violator is active computer intelligence. It is conducted through the use of soft–hardware and software tools, as well as certain patterns of computer attacks presented in Common Attack Pattern Enumeration and Classification (CAPEC) [1]. From the point of view of the mechanisms for obtaining intelligence about the attacked DIS, the following two stages should be distinguished: conducting reconnaissance from outside the perimeter of the DIS and conducting reconnaissance after penetrating inside the perimeter of the system. These two stages of the application of intelligence tactics differ in means (tools), techniques and methods, reflected in the formal description of methods and tactics of cyber- attacks (MITRE ATT&CK Matrix) [2]. In the first stage, the violator seeks to obtain intelligence that allows him to use one of the types of computer attacks to infiltrate, legalize and consolidate in the system. In the second stage, intelligence is conducted after the implementation of each type of SCA that makes up the stages of the CCA and is supplemented with new data. The closer the violator is to the target of the CCA, the higher his awareness of the structural and functional indicators of the attacked DIS.

It should be noted that at both stages, the intruder is faced with the task of concealing the fact that the CCA is being conducted, as well as bypassing the security measures. Modern intrusion detection systems (IDSs) and intrusion prevention systems (IPSs) can promptly detect not only the presence of DI application during CCAs, but also the use of active reconnaissance methods. A number of studies note the use of controlled IDSs based on single-layer neural networks such as Long Short-Term Memory (LSTM) [3] and IDSs based on combined two-layer neural network architectures such as Bidirectional Long Short-Term Memory (BiLSTM) [4]. These methods allow for the effective detection of the use of SSAs, including at the stage of obtaining intelligence information using the "black box" method. This is extremely important for an intruder when conducting active reconnaissance from outside the network perimeter.

It should be noted that artificial intelligence (AI) is widely used to quickly identify and respond to CCAs. Blockchain technology provides secure data exchange and document verification. However, intruders have also begun to use cyber-attacks using artificial intelligence, which leads to privacy violations in the IoT and the emergence of blockchain vulnerabilities [5].

Artificial intelligence is also being introduced into quantum computing systems, which significantly increases the efficiency and reliability of quantum cryptographic systems. However, intruders have also begun to use such systems to crack cryptographic algorithms [6].

Penetration into the system and access by the intruder to the protected information are prevented by means of protection of various types. The use of firewalls, access control models and cryptographic protection of external and internal traffic ensure the confidentiality of information. The use of hash functions ensures the protection of authentication data and the integrity of information. The means of protection and the techniques of their application are constantly being improved. Thus, in [7], a genetic hybrid hashing algorithm and a method for its application based on hidden Markov models are proposed. This complicates the task of an intruder obtaining intelligence data that would allow him to launch a direct intrusion attack on a DIS.

However, the tactics and techniques of intruders are also being improved. Therefore, determining the patterns and dependencies of the possibility of using certain DI tactics and techniques on target objects on the composition of the ID available to the intruder, as well as his potential capabilities for obtaining intelligence at various stages of the CCA, remains a pressing task for effective proactive DI modeling. This study is devoted to solving this problem.

2. Research Methods

A number of normative, methodological documents and scientific papers are devoted to the description and research of methods and ways of conducting active reconnaissance. Thus, in the taxonomy of common attack patterns, CAPEC (Common Attack Pattern Enumeration and Classification), five meta patterns, seven standard patterns and five detailed attack patterns are attributed to this type of destructive impact (DI) [1]. These include, for example, CAPEC-169: Collecting information about the system/organization; CAPEC-292: Hosts detection; CAPEC-309: Network topology mapping; CAPEC-312: Active scanning of the operating system; CAPEC-497: Listening to network traffic; CAPEC-290: Scanning ports; CAPEC-291: Detecting network services; etc.

Adversarial Tactics, Techniques, and Common Knowledge (MITRE ATT&CK) is a knowledge base on cybercriminal behavior that describes tactics and techniques used in CAs [2,8]. It is presented in the form of a matrix that includes 14 tactics, one of which is computer intelligence tactics. This tactic includes 10 techniques, each of which is detailed into a number of sub-techniques. They are presented in Table 1.

Table 1. The structure of the "Reconnaissance" tactics of the MITRE ATT&CK taxonomy.

Active Scanning	**IP Block Scanning**		**Vulnerability Scanning**	**Wordlist Scanning**		
Collecting information about attacked nodes	Simple computer attacks		Software	Firmware update process		Client configurations
Collecting information about users	Credentials		E-mail addresses	Employee names		
Collecting information about attacked network infrastructure	Domain properties	DNS systems	Trusted Networks	Network Topology	IP Addresses	Network defense tools
Gathering information about an organization	Determining the physical location		Counterparties	Study of work schedule and delivery mode		Employee role identification
Phishing for information	Spear phishing via third-party services		Spear phishing with attachment	Spear phishing with link		Verbal spear phishing
Search in closed sources	Threat information providers			Acquiring technical data		
Search in public sources	DNS/Passive DNS		Digital certificates	WHOIS	CDNs	Database scanning
Search for open sites/domains	Social networks		Search engines	Code repositories		

The taxonomy of MITRE ATT&CK reconnaissance tactics and techniques is interconnected with the taxonomy of CAPEC attack patterns conducted in the interests of intelligence and reveals their content.

DI objects are defined at the network, hardware, system, application and user levels. At these levels, active computer reconnaissance is conducted to identify certain types of objects available to SCAs and their vulnerabilities. Thus, it is possible to determine the applicability of specific patterns, techniques and sub-technique of SCAs to the levels of defining DI objects.

Review of Research on This Topic

Modern computer attacks are complex in nature and represent a set of consistent SCAs on DI target objects of various levels, gradually bringing the intruder closer to achieving its ultimate goal. An approach developing a technique for modeling the structure and life cycle of cyber-attacks called Cyber Kill Chain is presented in [9–13]. According to this methodology, the violator begins the CCA by collecting intelligence about the attacked object, which, after the implementation of the next stage, is supplemented with new available intelligence. Thus, it should be noted that intelligence is conducted throughout the CCA, and the intelligence obtained allows us to determine the available types of attacks at its stages. In refs.[11,12], the typical CCA structure correlated with the Cyber Kill Chain model is presented in the form of stages implemented by computer attacks of a certain type, linked to the CAPEC taxonomy meta templates. This structure is shown in Figure 1.

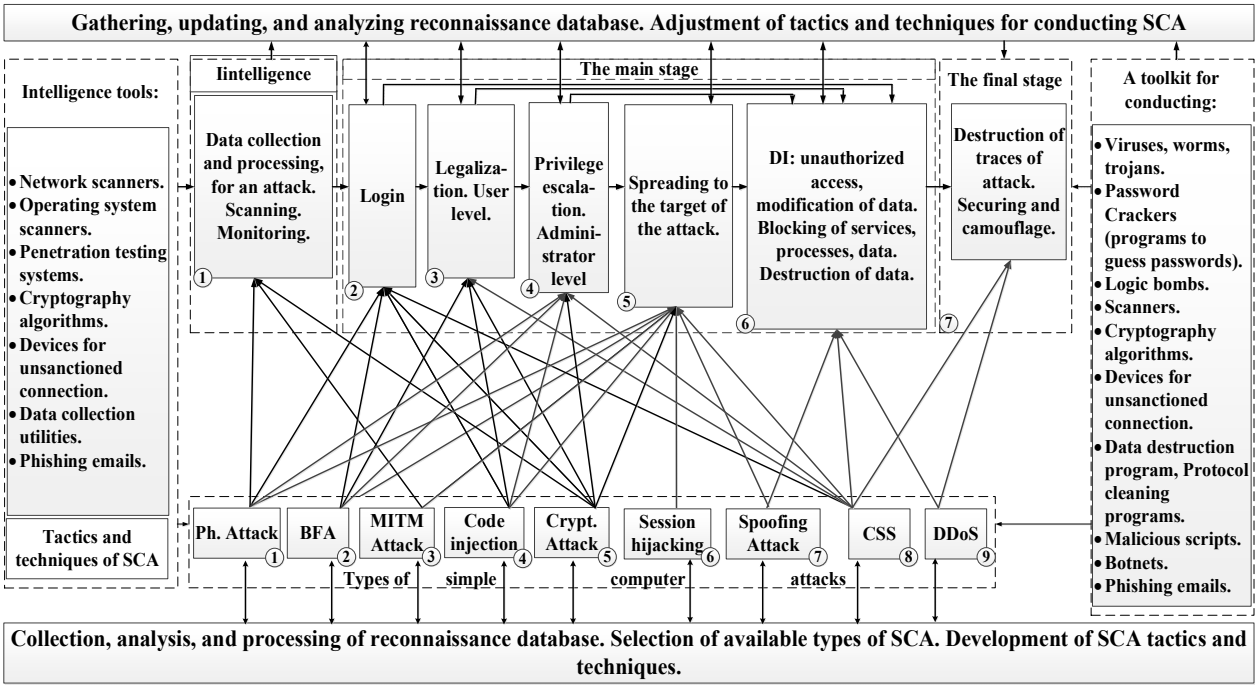

Figure 1. The structure of the CCA.

Modeling in the field of CCAs is also being developed by Positive Technologies, which has adapted the Cyber Kill Chain model to the taxonomy of tactics and techniques for implementing MITRE ATT&CK computer attacks and added security features blocking them. One of the latest developments of this company is the PT Dephaze software package, an automatic system for security assessment using penetration testing.

The analysis conducted in the scientific study [14] shows that attackers can bypass the IDS and IPS due to untimely updating of signatures and anomaly indicators. It is also noted that the use of network and host-level control in the IDS and IPS can improve the efficiency of detection and prevention of attacks in real time.

In practice, to ensure early identification of "visible" intruder objects of destructive influence (DI) and the possibility of committing certain types of attacks, symmetrical

methods of penetration testing or active audit are used. The following works are devoted to models, methods and standards for describing this process [15–18].

The Information System Security Assessment Framework (ISSAF) [15] methodology was developed by the Open Information Systems Security Group (OISSG) consortium and is an internal audit standard. It is convenient to use this technique at the stage of preliminary assessment of the security objects of the DIS (development of its structural and functional model and protection model of DIS), and at the stage of its operation.

The PTF (Penetration Testing Framework) [16] methodology provides a detailed guide on technology of penetration testing.

Unlike ISAF, this guide does not contain general theoretical information, but provides a fairly complete list of the facility's vulnerabilities, with practical recommendations on how to test and select tools for these purposes.

The PTES (Penetration Testing Execution Standard) was developed in 2009 by an international group of independent experts and enthusiasts in the field of information security [17]. The PTES provides seven main stages of penetration testing. A technical manual (PTES Technical Guidelines) is attached to this standard, detailing the main technical aspects of testing.

The Technical Manual (standard) of Special Publication 800-115 of NIST [18] is a practical guide to monitoring the security of the elements of the DIS; it is theoretical in nature, and it details the stages of penetration testing, including conducting reconnaissance and additional exploration of DIS elements.

As the analysis of these standards and techniques has shown, the structure of the penetration testing process is generally the same, differing only in the degree of detail and features of practical recommendations, and consists of the following stages:

(1) The development of a structural and functional model of the system under test and its protection model;
(2) The selection of testing tools:
    (a) application software, utilities;
    (b) hardware;
    (c) special radio-electronic equipment;
(3) Collecting information about the test object:
    (a) open-source intelligence (OSINT);
    (b) the use of social engineering methods;
    (c) analysis of social networks and contacts;
    (d) analysis of e-mail and telephone contacts;
    (e) network scanning;
    (f) analysis of the software used;
    (g) analysis of the hardware architecture of network nodes, switching equipment, peripheral equipment and information input/output devices;
    (h) security perimeter analysis;
(4) Vulnerability analysis of DI facilities at various levels;
(5) The identification of entry points and DI target objects;
(6) The identification of available CAs, tactics and techniques of implementation, patterns and vectors;
(7) The formation of the CCA template and vector;
(8) Practical implementation of penetration testing, adjustment ID, and the content of the next SCA after achieving the goals of the previous one;
(9) Preparation of a report and recommendations for adjusting the protection system of the elements of the DIS.

Reference [19] analyzed the works considering a fairly large list of threats aimed at critical infrastructure, as well as their localization in accordance with NIST recommendations. The results showed that the main reason for the implementation of information security incidents in the field of critical infrastructure is the human factor: low level of training, errors, negligence and the impact of social engineering techniques.

The conducted analysis allowed us to conclude that the scientific studies under consideration did not pay attention to important issues such as determining the degree of expansion of reconnaissance capabilities after the implementation of a certain stage of the SSA, determining the list of typical ID arrays available to the intruder at each of the DI levels, and determining the relationship between the content of the received ID and the possible SCA. It should be noted that one of the objectives of this study is to determine the applicability of the developed models and methods in practical activities for the training of information security specialists as well as in the course of assessing the risks of threat implementation and managing information security incidents.

3. Results and Discussion

3.1. The Development of Symmetric Models and Methods for Assessing the Awareness of the Intruder and Assessing the Intelligence Security of BIS Elements

To achieve the research objective, the authors developed symmetric models and methods for assessing the intruder's awareness and the intelligence security of DIS elements, designed to mathematically substantiate the required amount and semantic composition of the reconnaissance database for conducting the stages of the CCA, as well as the use of certain types of SCAs, tactics and techniques for their implementation.

In this study, to model the awareness of the violator at different stages of the CCA and determine the available types of SCA at different stages, a DIS with average structural–functional indicators was adopted, which has a basic set of information security tools and correctly formulated security policies.

To form the model, the analytical methods of the "black box", "gray box" and "white box" were applied, and the levels of identification of the objects of the DI, a system of structural–functional indicators, criteria for assessing the awareness of the violator about the elements of the DIS and their components, the typical structure of the CCA, and a scale for quantitative and qualitative assessment of the levels of awareness of the violator were determined. This conceptual model is presented in Table 2.

Let us move on to its description. In general, the modeling process boils down to the following actions. The model is divided into two clusters—computational and informational.

The calculation cluster displays the stages of the CCA (y_j) and $T(y_j)$—the linguistic terms of its description. For each of these stages, methods of investigation (testing) of the elements of the DIS are selected for the possibility of "DI "on them caused by the violator. These are the "black box" or "gray box" or "white box" methods. In the model, in relation to the previously discussed stages of the CCA, a scale of awareness of the violator about the structural–functional indicators of the attacked elements is formed in the DIS. This scale displays $T(x_i)$—linguistic terms for assessing awareness and numerical values of indicator X_i, reflecting the levels of awareness of the offender. The calculation of these characteristics is carried out using a preference function based on the theory of fuzzy sets.

The information cluster displays the ID received by the violator, according to the objects of the DI (the target objects of the SCA at the stages of the CCA) at various levels of their definition, which in the model are represented as $T(z_k)$—linguistic terms for describing the target objects of the CCA at the kth level of the awareness scale of the violator.

Table 2. The conceptual model for assessing the violator's awareness of DIS elements.

The Stage of a CCA	The Violator's Awareness of the Elements of a DIS			Information Security Threat Model Levels that Define DI Objects				
	Assessment Methods	Rating Scale	Calculation of Indicators	Network	Hardware	System	Application	User Defined
$T(y_j)$	«White box»	X_i, $T(x_i)$	$T_{X_i}(x_i;a,b) = \begin{cases} 0, x_i \le a \\ \frac{x_i-a}{b-a}, a \le x_i \le b \\ 1, x_i \ge b \end{cases}$	$T(z_k)$	$T(z_k)$	$T(z_k)$	$T(z_k)$	$T(z_k)$
$T(y_n)$	«Gray box»	X_n, $T(x_n)$		$T(z_n)$	$T(z_n)$	$T(z_n)$	$T(z_n)$	$T(z_n)$
.....		.....		.....	.....	.....	.....	.....
$T(y_3)$		X_3, $T(x_3)$		$T(z_3)$	$T(z_3)$	$T(z_3)$	$T(z_3)$	$T(z_3)$
$T(y_2)$		X_2, $T(x_2)$		$T(z_2)$	$T(z_2)$	$T(z_2)$	$T(z_2)$	$T(z_2)$
$T(y_1)$	«Black box»	X_1, $T(x_1)$		$T(z_1)$	$T(z_1)$	$T(z_1)$	$T(z_1)$	$T(z_1)$
Computational cluster				**Available data on awareness level**				

Let us consider in more detail the methodology of the formation and functioning of this model. Let us start with the foundation of its structure. To form the lower tier of the model, the "black box" system analysis method is used [20]. The method under consideration is based on the fact that the researcher, in this case the violator, is not aware of either the structural or functional indicators of the system under study. He knows the entry point into the system, where certain data or signals can be sent, and the exit point through which the intruder receives data transformed by the internal elements of the system, which can be used to determine a certain part of the structural and functional indicators of the system. Such a state of awareness of the intruder about the attacked system will correspond to the stage of conducting reconnaissance from outside the network perimeter.

Next, it is necessary to determine the upper tier of this model, which is conventionally designated as a "white box" in accordance with the applied testing methodology [21].

When using the "white box" method, the violator knows the full set of structural and functional indicators of the system under study. These are many network protocols and services at the system and application levels, many vulnerabilities of all protocols and services at the system and application levels, many hardware architectures and embedded software, many configurations and many IP addresses.

Testing of the system, the structural and functional characteristics of which are partially known to the violator, will be carried out using the "gray box" method [22]. The proposed methodology includes a step-by-step increase in this level. Each of the stages is characterized by different possibilities.

We will divide the awareness scale using the tools of fuzzy logic and linguistic terms [23–25] (Table 2).

Linguistic terms are the values of a linguistic variable that represent words or sentences in a natural or formal language that serve as an elementary characteristic (description) of information security events (incidents) [23].

To form the awareness scale, we will introduce the following notation:

X—invader's awareness $X \in [0;1]$;

X_i—invader's awareness levels $X_i \in \{[0;0.2], [0.2;0.4], [0.4;0.6], [0.6;0.8], [0.8;1]\}$;

x_i—the numerical value of the invader's awareness at a certain level;

y_j—the stages of the CCA;

z_k—possible DI target objects at the kth level of their definition;

$T(x_i)$—the linguistic terms of awareness assessment;

$T(y_j)$—the linguistic terms describing the stages of the CCA;

$T(z_k)$—the linguistic terms describing target objects of the CCA.

Based on the data presented in Table 3, it becomes necessary to determine whether a certain category of awareness belongs to a specific level of the offender's awareness scale according to the elements of the DIS. For this purpose, the mathematical apparatus of membership functions of fuzzy sets is used.

Table 3. Splitting the awareness scale using linguistic terms.

The Scale of Awareness Levels *Xi*	**[0;0.2]**	**[0.2;0.4]**	**[0.4;0.6]**	**[0.6;0.8]**	**[0.8;1]**
Linguistic terms for assessing awareness $T(x_i)$	VL	L	M	H	VH
Linguistic terms describing the stages of CCA $T(y_j)$	Reconnaissance	Reconnaissance, login, legalization	Reconnaissance, login, legalization, privilege enhancement	Reconnaissance, login, legalization, privilege enhancement, dissemination	Reconnaissance, login, legalization, privilege enhancement, DI
Linguistic terms for describing CCA targets $T(z_k)$	Externally accessible network objects of the attacked DIS element	The attacked node of the DIS element network	DI objects of the attacked DIS element, available according to the access control model	DI objects of the attacked DIS element, accessible nodes of the network of interacting elements of the DIS	Objects of DI of the attacked element and interacting elements of the DIS

The membership functions of fuzzy sets allow us to describe the degree to which a certain category of awareness belongs to a specific level of the awareness scale, in the range from 0 to 1. This makes it possible to more flexibly analyze and classify the level of knowledge of the violator regarding the elements of the DIS, taking into account their probabilistic nature [25].

The awareness scale is an ordered set of levels, each of which characterizes a certain set of arrays of ID received by the intruder about objects of the DI elements of the DIS. The content of the received ID allows us to determine the available SCAs and apply tactics and techniques for their implementation, which are characteristic of the corresponding stage of the CCA.

Each level of awareness is described by the membership function, which sets the degree to which a specific value of the awareness indicator corresponds to this level.

For each level of awareness, the membership function $T(x_i)$ is set, where (x_i) is the numerical value of the degree of awareness.

The awareness level membership function $T(x_i)$ takes values in the range [0;1]. It can take extreme values: ((x_i) = 1)—full correspondence of the degree of awareness (x_i) to this level and и ($T(x_i)$ = 0)—the absence of belonging of the degree of awareness (x_i) to this level. Values between 0 and 1 reflect a partial degree of compliance with any kind of level of awareness.

Let us represent this function as an expression:

$$T_{X_i}(x_i; a, b) = \begin{cases} 0, x_i = a \\ \frac{x_i - a}{b - a}, a < x_i < b \\ 1, x_i = b \end{cases}$$

where (a, b) is the range of a specific level of the awareness scale.

Using this method, we will obtain the relative values of x_i for each diapason of the offender's awareness scale, which ranges from 0 to 1.

As noted earlier, the awareness scale includes five levels: "very low" (VL), "low" (L), "medium" (M), "high" (H) and "very high" (VH).

For a "very low" (VL) level of awareness, which characterizes minimal knowledge about the system, the range is set as [0;0.2] and the following function of this level is formed:

$$T_{X_1}(x_i; 0, 0.2) = \begin{cases} 0, x_i = 0 \\ \frac{x_i - 0}{0.2}, 0 < x_i < 0.2 \\ 1, x_i = 0.2 \end{cases}$$

This function has the following values:

If (x_1 (x_i;0,0.2) = 0, then the intruder does not have the necessary ID to apply attack scenarios available for the VL level;

If Tx_1 (x_i;0,0.2) = 1, then the ID are sufficient to apply all attack scenarios available at the VL level, and the violator also has the opportunity to switch to a low awareness level (L) and expand intelligence capabilities;

If Tx_1 (x_i;0,0.2) = $\frac{x_i - 0}{0.2}$, the ID were not fully received and the intruder may conduct additional reconnaissance and attacks aimed at obtaining the missing ID necessary to move to the next level of awareness.

Next, let us consider the "low" level of awareness, at which the intruder has basic ID about the structure and functionality of the system and the attacked object of DI. For this level X_2, the values of the indicator x_i are set in the range [0.2;0.4] and the following function is formed:

$$T_{X_2}(x_i; 0.2, 0.4) = \begin{cases} 0, x_i = 0.2 \\ \frac{x_i - 0.2}{0.2}, 0.2 < x_i < 0.4 \\ 1, x_i = 0.4 \end{cases}$$

Based on this function, the following conditions are formed:

If Tx_1 (x_i;0.2,0.4) = 0, then the violator does not have the necessary ID to move to this level of awareness;

If T_{X1} (x_i;0.2,0.4) = 1, then the available ID are sufficient to apply all types of attacks available at this level of awareness, move to the next level and conduct further reconnaissance with new features;

If Tx_1 (x_i;0.2,0.4) = $\frac{x_i - 0.2}{0.2}$, the ID have not been fully obtained and are insufficient for the use of all types of attacks available at this level of awareness, and the use of additional intelligence tools is necessary.

At the awareness level, the "medium" intruder has sufficient knowledge to analyze the system structure, configuration and characteristics of the available DI objects of the attacked system element. The values of the indicator x_i for this level X_3 are set in the range [0.4;0.6], on the basis of which the following function is formed:

$$T_{X_3}(x_i; 0.4, 0.6) = \begin{cases} 0, x_i = 0.4 \\ \frac{x_i - 0.4}{0.2}, 0.4 < x_i < 0.6 \\ 1, x_i = 0.6 \end{cases}$$

Based on the above function, the following can be said:

The intruder does not have ID corresponding to this level and so cannot carry out possible attacks available for this level if the value of the function x_3 is 0, i.e., Tx_1 (x_i;0.4,0.6) = 0;

If Tx_1 (x_i;0.4,0.6) = $\frac{x_i - 0.4}{0.2}$, then the intruder does not have the full volume of ID arrays that correspond to this level of awareness, and additional means of reconnaissance are needed to achieve this;

The violator has the full amount of information available at this level, if Tx_1 (x_i;0.4,0.6) = 1, and so moves to the next level of awareness and can take advantage of new opportunities for intelligence and conducting an SCA.

ID corresponding to the "high" awareness level allows the intruder to determine the structure of all elements of the DIS, as well as the characteristics of all DI objects in the attacked DIS element. The values of the indicator x_i for this level X_4 will correspond to the range [0.6;0.8]. Thus, the following membership function is formed:

$$T_{X_1}(x_i; 0.6, 0.8) = \begin{cases} 0, x_i = 0.6 \\ \frac{x_i - 0.6}{0.2}, 0.6 < x_i < 0.8 \\ 1, x_i = 0.8 \end{cases}$$

The following gradations are allocated for this membership function:

The expression $T(x_1$ (x_i;0.6,0.8) = 0 means that the minimum ID have been obtained to achieve the "high" awareness level, but not to take its capabilities;

Tx_1 (x_i;0.6,0.8) = $\frac{x_i - 0.6}{0.2}$ corresponds to incomplete acquisition of ID characteristic of a given level of awareness, according to which not all types of SCAs of the "high" awareness level will be available and it is necessary to continue collecting ID;

Tx_1 (x_i;0.6,0.8) = 1 corresponds to the violator obtaining all possible ID at a given level in terms of the characteristics of the available DI objects DI of DIS elements, as well as the structure and functionality of the DIS elements and the possibility of using all types of SCAs at this level and moving to the next level of awareness.

The fifth level of awareness is "very high." At this level, the intruder receives data on the characteristics of all DI objects of all DIS elements and full access to them. The values of the indicator x_i for this level X_5 are set in the range [0.8;1] and the following membership function is formed:

$$T_{X_5}(x_i; 0.8, 1) = \begin{cases} 0, x_i = 0.8 \\ \frac{x_i - 0.8}{0.2}, 0.8 < x_i < 1 \\ 1, x_i = 1 \end{cases}$$

The following conditions are formed for the membership function of this level:

If Tx_1 (x_i;0.8,1) = 0, the intruder has the necessary ID to move to this level of awareness, but they are not enough to carry out attacks available at this level;

If Tx_1 (x_i;0.8,1) = 1, then ID are sufficient to apply all types of available attacks for a given level;

If Tx_1 (x_i;0.8,1) = $\frac{x_i - 0.8}{0.2}$, then in order to carry out all types of SCA available for this level, additional ID are required.

Collectively, the ranges of changes in the values of the indicators presented above represent a scale of awareness of the violator.

This model and methodology can be symmetrically used to assess the intelligence security (IS) of DIS elements. For this purpose, we will introduce hi, which is an indicator of intelligence security assessment, and Hi, which reflects the range of its values for the intelligence security assessment scale. Their numerical values will be calculated using the following formula:

$$T_{H_i}(h_i; a; b) = 1 - T_{X_i}(x_i; a; b)$$

The linguistic terms used in the intelligence security model are the same as in the intruder awareness assessment model. Consequently, the scale for assessing intelligence security will be inversely symmetrical in terms of the values of the range of the scale for assessing the intruder's awareness. Their ratios are shown in Table 4.

Table 4. Inversely symmetrical ratio of ranges for assessing the awareness of the violator and the intelligence security of DIS elements.

Linguistic terms of the scale for assessing the awareness of the violator $T_{Xi}(x_i;a,b)$	VL	L	M	H	VH
Linguistic terms of the scale for assessing the IS of elements DIS $T_{Hi}(h_i;a,b)$	VH	H	M	L	VL
Numerical values of the scale ranges	[0;0.2]	[0.2;0.4]	[0.4;0.6]	[0.6;0.8]	[0.8;1]

Thus, this methodology substantiates the dimension of the awareness scale, substantiates the type of membership function of a fuzzy set and provides a decoding of linguistic terms of various origins. In addition, with the help of the awareness membership function, additional information is obtained on the compliance of the ID content with a specific level of awareness. This technique also allows you to identify DI objects based on a specific level of awareness that the intruder can access and the list of SCAs available for this level.

In addition, it is clarified that the violator, starting from the "medium" awareness level, has the opportunity to conduct reconnaissance within the DIS elements and at the "high" and "very high" awareness levels has the opportunity to extend to the interacting DIS elements and conduct reconnaissance of their structural–functional characteristics. Thus, by applying in practice the models and techniques presented in this study, an information security specialist has the opportunity for a priori dynamic assessment of changes in the intelligence security indicators of the DIS elements depending on the type of applied SCA and the stages of the CCA.

3.2. Development of Experimental Models

In order to test the developed model and methodology, we will conduct an experiment, for which it is necessary to generate the initial data. The formation of initial data to assess the intruder's awareness and intelligence security of the DIS involves the collection and systematization of key information about the structural–functional characteristics of its elements and the vulnerabilities of DIS objects.

The initial data consider the DIS, which consists of three elements: local area networks, a data center, and a remote user. Each of the network elements consists of a certain number of switching equipment (SE) devices and network nodes (NNs), which are presented in Table 5. Table 5 also presents data on the applied models of access control and inter-network interaction within the DIS.

Table 5. Structure of DIS elements, applied access control and inter-network interaction.

Inter-Network Interaction	**Local Area Networks (LANs)**	**Data Center (DC)**		**Remote User (RU)**
LAN Segment1 DC; RU Segment1 DC; Segment1-Segment2 DC	Firewall 1.1 Router 1.1 Switch 1.1 Server 1.1 **AW1.1** AW1.2 AW1.3 . . . . . . AW1.n	Firewall 2.1 Router 2.1 Switch 2.1		Firewall 3.1 AW3.1
		Virtualization Server 2.1 **Server 2.1** AW2.1 . . . . . . AW2.n	Container Virtualization Server 2.1 Container 2.1 . . . . . Container 2.n **Database Server 2.1**	
	No	Segment1	Segment2	No
		Access control		

Figure 2 shows a model of active intelligence, which is carried out by an intruder from outside the perimeter of the network.

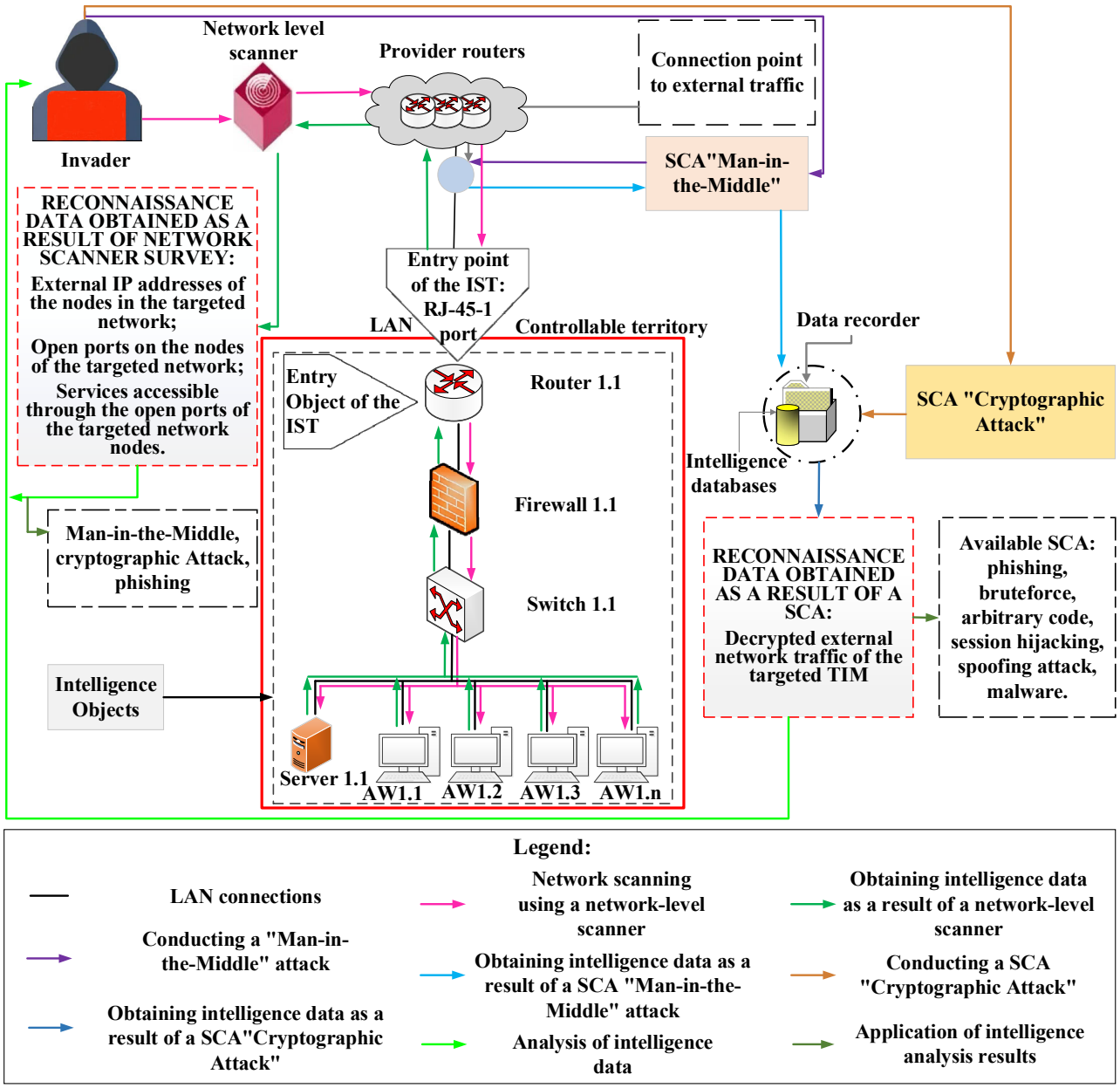

Figure 2. Simulation of the "black box" method of the CCA stage—conducting active reconnaissance from outside the network perimeter.

At the stage of collecting initial information about the attacked object, the attacker uses some tools to obtain information from outside the network perimeter. The main purpose of this stage is to collect ID necessary for penetration, implementation and legalization on one of the devices (NN or SE) of the attacked DIS element. To do this, the intruder uses a network-level scanner and certain types of SCAs suitable for intelligence gathering.

The intruder connects a network-level scanner through the routers of the telecom operator to the entrance of the attacked element of the DIS and, as a result of scanning, receives data on the following objects of DI: IP addresses of external network nodes; open ports of network nodes; services accessible through open ports of network nodes.

If the access control model (ACM) is configured correctly, services will be unavailable through open ports. In the experiment being conducted, open ports will be those ports that

ensure the formation of the network and intra-network interaction. Based on the developed methodology, we assess the violator's awareness of the elements of the DIS. Comparing the data obtained during this stage, it can be concluded that the ID obtained correspond to a very low level of awareness. The results are shown in Table 6.

Table 6. Indicators of the level of "very low awareness of the violator".

The Stage of the CCA	The Violator's Awareness of the Elements of the DIS	Levels of Identification of DV Objects				
		Network	Hardware	System	Application	User defined
ID gathering	Very low: $0.2 > \frac{N_{ODIin.}}{N_{ODItotal}} \geq 0$	External IP addresses; external open node ports; encrypted external traffic	No data available	No data available	No data available	No data available
	Evaluation method: «black box»	**Available data on awareness level**				

In this case, the data obtained were insufficient to carry out an attack to introduce and legalize the network, and no vulnerabilities were found. Therefore, the attacker uses SCA services that allow them to obtain the data necessary to enter the network, legalize, identify and authenticate on the network node as a legitimate user.

In the experiment, such an attack is the CAPEC-94: Adversary in the Middle (AiTM) Man-in-the-Middle attack, which exploits the CVE-2023-50703 vulnerability. Its essence is as follows. The intruder, in some way, connects to the line between the attacked element of the DIS and the provider, gains access to external encrypted network traffic and records it, creating ID. Since external traffic is protected by encryption, the intruder uses another type of SCA "Cryptographic attack" CAPEC-463: Padding Oracle Crypto Attack and CAPEC-20: Encryption Brute Forcing, which exploits CVE-2018-12404. With the help of cryptographic algorithms, he can decrypt the received ID.

A phishing attack can also be used to obtain the ID necessary for implementation and legalization.

After analyzing the ID, the violator uses them to introduce and legalize himself on the network. For these purposes, the attacker conducts a CAPEC-49 brute force attack: Brute-force, the password, determines the user credentials on ARM 1.1, 1.3 and Server 1.1, using the vulnerability CVE-2025-49195. Next, he performs identification and authentication on the LANs as a legal user and takes them under external control. As a result of the attack, the intruder is introduced and legalized in the attacked element of the DIS (Figure 3).

Thus, the intruder has the opportunity to move to the "low" level of awareness of the corresponding scale and apply the "gray box" testing method, which allows him to obtain additional ID. The model of the "Implementation and legalization in the network" stage of the CCA is shown in Figure 3, and the arrays of ID available to him are presented in Table 7.

Next, using the "gray box" method, we conduct modeling of the "Privilege Elevation" stage of the CCA. Figure 4 shows an example when an infringer, having obtained the rights of users of AWs 1.1, 1.2 and Server 1.1, implements the operating system (OS)-level scanner software (SW) on them. The OS-level scanner is used to identify SW vulnerabilities, available network nodes (NNs), and obtain the data necessary to achieve the goal of this stage, which is to upgrade privileges to the network administrator level. Based on the obtained data (the presence of vulnerabilities CVE-2025-8453-CWE-269), the intruder decides to increase privileges on ARM 1.1. and carries out a CAPEC-233: Privilege Escalation attack. As a result of increasing privileges to the network administrator level, the intruder gains access to all the interacting DIS elements and the ability to scan them with a network-level

scanner, having received the necessary ID for carrying out the "Distribution" stage of the CCA. Thus, he moves to a new level of awareness. The arrays of ID available to him are reflected in Table 8.

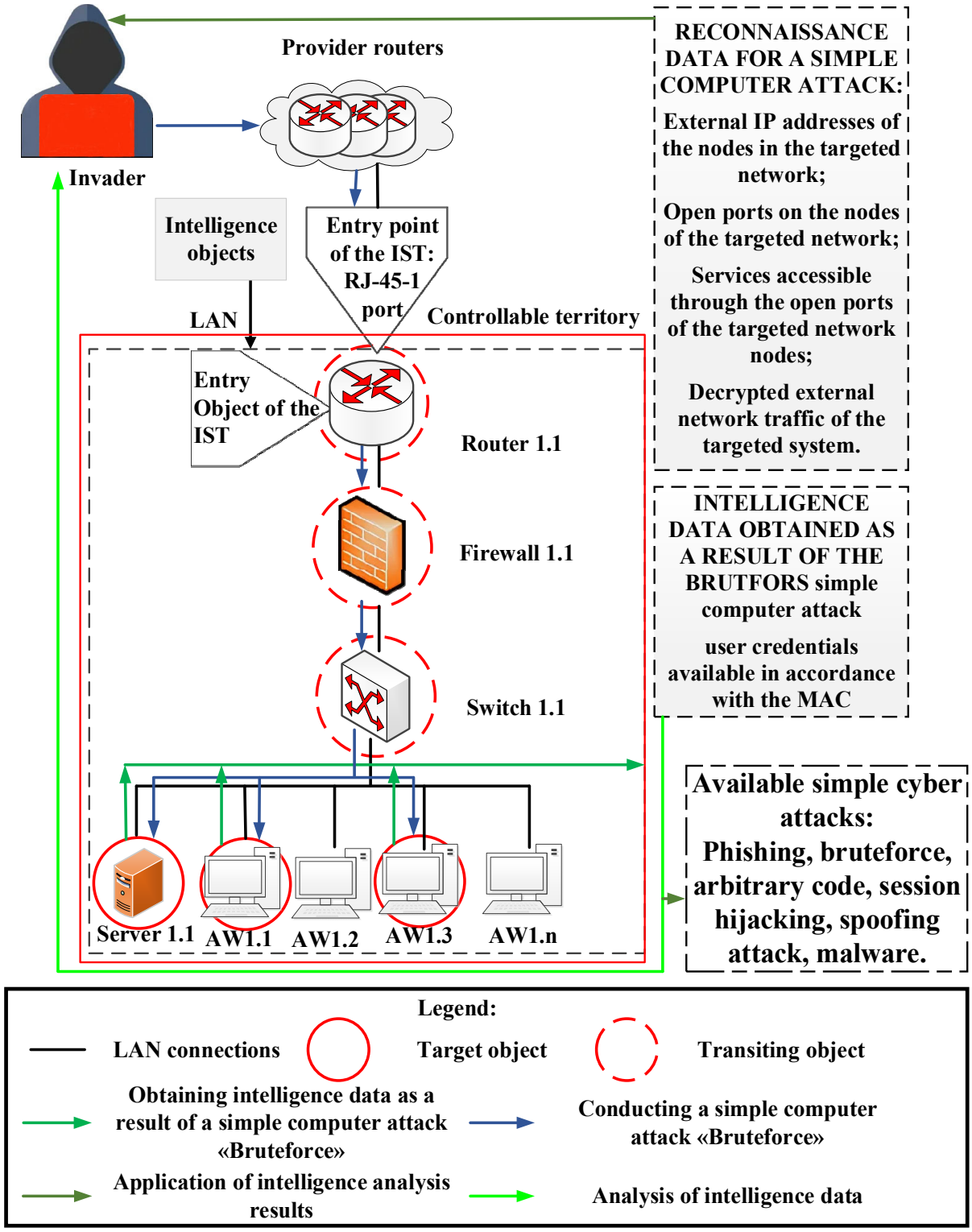

Figure 3. "Gray box" simulation of the CCA stage—implementation and legalization in the network.

Table 7. Indicators of the level of "low awareness of the violator".

The Stage of the CCA	The Violator's Awareness of the Elements of the DIS	Levels of Identification of DV Objects				
		Network	Hardware	System	Application	User defined
Penetration, legalization, ID gathering	«Low» $0.4 > \frac{N_{ODIin.}}{N_{ODItotal}} \geq 0.2$	Data on the attacked NN:				
	Evaluation method: "grey box"	External IP addresses; external open node ports; encrypted external traffic	No data available	Protocol vulnerabilities on an external IP address	Vulnerabilities of protocols and services on the external IP address of the port	User credentials
		Available data on awareness level				

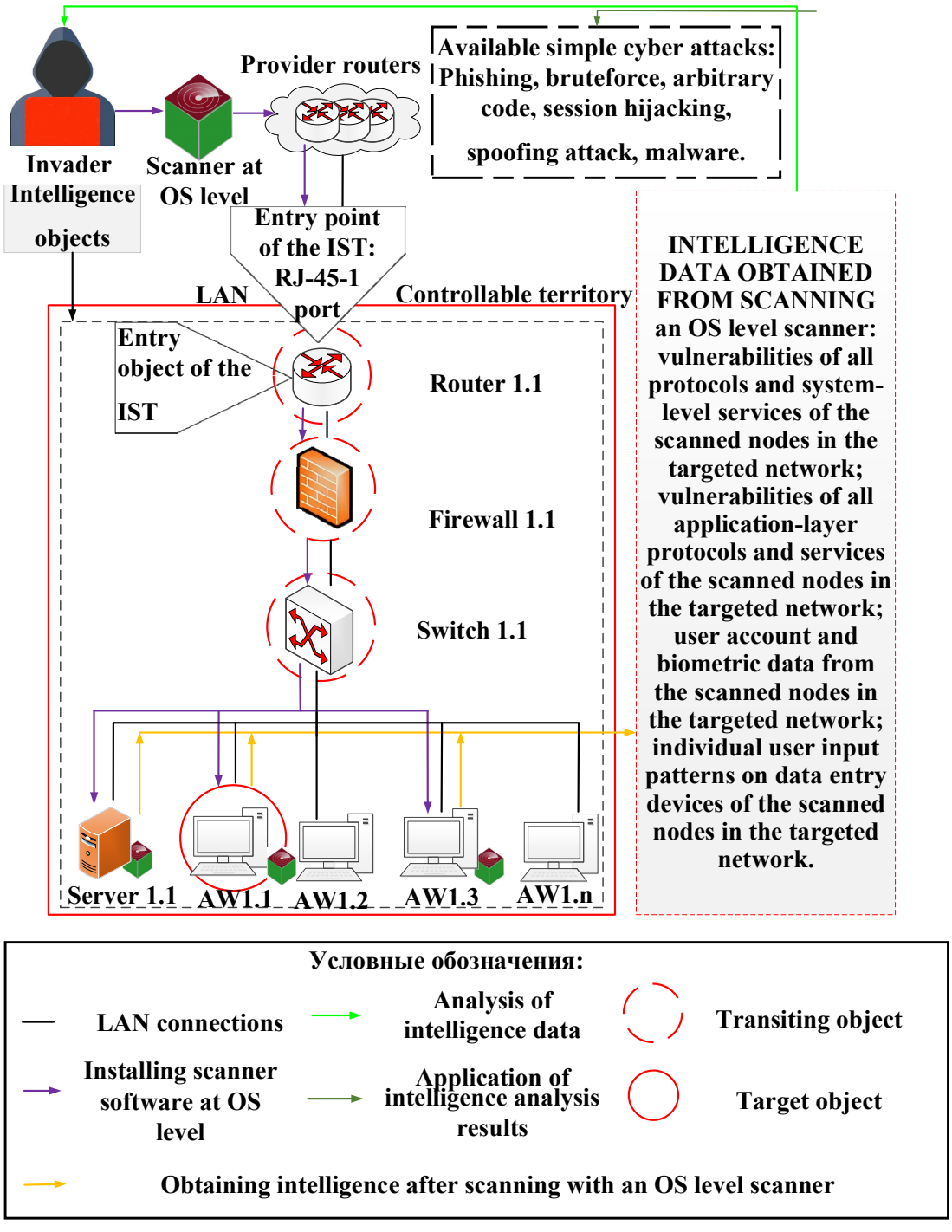

Figure 4. "Grey box" simulation of the CCA stage—privilege escalation.

The "Spread" stage of a CCA is shown in Figure 5. To implement it, the intruder installs a network-level scanner at AW 1.1.

Table 8. Indicators of the level of "medium awareness of the violator".

The Stage of the CCA	The Violator's Awareness of the Elements of the DIS	Levels of Identification of DV Objects				
		Network	Hard Ware	System	Application	User Defined
		Data on the Attacked NN in Accordance with the ACM:				
Privilege escalation, penetration, legalization, ID gathering	Medium $0.6 > \frac{N_{ODIin.}}{N_{ODItotal}} \geq 0.4$	View of a network node of a DIS element; IP addresses; open ports; encrypted external traffic.	Types and specification of hard ware architecture, embedded SW of NN and their vulnerabilities.	OS types and specification; vulnerabilities and types of all network protocols and control systems (CSs); ACM; file systems; drivers; process management subsystems.	Types and specification of ASW; all network protocols and application layer services; vulnerabilities in application-level protocols and services.	Types and specification of user-level devices and their vulnerabilities; credentials and biometric data of users of the NN; the individual handwriting of the users of the NN.
	Evaluation method: "gray box"	Available data on awareness level				

By scanning with a network-level scanner from automated workplace 1.1, the intruder receives data on the points of transition to the interacting elements of the DIS, access to the elements of the interacting elements of the DIS in accordance with the ACM, and the presence of vulnerabilities in these elements. As a result, the intruder receives information about the configuration and types of NNs available in accordance with the ACM, their hardware architecture, embedded SW, their vulnerabilities, network protocols and services at the system and application levels, and user credentials. By increasing their privileges after being legalized on the network, the violator gains access to additional data on the attacked NNs, which corresponds to an average awareness of the elements of the DIS. However, the data obtained as a result of scanning using a network-level scanner from AW 1.1 LAN do not allow access to the target object of the CCA—the Database Server 2.1 of the Data Center (DC), because the LAN interacts with segment 1 of DC, and Database Server 2.1 is part of Segment 2. To obtain the missing data, the intruder implements the OS scanner SW on the objects of DI of the DC and the remote user available in accordance with the access control model and the vulnerabilities found.

After the SW scanner is implemented, data are obtained on vulnerabilities in the protocols and services of the system and application layer of the NN and SE of interacting elements of the DIS, as well as user credentials, biometric data, and the individual handwriting of their work on data entry devices.

As a result, the attacker discovers the vulnerability and exploits CVE-2018-20735, which is necessary to conduct a CAPEC-652: Use of Known Kerberos Credentials attack to propagate and escalate privileges on Data Center Server 2.1. By spreading through the network, the violator increases his awareness of the elements of the DIS in accordance with the evaluation criteria to a high level, which gives him access to move to the next level to carry out a DI attack. The arrays of available RDs of this level are shown in Table 9.

At this point, the "gray box" testing stage is complete.

Testing at the stage of high intruder awareness is carried out using the "white box" method. Its model is presented in Figure 6.

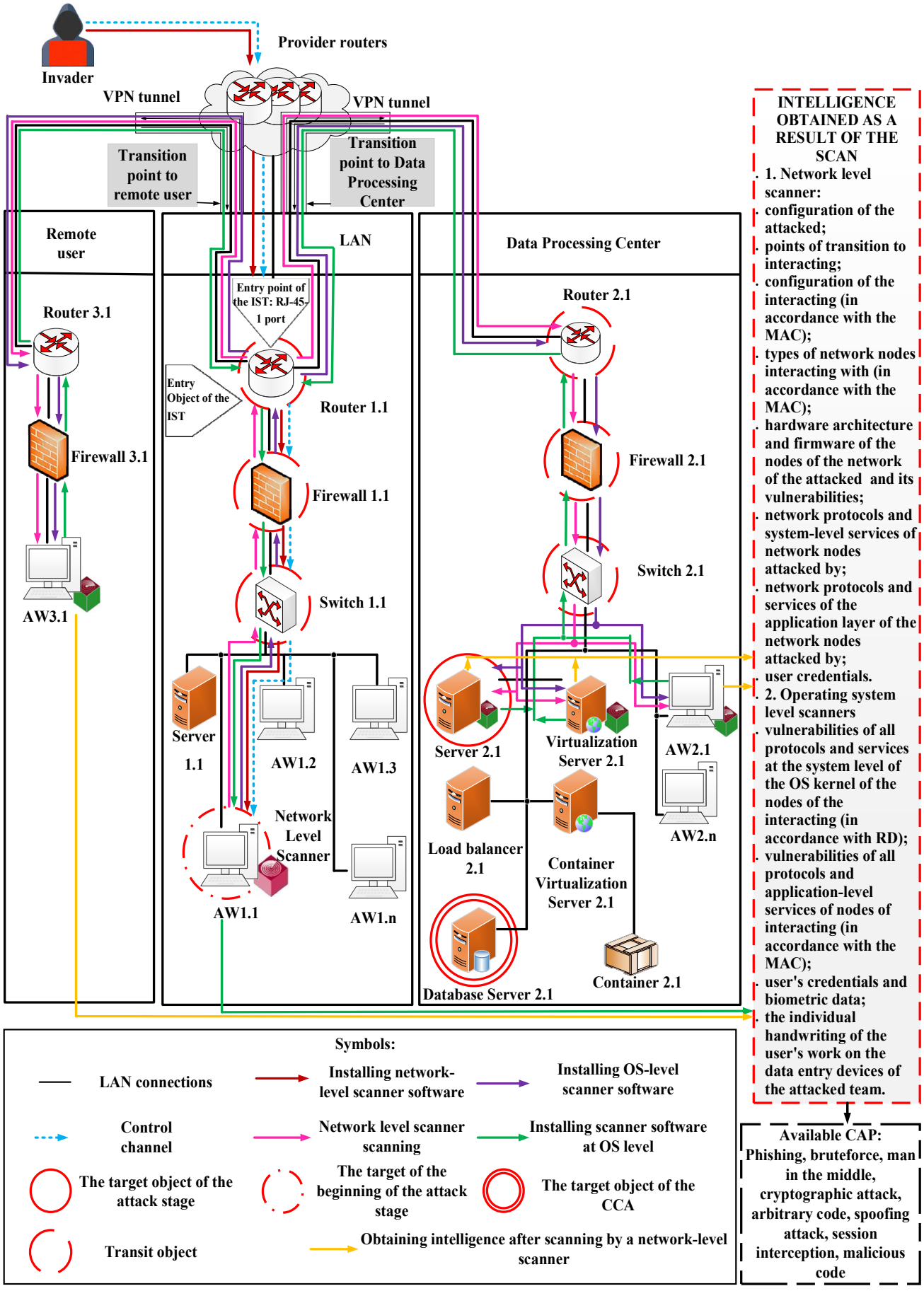

Figure 5. "Gray box" simulation of the CCA stage—propagation in the system.

Table 9. Indicators of the levels of "high awareness of the violator".

The Stage of the CCA	The Violator's Awareness of the Elements of the DIS	Levels of Identification of DV Objects				
		Network	**Hardware**	**System**	**Applica- tion**	**User defined**
Proliferation, privilege escalation, penetration, legalization, ID gathering		**Data on available NN:**				
	High: $0.8 > \frac{N_{ODIin.}}{N_{ODItotal}} \geq 0.6$	Configuration of available NN; entry and transition points on accessible NN; types of available NN; all IP addresses; open ports; encrypted external traffic.	Types and specification of hardware architecture, embedded SW of NN and their vulnerabilities.	OS types and specification; vulnerabilities and types of all network protocols and control systems (CSs); ACM; file systems; drivers; process management subsystems.	Types and specification of ASW; all network protocols and application layer services; vulnerabilities in application-level protocols and services.	Types and specification of user-level devices and their vulnerabilities; credentials and biometric data of users of the NN; the individual handwriting of the users of the NN.
	Evaluation method: "gray box"	**Available data on awareness level**				

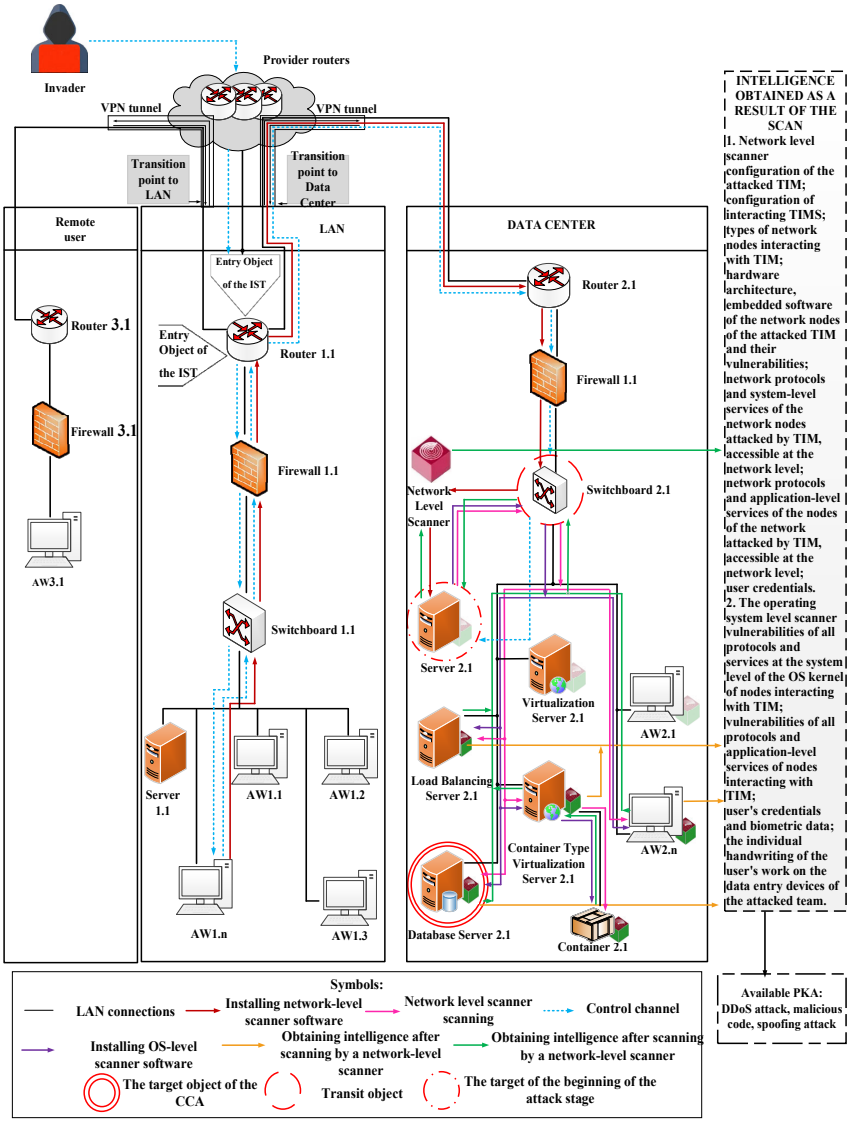

Figure 6. "Gray box" modeling of the CCA stage—implementation of destructive impact.

At this stage, the violator has a complete array of ID on all potential objects of DI of elements of the DIS. Having elevated privileges on Server 2.1 of the Data Center to the network administrator level, the attacker exploits the CVE-2021-41379 vulnerability and, having carried out a CAPEC-122 "Abuse of Privilege" attack, gains access to the target object of the CCA DV—Server 2.1 of the Data Center and gains the ability to take over the data center database. This completes the "white box" testing phase. The results are presented in Table 10.

If necessary, the numerical values of the intruder awareness indicator can be converted into numerical values of the indicator for assessing the intelligence protection of RIS elements.

The results of the experiments conducted to verify the practical applicability of the developed models and techniques confirm the possibility of proactive assessment of the awareness of the violator and analyzing the typical ID arrays available to him.

Table 10. Indicators of the levels of "very high awareness of the violator".

The Stage of the CCA	**The Violator's Awareness of the Elements of the DIS**	**Levels of Identification of DV Objects**				
		Network	**Hardware**	**System**	**Application**	**User defined**
		Data on all network nodes:				
Destructive impact, proliferation, privilege escalation, penetration, legalization, ID gathering	Very high: $1 \geq \frac{N_{ODIin.}}{N_{ODItotal}} \geq 0.8$ Evaluation method: "white box"	Element configuration; entry and transition points to interacting elements; types of NN; all IP addresses and open ports of NN; decrypted network traffic.	Types and specification of the entire hardware architecture and embedded SW of NN and their vulnerabilities.	OS types and dpecification; vulnerabilities and types of all network protocols and services of NN; ACM; file systems; drivers; system-level process management subsystems.	Types and specification of ASW; vulnerabilities and types of all network protocols and application layer services.	Types and specification of user-level devices and their vulnerabilities; accounting and biometric data and individual handwriting of the users of the NN.
		Available data on awareness level				

4. Conclusions

In conclusion, the authors would like to note that this study was conducted on a very relevant topic. Its novelty lies in the fact that for the first time at the system level, the scientific task was performed to determine the typical arrays of identifiers available to an attacker after passing through the stages of CCA "Penetration and legalization", "Privilege escalation", "Proliferation" and "Destructive impact", as well as their dependence on the arsenal of potentially feasible types of attacks. It has been established that the contents of the arrays of identifiers do not depend on the techniques used for achieving the goal of the CCA stage, but depend on the security policies applied to the DIS element. A system of standard models has been developed for testing the capabilities of the attacker to carry out active intelligence and DI for various SCA scenarios. These models are universal, because they assume the formation of the studied elements of a DIS by entering source data on the network, hardware and software infrastructure, as well as the applied security measures.

The obtained ID arrays are distributed according to the levels of identification of objects of DI. The developed methodology for determining awareness levels makes it possible to quantify and qualitatively evaluate ID arrays and transfer them to the category of standard ones corresponding to one of the assessment levels of the awareness scale or the intelligence assessment scale symmetrical to it.

The models and methods presented in this study can be used both for proactive assessment of the security of DIS elements and in the course of information security incident management. Currently, the results of this study are used as part of the software for the information and calculation part of the decision support system when assessing the security of DIS elements.

The direction of further research in this area is the development of neuro-Bayesian ontological structural and functional models of DI on DIS elements, enabling us to automate the formation and determination of preferred scenarios and vectors of the CCA.

Author Contributions: methodology, formal analysis, writing—original draft: V.V.B.; conceptualization, validation, funding acquisition, visualization, writing—original draft: A.A.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

Conflicts of Interest: The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

References

1. CAPEC (Common Attack Pattern Enumeration and Classification)—A Standard for Describing Attack Classes and Their Hierarchical Relationships, a Catalog of Known Cyberattacks. Available online: https://capec.mitre.org (accessed on 18 April 2025).
2. MITRE ATT&CK Matrix–Formal Description of Techniques and Tactics for Implementing Cyber-Attacks. Available online: https://attack.mitre.org/ (accessed on 25 July 2025).
3. Almedires, M.A.; Elkhalil, A.; Amin, M. Adversarial attack detection in industrial control systems using LSTM-based intrusion detection and black-box defense strategies. *J. Cyber Secur. Risk Audit.* **2025**, *2025*, 4–22. [CrossRef]
4. Wei, Y.; Wu, F. Self-adaptive intrusion detection model based on Bi-LSTM-CRF using historical access logs. In *Proceedings on Advances in Natural Computing, Fuzzy Systems, and Knowledge Discovery: Proceedings of the ICNC-FSKD 2021 Conference 17*; Springer International Publishing: Cham, Switzerland, 2022; pp. 185–197.
5. Radanliev, P. Cyber diplomacy: Defining the opportunities for cybersecurity and risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing. *J. Cyber Secur. Technol.* **2024**, *9*, 28–78. [CrossRef]
6. Radanliev, P. Artificial intelligence and quantum cryptography. *J. Anal. Sci. Technol.* **2024**, *15*, 4. [CrossRef]
7. Alshuaibi, A.; Arshad, M.W.; Maayah, M. A hybrid genetic algorithm and hidden markov model-based hashing technique for robust data security. *J. Cyber Secur. Risk Audit.* **2025**, 42–56. [CrossRef]
8. Al-Shaer, R.; Ahmed, M.; Al-Shaer, E. Statistical Learning of APT TTP Chains from MITRE ATT&CK. In Proceedings of the RSA Conference 2017, San Francisco, CA, USA, 13–17 February 2017; pp. 1–2. Available online: https://www.researchgate.net/publication/351452885_Assessing_MITRE_ATTCK_Risk_Using_a_Cyber-Security_Culture_Framework (accessed on 25 July 2025).
9. Skabtsov, N. *Information Systems Security Audit*; Peter: Saint Petersburg, Russia, 2018; p. 272; ISBN 978-5-4461-0662-2. Available online: https://books.yandex.ru/books/T54pW6oL/read-online (accessed on 20 July 2025).
10. Kotenko, D.I.; Kotenko, I.V.; Saenko, I.B. Methods and tools for modeling attacks in large computer networks: The state of the problem. *SPIIRAN* **2012**, *22*, 5–30. [CrossRef]
11. Baranov, V.V.; Shelupanov, A.A. Models and methods for assessing the destructive impact of violators on elements of distributed information systems. *Rep. Tomsk. State Univ. Control. Syst. Radio Electronics* **2024**, *25*, 88–100. Available online: https://journal.tusur.ru/storage/178924/5-Baranov-Shelupanov_%D0%BF.pdf?1741931041 (accessed on 20 July 2025).

12. Baranov, V.V.; Shelupanov, A.A. Cognitive model for assessing the security of information systems for various purposes. *Symmetry* **2022**, *14*, 2631. [CrossRef]
13. Avezova, Y.; Badaev, A. In the Sights of APT Groups: Kill Chain of Eight Steps. Habr, 2023. Available online: https://habr.com/ru/companies/pt/articles/802697/ (accessed on 2 June 2025).
14. Ang, S.; Huy, S.; Janarthanan, M. Utilizing IDS and IPS to improve cybersecurity monitoring process. *J. Cyber Secur. Risk Audit.* **2025**, 77–88. [CrossRef]
15. ISSAF—Information System Security Assesment Framework. 2006, 1264p. Available online: http://www.oissg.org/issaf02/issaf0.1-5.pdf (accessed on 8 June 2025).
16. Orrey, K. Penetration Test Framework. Vulnerability Assessment, 2014. Available online: https://www.secureinfo.eu/data/files/docs/Framework_-_Penetration_Test.html (accessed on 8 June 2025).
17. PTES–The Penetration Testing Execution Standard. 30 April 2012. Available online: http://www.pentest-standard.org/index.php/Main_Page (accessed on 9 June 2025).
18. Special Publications 800-115, *Technical Guide to Information Security Testing and Assessment*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2008. Available online: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf (accessed on 12 June 2025).
19. Aljumaiah, O.; Jiang, W.; Reddy Addula, S.; Amin Almaiah, M. Analyzing cybersecurity risks and threats in IT infrastructure based on NIST framework. *J. Cyber Secur. Risk Audit.* **2025**, *2025*, 12–26. [CrossRef]
20. Beizer, B. Black box testing. In *Technologies of Functional Testing of Software and Systems*; Peter: Saint Petersburg, Russia, 2004; p. 320; ISBN 5-94723-698-2. Available online: https://djvu.online/file/UlGilEprxDkPy (accessed on 8 June 2025).
21. Binder, R. *Testing Object-Oriented Systems*; Publisher Addison-Wesley Publishing Company Inc.: Reading, MA, USA, 2000; ISBN 9780201809381. Available online: http://kagowyje.blog.free.fr/index.php?post/2016/10/22/Testing-Object-Oriented-Systems%3A-Models%2C-Patterns%2C-and-Tools-pdf (accessed on 18 June 2025).
22. Ammann, P.; Offutt, J. *An Introduction to Software Testing*; University Press: Cambridge, UK, 2008; ISBN 978-0-521-88038-1. Available online: https://assets.cambridge.org/97805218/80381/frontmatter/9780521880381_frontmatter.pdf (accessed on 12 June 2025).
23. Zadeh, L. (Ed.) *The Concept of a Linguistic Variable and Its Application to Making Approximate Decisions*; Translated from English; Mir: Moscow, Russia, 1976; p. 167; ISBN 978-5-85582-423-0.
24. Sapkina, N.V. Properties of Operations on Fuzzy Numbers. Bulletin of the VSU. Series: System Analysis and Information Technology. 2013, Volume 1, pp. 23–28. Available online: https://www.elibrary.ru/download/elibrary_20156009_60491464.pdf (accessed on 12 June 2025).
25. Asfha, A. Information security risk assessment in industry information system based on fuzzy set theory and artificial neural network. *Inform. Autom.* **2024**, *23*, 542–571. [CrossRef]