Journal of Open Innovation:
Technology, Market, and Complexity

Article

Banking Information Resource Cybersecurity System Modeling

Olha Shulha [1], Iryna Yanenkova [2], Mykhailo Kuzub [3], Iskandar Muda [4,*] and Viktor Nazarenko [5]

[1] Department of Management and Marketing, Faculty of Business and Social Communications, State University of Intelligent Technologies and Telecommunications, 65023 Odesa, Ukraine; shulha@ua.fm
[2] Sector of Digital Economy, Institute for Economy and Forecasting of National Academy of Ukraine, 01011 Kyiv, Ukraine; yanenkova@i.ua
[3] Department of Accounting and Taxation, Kyiv National University of Trade and Economic, 02156 Kyiv, Ukraine; kuzub@ua.fm
[4] Department of Accounting, Faculty of Economics and Business, Universitas Sumatera Utara, Medan 20155, Indonesia
[5] Department of Information Systems and Technologies, Faculty of Engineering and Education, Dragomanov National Pedagogical University, 01601 Kyiv, Ukraine; nazarenko@email.ua
* Correspondence: mudaiskandar820@yahoo.com

Abstract: The rapid development of the process of informatization of modern society has necessitated cybersecurity in all spheres of human activity, as the implementation of deliberate or unintentional influences on the information sphere by both external and internal sources can damage security and lead to moral, material, financial, reputational and other forms of damage. The purpose of the paper is to create functional cognitive models to assess the level of their protection. The method of building a fuzzy cognitive map of the state of cybersecurity of banks is used. There have been developed cognitive models to determine the level of protection of the computer network, information security system and critical infrastructure (banks). Scenarios have been developed that reflect the response of the system at the complex maximum attenuation of the impact of the most important cyber threats. In conclusion, the practical implementation of the method provides an opportunity to predict the state of cybersecurity of banks, and contributes to the implementation of the necessary mechanisms to prevent, protect and control access at the appropriate levels of network infrastructure.

Keywords: cyber threat; Internet banking; banking information resources; hybrid threat; efficiency

check for updates

Citation: Shulha, O.; Yanenkova, I.; Kuzub, M.; Muda, I.; Nazarenko, V. Banking Information Resource Cybersecurity System Modeling. *J. Open Innov. Technol. Mark. Complex.* **2022**, *8*, 80. https://doi.org/10.3390/joitmc8020080

Received: 23 March 2022
Accepted: 24 April 2022
Published: 28 April 2022

1. Introduction

Active informatization of modern society and increasing flows of confidential information have led to the need to provide information (data) security (DS) in various spheres of public activity, since any process in the financial, industrial, political or social spheres is directly related to information resources and the use of information technology (IT).

At the same time, due to the growing complexity of information systems (IS) and technology, the number of potential threats to these systems is increasing. Therefore, to provide DS and predict the development of specific situations, it is important to assess the level of security of systems for protection of information (IP) circulating in IS.

It is possible to solve this problem by means of methods of the statistical analysis, in particular the method of correlation-regression. However, these methods require complex calculations, a significant amount of experimental data, take a long time to process and do not provide the ability to work with quality factors that are determined by experts. In this regard, it is worth paying attention to the cognitive approach based on building fuzzy cognitive maps (FCM), first proposed by Bart Kosco [1].

The priority of FCM selection is their simplicity, constructiveness and clarity, identification of the structure of causal relationships between elements of a complex system that are difficult to quantify with traditional methods, use of knowledge and experience of subject matter experts, adaptation to uncertainty of initial data and conditions [2]. Furthermore, it is worth noting the simplicity of the expansion of factors by introducing additional vertices and arcs of the graph of a cognitive map [3].

Methods of description and classification are important methods for analysis of the state of DS provision. To implement effective information protection, it is necessary to first describe and only then classify the various types of threats and dangers, risks and challenges, and accordingly, formulate a system of measures to manage them [4]. The methods of casual relationship study are used as common methods for analysis of the level of DS provision. These methods help to identify the causal relationships between threats and hazards, search for the causes that became the source and caused the actualization of certain risk factors, as well as to develop measures for their neutralization. The selection of methods for analysis of the state of DS provision depends on the specific level and scope of protection [5]. Depending on the threat, the task regarding the differentiation between both different levels of threats and different levels of protection is made possible. In the sphere of DS, such levels of protection are usually distinguished [6–12]:

- Physical: organization and physical protection of information resources, information and management technologies;
- Software and hardware: identification and authentication of users, access control, logging and auditing, cryptography, shielding, high information assurance;
- Management: management, coordination and control of organizational, technological and technical measures;
- Technological: implementation of DS policy through the use of modern automated IT;
- User: implementation of IS policy aimed at reducing the reflective impact on DS objects, preventing information impact from the social environment;
- Information and telecommunication networks: this policy is implemented in the format of coordination of actions of the subjects of DS system, which are interrelated by one goal;
- Procedural: measures are taken that are implemented by the subjects (personnel management, physical protection, maintenance of working capacity, response to security breaches, planning of restoration works, etc.).
- Furthermore, the methods of DS provision can be subdivided into several types [13–18]:
- One-level methods that are based on one principle of DS management;
- Multi-level methods that are based on several principles of DS management, each of which serves to solve a specific problem;
- Integrated methods, multi-level technologies that are integrated into a single organizational-level system of coordination functions for the purpose of DS provision based on the analysis of a group of risk factors that are semantically-related or are generated by a single center of information influence;
- Integrated highly intelligent methods, multi-level, multi-component technologies, which are built on the basis of powerful automated intelligent tools with organizational management.

The purpose of the paper is to increase the level of security of systems for protection of information (IP) circulating in IS, the creation of functional cognitive models to evaluate the level of their security.

2. Literature Review

Successful open innovations also depend on the open nature of the business model. Since knowledge has become a key resource for companies, open innovation must be embedded in the overall business strategy, which clearly recognizes the potential use of external ideas, knowledge and technology in value creation [19]. Due to the integration of different technologies, the boundaries of the industry are changing or even disappearing, which necessitates new business models and organizational structures, including effective human capital management (open culture, diversity, etc.) [20].

Factors that contribute to the spread of open innovations include: growing global competition; reduction of product life cycles; complexity of new technologies; global mobility of innovators; state support for the development of small innovative enterprises; market orientation of research; the need for the commercialization of projects by state laboratories; the emergence of private research institutes; the availability of the Internet and search technologies; and the need to optimize existing networks of suppliers of strategic importance [21].

Higher competition and other factors reduce the profitability of innovative companies in terms of increasing costs in a closed model of the innovation process [22]. Applying a more open model allows you to monetize unused in-house innovation.

The concept of open innovations defines the process of research and development as an open system, i.e., any company can attract new ideas to create a new product and enter the market with this product not only through their own development, but also through cooperation with other organizations.

Open innovations are an approach that allows you to maximize profits from the joint creation and commercialization of innovative projects, which involves, on the one hand, using external sources of inventions and technologies to effectively implement their projects, and on the other hand, opening access to their inventions and technologies to get the maximum profit from their implementation [23].

The model of "open innovations" assumes that the bank not only relies on its own in-house research and development when developing new technologies and products, but also actively uses external innovations and competencies [24].

In general, the authors propose to consider the paradigm of open innovations in terms of different research determinants.

Spatial determinant. The study of innovations on a global scale is carried out on the basis of this determinant. As research, technology and product development become global, the process of open innovation has been simplified [25]. Geographical proximity to leading regional centers allows the company to increase its absorption capacity, thus facilitating access to knowledge and competencies of the world's best talents. Access to resources is one of the main factors in the internationalization of research projects.

Structural determinant. There is a trend to increase the amount of outsourcing and number of alliances in the field of research and development [26]. Industry price chains are becoming more disaggregated. Cost reduction and greater specialization through more sophisticated technologies and product systems are drivers of this trend. The use of open innovations is compensated for the central research and development departments of firms not only by concentrating on short-term, customer-oriented research activities.

User determinant. This is a determinant, in which users are integrated into the innovation process. This area of research of the innovation process began with the participation of users, the availability of tools, the idea of mass adaptation and the use of the concept of democratization of the innovation process [27]. User innovation is one of the most studied parts of the open innovation paradigm.

Supplier determinant. Involving suppliers in the innovation process can significantly increase innovation productivity in most industries [28].

Technology use determinant. Most studies and practical actions focus on the existing market and business [29]. Despite the potential for new revenue streams, existing research competencies and the spread of intellectual property to new markets have often been neglected. Technology development and external commercialization of intellectual property is a future field of research with high potential.

Process determinant. There are three main processes through which open innovations are carried out: outside to inside, inside to outside and double process [30]. Sometimes these processes complement each other, but in most cases the external attraction of innovations is dominant.

Tool determinant. The phenomenon of the open innovation process requires certain tools that allow customers to, for example, create or customize their own product or allow companies to integrate through the websites of idea creators [31].

Institutional determinant. Open innovation can be considered as an individual-collective innovation model [32]. The private investment model of innovation with temporary monopolistic profits is replaced by the free search for inventions, findings, discoveries and knowledge, which is the defining characteristic of the model of open innovations.

Culture determinant. The process of open innovation begins with reflection. Creating a culture that will be able to assess external competence and know-how is important for the practice of open innovations [33]. This culture, in addition to the internal values of a company, is influenced by many factors, such as incentive systems, management systems, communication platforms, project acceptance criteria, supplier evaluations, etc.

Competent search for novel ideas of "open innovations" can save companies a lot of resources and time. The value of the open innovation model is that it allows you to synchronize efforts for internal and external research [34].

Thus, "open innovations" reduce the company dependence on high innovation and other current risks, enabling the company to gain strategic advantages in competition. However, the process of using "open innovations" has its difficulties and internal risks [35]. The most important thing is managerial risk. Implementation of "open innovations" requires high analytical and managerial skills from managers, it is necessary to be able to timely anticipate current innovations, track them, and work productively not only with your team but also other people, often even from other states [36].

Since the market for "open innovations" is accessible for all players in risky innovation, there is a risk of interception of innovative business ideas and insecurity of intellectual property [37]. Thus, to create a unique innovation, it is important to support external research with internal research. That is, the reference model of "open innovations" involves a two-way combination of promising external innovations complemented by internal solutions aimed at improving or creating new business models.

Formation of risk management, especially in the field of cyber security, should take into account the risks of innovation and create a platform for the use of promising ideas, which is possible only in the formation of integrated risk management, which aims to reconcile innovation and risk at all levels. Risk management structure should include a unit of innovation management of banks.

3. Methods

It is convenient to use fuzzy logic methods to solve problems related to the analysis of DS threats and risks. Thus, in the paper [19], a fuzzy hierarchical model was built, which contains linguistic variables and fuzzy knowledge bases; a linguistic risk assessment of information assets based on the Coras methodology was suggested [20].

In the paper [21], it is demonstrated that when calculating the risk of DS threat using a fuzzy set model with different possible options for the content of expert data for the same threats, the levels of DS risk can differ significantly. These data are as follows: membership functions; term sets; and production rules.

The authors of the paper [22] developed methods and models for fuzzy quantification of DS risks based on fuzzy set theory. However, the methods suggested by the authors do not take into account the impact of assets on the end result of the organization operation.

In the paper [38], a fuzzy production model was developed, which allows to significantly expand the capabilities of existing methods, remove restrictions on the number of input variables and integrate both qualitative and quantitative approaches to risk assessment. The risk assessment mechanisms based on fuzzy logic that are used in the technique allow to obtain a linguistic description of the degree of risk, which makes it possible for IT managers to identify risk priorities and select an action plan to reduce the most dangerous DS threats of the organization.

In the paper [23], the authors describe the general provisions of DS risk assessment using fuzzy set theory. Linguistic variables characterize the general parameters that are most often used in risk assessment: threat probability; assets; and their ratio of vulnerabilities to threats.

The authors of the paper [24] describe a fuzzy model of risk assessment for the whole organization and take fuzzy variables that describe risk factors (organizational, technical levels of IP, value and volume of information resources) as input characteristics. With that, specific vulnerabilities and their impact on the target system are not taken into account.

In the paper [25], the process of creation of a fuzzy production model for DS risk assessment is considered. The model includes the bases of rules and allows to carry out the linguistic analysis of risks which pose potential threats and incur losses for the organization. The relationship between factors (antecedent) and risk indicators (consequent) is a binary fuzzy relationship based on the Cartesian product of the corresponding fuzzy sets. Fuzzy causal relationship between the antecedent and consequent is defined as a fuzzy product. The mechanism of obtaining risk assessments based on fuzzy logic allows us to obtain the numerical value of risk, linguistic description of the degree of risk, as well as the level of confidence of the expert in the occurrence of risk.

The authors of the paper [26] built a model for evaluation of the general level of information risks in the CRM system using a linguistic approach that provides a quantitative description of individual elements of the model in terms of fuzzy information on the importance of criteria for evaluation risk factors. This makes it possible to identify significant risk factors, their consequences in the conditions of the threat agent action, and thus, to identify alternative ways to avoid the negative impact of risk.

The authors of the paper [27] suggested an approach to assessing the risks of DS based on the concept of logical-linguistic fuzzy model based on the set of Mamdani rules.

It should be noted that the evaluation of the cumulative effect of threats on the system and the ability to identify risks in different scenarios of implementation of multiple threats are important issues of DS provision. These issues can be solved using cognitive modeling methods. Cognitive models are built by an expert or a group of experts in the subject area under study on the basis of theoretical, statistical and expert information about the object of study [28]. The adequacy of the model is determined by the completeness of the set of input knowledge; the model can be refined in the process of study and use, itself being a source of structured knowledge.

Cognitive modeling methods are based on the use of FCMs, which are characterized by relative ease of interpretation, integration with evaluation methods of analysis results, visual clarity, flexibility, constructability, adaptability to uncertainty of input data, use of specific expert knowledge and experience, absence of need for anticipatory specification of data and impact relationships [29].

The FCM of a complex system (problem) is an oriented graph, which vertices (concepts) represent system variables, and arcs—causal relationships between concepts, with the weights of these relationships determining the strength of the mutual concept influence [30].

A cognitive map is a model of presenting expert knowledge of the laws of development and properties of the situation under study, and their diversity is determined by different ways of expert determination of the strength of causal relationships and the values of factors in the cognitive map [31].

Special attention is paid to network security for the proper network operation and reliable provision of all the above services, since computer networks (CNs) and their resources are constantly at risk of infection with malicious software (SW) or various types of network attacks. As a result of these attacks, attackers can get unauthorized access (UAA) to information resources, commit theft, destruction or corruption of data, disrupt the operation and availability of the service, gain control over the whole system. To prevent the above actions, it is necessary to analyze the impact of possible threats on the system, assess the strength of their action, highlighting the most important of them.

It is possible to solve this problem with the help of statistical analysis methods, specifically, the methods of variance analysis and correlation-regression analysis. However, these methods require complex calculations, the availability of sufficiently complete statistical information and a long time to process the necessary data. Thus, it is worth paying attention to the cognitive approach, which provides an opportunity to solve problems that cannot be strictly formalized, clearly present the system or problem, use incomplete, fuzzy information and subjective judgments of subject experts, and build flexible, constructive models that adequately respond to change.

Taking into account the above advantages of cognitive modeling, the authors will conduct a study of the impact of threats on the level of CN protection on its basis.

To achieve the purpose in hand, the authors will first analyze the possible threats to network security, which characterize the possible actions that can be taken in relation to the system. They manifest in various forms, but the most common of them are as follows [27,28]:

- Random hazards: a person who is unfamiliar with the relevant regulations and policies, or through improper care, creates a random hazard;
- Unauthorized changes: updates, fixes and other changes to operating systems, software applications, configurations, interoperability and hardware may pose an unexpected threat to the security of industrial automation and control systems or related industrial processes.

To identify general change trends in network security, the authors will study a corporate network with common characteristics.

Here is a list of possible threats, the implementation of which will lead to negative consequences of the network operation [23–28]:

1. Scan attacks—search for possible system vulnerabilities:

- Packet sniffers—interception and analysis of traffic;
- Ping sweeps—search for IP addresses of running computers;
- Port scanner—scanning open TCP and UDP ports;
- Phishing—method of obtaining the necessary information directly from CN users.

2. Web attacks:

- Cross-Site Scripting (XSS)—malicious collection of user information through web application pages;
- SQL injection—one of the common ways to hack sites and programs that work with databases based on the introduction of a random SQL code in the query;
- Path traversal—processing of HTTP requests by attackers to bypass access control and access other directories and files on the system.

3. Spoofing—replacement of a trusted entity:

- IP-spoofing—using someone else's sender's IP address to defraud the security system;
- DNS-spoofing—changing domain name cache data to assign an erroneous IP address;
- DHCP-spoofing—replacement of a default gateway.

4. Attacks aimed at gaining access to the system:

- Password attacks—password hacking;
- Trust exploitation—compromising a trusted host by using it to attack other hosts on the network;
- Man-in-the-middle attack—compromising a communication channel with help of which an attacker interferes with the data transmission protocol by deleting or modifying information.

5. Session hijacking—using an ongoing computer session to gain unauthorized access (UAA) to CN information or services.

6. Compromised key attack—interception of a secret key.

7. Spamming—abuse of email capabilities.

8. Denial of Service (DoS) attack—avalanche packet routing, which overloads the network, and as a result makes it inaccessible.

9. Malicious SW (trojans, worms, virus, botnets, etc.)—software intended for disrupting the network operation, collecting confidential information or gaining access to private computer systems.

10. Physical impact on the network on the side of an attacker that leads to the destruction or failure of physical components, such as hardware, software storage devices, connectors, sensors and controllers.

11. Disclosure of information, intentional or negligent actions of the user, as a result of which a person who does not have access to this information, gets acquainted with it.

12. Unintentional actions, mistakes of network users including accidental actions that are taken due to ignorance, carelessness or negligence, out of curiosity, but without malicious intent.

13. Natural and technogenic disasters (accidents, hurricanes, earthquakes, fires, etc.).

It should be noted that the author's novelty is the improvement of the cyber security assessment model in banks. The main specificity of the model is that the analytical base (initial data for calculations) is a trade secret of the bank. According to the bank internal protocols, this base is not open information that is subject to publication. So, the novelty of open innovation is just the cognitive model.

The authors examine the object of the banking institution, which belongs to the class of objects that provide access to the Internet and reflects the maximum representation of the structural components. The authors create a number of threats to this object, noting that the main directions of the attack vector are aimed at IT infrastructure and operational technologies. With that, a large number of threats are aimed at the Supervisory Control and Data Acquisition (SCADA) and Distributed Control Systems (DCS), which provide essential services to banks.

Analysis of existing methods demonstrated that they require complex calculations, the availability of sufficiently complete statistical information, a long time to process the necessary data. Besides, in case of most methods, the risk assessment is carried out only to the level of assets, and their impact on the functioning of the system under study is not taken into account. With that, the solution of this problem is directly related to the human factor and is characterized by a high degree of uncertainty, the complexity of formalizing the impact of threats. Therefore, to address this issue, it is advisable to pay attention to the methods of cognitive approach, which provides an opportunity to solve the above problems, clearly presenting the system under study with the help of flexible design models capable of adequate response to change.

The developed cognitive model for determining the level of security of the information protection system provides a sufficient degree of detail, allows taking into account the presence of a large number of alternative scenarios for implementation of threats. Based on the data obtained from the launch of these scenarios, it is possible to develop a clear plan for improving the security of the information protection system, timely take the necessary measures to prevent, localize, eliminate or reduce the impact of potential information security threats.

To build the FCM, which determines the security status of a computer networks (CN), first of all, it is necessary to form from the above list a variety of concepts, which are most important from the point of view of studying this problem. In accordance with the above methodology, the following concepts were distinguished:

- Network attacks (scan attacks, web attacks, spoofing, attacks aimed at gaining system access, session hijacking, and compromised key attacks);
- Spamming;
- Malware;
- Physical impact on the network on the side of an attacker;
- DoS attacks;
- Disclosure of information;
- Unintentional actions, mistakes of network users;
- Reliability, fault tolerance of hardware and software;
- CN security;
- Fault tolerance of network service;
- Natural and technogenic disasters.

Having formed the list of concepts, the authors define values of influence force between each pair of concepts by processing of the data received as a result of expert poll.

To do this, the authors set a fuzzy linguistic scale, which is an ordered set of linguistic values (terms) of estimates of the occurrence of probable consequences obtained as a result of influence of one concept on the other concept:

$$Relationship\ strength = \left\{ \begin{array}{l} No\ influence; Weak; Very\,weak; \\ Medium; Strong; Very\,strong \end{array} \right\} \tag{1}$$

To each of these values the authors assign a numerical range belonging to segment [0, 1] for positive relationships and segment [−1, 0] for negative relationships:

$$v_{o,u} = \left\{ \begin{array}{l} (0.85; 1],\ positive\,very\,strong; \\ (0.6; 0.85],\ positive\ strong; \\ (0.35; 06),\ positive\ medium; \\ (0.15; 0.35),\ positive\ weak; \\ (0; 0.15),\ positive\,very\,weak; \\ 0,\ no\,\text{in}fluence; \\ (0; -0.15],\ negative\,very\,weak; \\ (-0.15; -0.35],\ negative\ weak; \\ (-0.35; -0.6],\ negative\ medium; \\ (-0.6; -0.85],\ negative\ strong; \\ (-0.85; -1],\ negative\ very\ strong \end{array} \right\} \tag{2}$$

The FCM, which illustrates the multiple causal relationships and the nature of the interaction of certain factors, is given in Figure 1.

The modeling was carried out using the tools of Mental Modeler SW.

The built FCM consists of eleven concepts:

(1) Six concepts of "Driver" type—they influence other concepts but are not influenced by any of the concepts of the system;

(2) One concept of "Receiver" type—it is influenced by the concepts of the system, and it does not influence any of them;

(3) Four concepts of "Ordinary" type—these are ordinary, intermediate concepts, which influence and are influenced by some system concepts.

To determine the complexity of the developed FCM, the authors calculate the density of relationships using the formula Department of Accounting and Taxation, Kyiv National University of Trade and Economic, Kyiv, 02156, Ukraine

$$D = \frac{K}{M \times (K-1)} \tag{3}$$

where D—density of cognitive model relationships; K—number of relationships; M—number of concepts.

In this case M = 11, K = 16, then D = 0.15. This indicates the sufficient complexity of the developed cognitive model.

To analyze the FCM, it is necessary to take into account all the indirect mutual influence of concepts. For the purpose, on the basis of the built cognitive map, the authors create a contiguity matrix $V = [v(F_0, F_u)]_{M \times M}$ (Table 1).

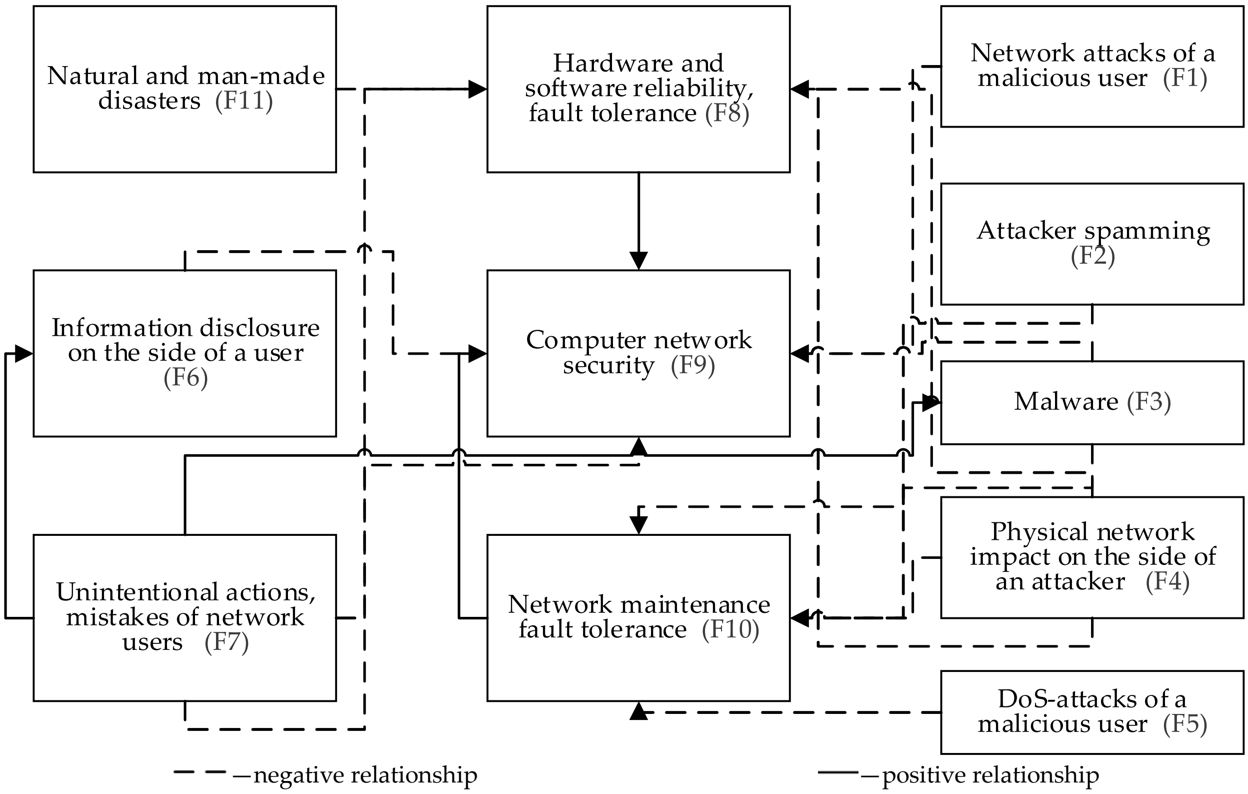
Natural and man-made disasters (F11)
Hardware and software reliability, fault tolerance (F8)
Network attacks of a malicious user (F1)
Attacker spamming (F2)
Information disclosure on the side of a user (F6)
Computer network security (F9)
Malware (F3)
Physical network impact on the side of an attacker (F4)
Unintentional actions, mistakes of network users (F7)
Network maintenance fault tolerance (F10)
DoS-attacks of a malicious user (F5)
—negative relationship
—positive relationship

Figure 1. Fuzzy cognitive map of the state of bank cybersecurity.

Table 1. Contiguity matrix of fuzzy cognitive map of bank cybersecurity.

Concept	F1	F2	F3	F4	F5	F6	F7	F8	F9	F10	F11
F1									–0.79		
F2									–0.18	–0.48	
F3									–0.89	–0.59	
F4										–0.81	
F5								–0.42		–0.99	
F6									–0.74		
F7									–0.71		
F8			0.49			0.61		–0.62	0.65		
F9											
F10									0.65		
F11								–0.79			

After analyzing the value of these indicators it is possible to identify the most important concepts of the system under study: F3—malware; F4—physical impact on the network on the side of an attacker; F7—unintentional actions, mistakes of network users. Furthermore, it should be noted that such concept as F2—spamming has the smallest impact on the network operation.

4. Results

To obtain forecasts for the situation development, the authors determine the relative change in the concepts of the system with the maximum value of the influence of the most important factors on them. That is, they model the corresponding scenarios.

Scenario 1. The authors consider how the state of the system will change with the maximum increase in the value of the concept F3—malware.

Malicious programs include: trojans and spyware, worms, viruses, logic bombs, and some other programs designed for DS violation. These programs can infiltrate attacked computers in a variety of ways. This is most often the case when a user downloads files from unverified sources (removable media or websites) or thoughtlessly opens a suspicious file that he or she receives in an email. There are also more dangerous malicious programs that have their own "reproduction" mechanisms, copies of these programs are distributed to computers on the network without the participation of users.

In the system under study, the concept F3—malware has a direct influence on F10—fault tolerance of network service and F9—CN security.

As a result of the maximum increase in the value of the influence of malicious programs, the fault tolerance of network service is reduced by 0.04, and the computer network security is reduced by 0.05 (Figure 2).

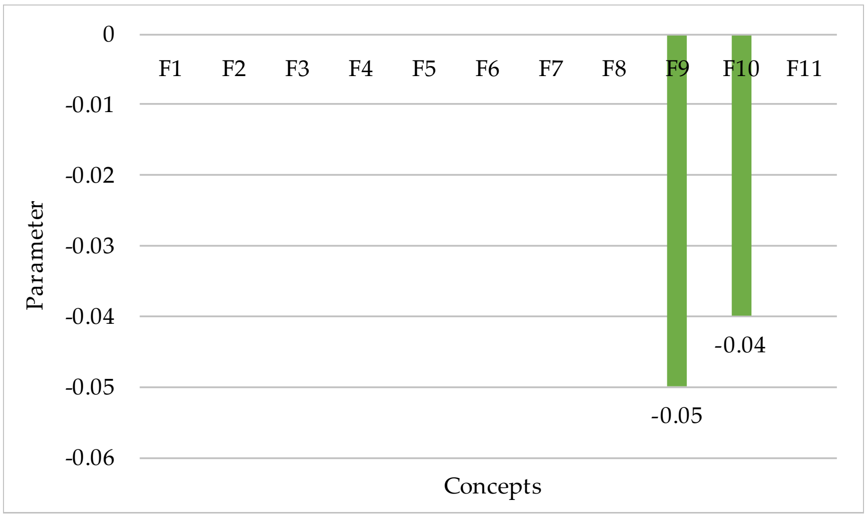

Figure 2. Scenario demonstrating the system response to the most negative changes in the concept F3—malware.

To avoid or prevent the negative action of malware, it is advisable to regularly update software, including the operating system and all applications, use reliable antivirus programs, create backups that are stored on the hard drive offline, etc.

Scenario 2. The authors model a situation that will reflect changes in the system with the maximum increase in the value of the concept F4—physical impact on the network on the side of an attacker.

In this case, an important place is occupied by physical means of network protection, which are designed to create obstacles in the way of a potential intruder who may enter the premises without authorization, make an act vandalism, commit a theft and other actions that adversely affect the network.

The concept F4—physical impact on the network on the side of an attacker has a direct impact on such system concepts as: F8—reliability, fault tolerance of hardware and software, and F10—fault tolerance of network service, and an indirect impact on F9—CN security. The authors study the relative changes in these concepts (Figure 3).

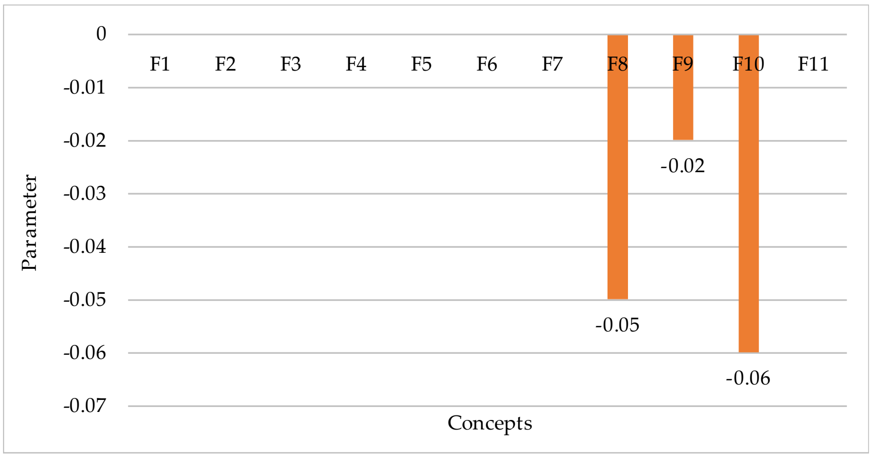

Figure 3. Scenario demonstrating the system response to the most negative changes in the concept F4—malware.

Based on this bar chart, one can draw a conclusion that when increasing the value of this concept, the security of computer networks decreases by 0.01, reliability, fault tolerance of hardware and software—by 0.04, and fault tolerance of network service—by 0.05. Therefore, special attention should be paid to strengthening the physical means allowing the solving of problems related to the protection of territory, premises, equipment and the implementation of controlled access to them.

Scenario 3. The authors examine possible changes of concepts at the maximum increase of negative influence of the concept F7—unintentional actions, mistakes of network users on the network.

Unintentional actions, mistakes of users, operators and system administrators who maintain the network can lead to malfunctions or complete inoperability of the system, as well as to create vulnerabilities that can be exploited by attackers.

The concept F7—unintentional actions, mistakes of network users has a direct influence on the concepts F3—malware, F6—disclosure of information by a user, F8—reliability, fault tolerance of hardware and software, F9—CN security and an indirect influence on the concept F10—fault tolerance of network service. The authors consider the relative changes in the values of these concepts (Figure 4).

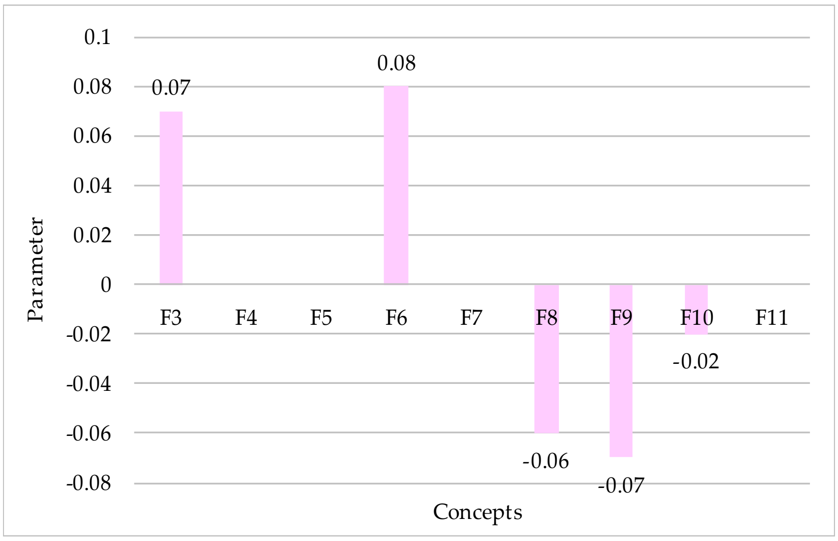

Figure 4. Scenario demonstrating the system response to the most negative changes in the concept F7—malware.

The resulting bar chart shows that the above actions will result in increase in the values of such concepts as F3—malware (by 0.07) and F6—disclosure of information by a user (by 0.08), which will worsen the fault tolerance of network service (by 0.02) and fault tolerance of hardware and software (by 0.06), and this, in turn, will decrease CN security by 0.07. Thus, it is necessary to properly organize work with staff, which involves quality selection and placement of staff, including training in the rules of confidential information, familiarization with measures of responsibility for violating the rules of IP, systematic control over the work of staff with confidential information, accounting, storage and destruction of documents and technical media, periodic training, etc.

Figure 5 demonstrates the relative change in the level of CN security, with a complex maximum weakening of the impact of the most important threats.

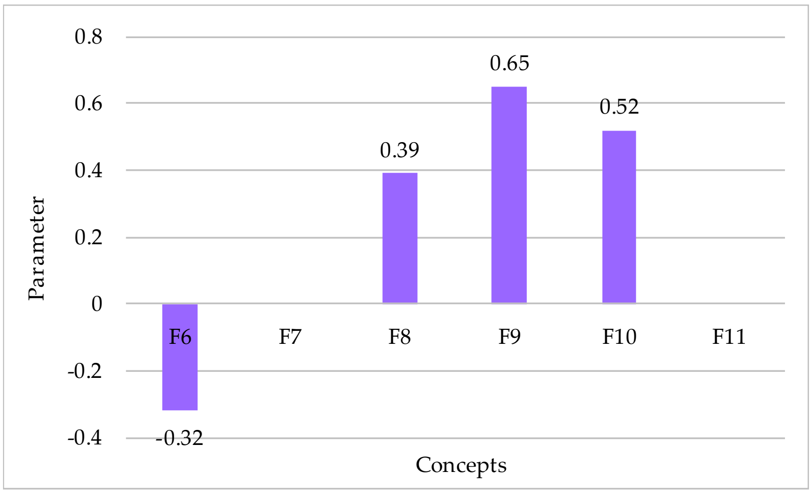

Figure 5. Scenario demonstrating the system response, with a complex maximum weakening of the impact of the most important threats.

As a result of the analysis of this bar chart, it is possible to draw a conclusion that under the given conditions CN security will increase by 0.65 conditional units, i.e., by 65%.

Thus, the developed fuzzy cognitive map of the analysis of the impact of threats on the level of network security reflects mainly the qualitative trends in the situation development, and is one of the means of work optimization when setting up computer network protection.

5. Discussion

5.1. The Key Factors of Banking Information Resource Cyber Security System

The rapid development of IT and their implementation in all spheres of public life determines the extreme importance of creating reliable information protection systems. The problem of quality functioning of these systems, given the emergence of new threats and growing levels of existing ones in the information space, is becoming increasingly important [39]. Moreover, an important practical problem is to establish an optimal balance between ensuring the security of the information protection system and the amount of costs for its support, given the rational distribution between the individual areas of protection [40].

Separately, it should be noted that at the initial stages of creating an effective security system of banks there appears a need to quantify the importance of potential threats, the implementation of which will lead to disruption of research facilities operation and will manifest itself in the form of stopping provision of population of both individual cities, and the state as a whole, with vital services and goods. In turn, this can lead to socio-political and economic instability, exacerbation of conflicts of various kinds [41].

At the same time, the main sources of threats may be the high level of depreciation and breakdown rate of fixed assets, the impact of dangerous natural phenomena, the tense military-political and economic situation in the country, etc. [42].

In the vast majority of cases, the above issues are solved using statistical analysis methods, which require consideration of a significant amount of information and complex calculations, and take a long time to process [43].

One of the options to solve this problem may be the ranking of threats, which will permit to determine the acceptable intensity of reduction of the systems under study, and establish the proportional ratio of allowable costs to ensure their security.

Specifically, the method of non-strict ranking is proposed in [12]. According to this method, an expert develops a numbering of all criteria in descending order of acceptability of the negative consequences related with the given security criterion. The ranked criteria are then numbered sequentially. The rating (rank) of the criterion is determined by its number.

In [44], fuzzy logic-based ranking of information risks is carried out using the algorithm of Mamdani, which was one of the first algorithms to be used in fuzzy inference systems.

Moreover, there are a lot of works related to the ranking of elements in other areas of activity. For example, there suggested a method of ranking the factors influencing the reliability of the system based on the theory of a fuzzy cognitive map (FCM) [45]. The method is based on the formalization of causal relationships in the form of FCM, i.e., an oriented graph, which vertices correspond to the reliability of the system and the factors that influence it, and weighted arcs reflect the power of factor influence on each other and the reliability of the system. The rank of the factor is defined as analogous to the index of element importance according to Birnbaum.

Let us pay attention to another work of this scientist [46], where he suggests a method of ranking the elements of a multi-functional system based on fuzzy mathematics. The problem is reduced to automatic classification using transitive closure of fuzzy similarity relationship. The initial information about the system is given in the form of a fuzzy ratio of the influence of element failures on the performance of the function. The degree of influence of elements on the system functions is calculated by comparing with the smallest influence on the Saaty scale.

It can be concluded that there are many methods for evaluation of information security, in particular cyber security. Depending on the specifics of the methodological platform, different evaluation results are obtained.

5.2. Banking Cyber Security System and Open Innovation

In the current conditions, the task of preventing the development of negative trends in relation to the continued bank operation, as well as minimizing the causes of threats of cyber attacks, is assigned to modern technologies.

Banking open innovations are practical innovations introduced into any area of bank activities to achieve a positive economic and strategic effect [47]. At the same time, the needs of customers should be met, and the current process of providing banking services should be modernized.

Open innovations are considered not only as a way to improve the effectiveness indicators of a financial and credit organization, but furthermore, in the conditions of constant risks, as a tool for ensuring information security.

At the moment, innovations in the banking sector are related to distance customer service, Internet banking, electronic money, etc. [48].

Demanded bank of the 21st century is a bank with a set of unique technologies that allow you to make financial transactions anywhere and anytime fast, efficiently and safely [49].

In addition, open innovations introduced into the workflow are designed to provide the following customer-centric services: simple, fast, round-the-clock and accessible search for information about the bank products and services from any digital device; information security of user data; promt feedback; business process optimization [50].

Thus, today a process of reorganization of bank activities is taking place that is oriented to the client through the development and implementation of the technology of the future, as well as by stimulating behavior focused on open innovative transformation [51].

Determining the effect of the introduction of open innovations as profitable solutions by banks, one should take into account such indicators of the bank operation as profitability and growth of assets, an increase in client resources and interest income, as well as loans and debts of clients [52].

Strategically, it is important to rely on the best practices of the banking innovative development, to constantly monitor the emergence of advanced technologies on the ICT market, and to qualitatively adapt them to the national conditions of the bank operation [53].

For example, there are a number of IT security innovations aimed at ensuring the security of personal data, preventing information leakage, storing and backing up data, protecting against cyber attacks, viruses and other threats to system security [54]. Such innovations are based on a process-oriented approach (for example, service-oriented architecture, cloud computing, data leak prevention, etc.) [55].

The technology that is most widely used by banks is the Big Data technology (or "Big Data") [56], which makes it possible not only to store huge amounts of information, quickly find the necessary data in big arrays, process and structure the data, but also protect information resources against theft, loss, destruction, disclosure and distortion by unauthorized users. With the help of Big Data, Mastercard, VISA, Facebook, Google, etc. are actively used in their activities [57].

Thus, the analyzed innovations perform the following functions in the area of information security: a timely response to attempts of unauthorized access to databases; maintaining a record of all operations on the local network; identification of users, resources and personnel of the network information security system, including identification and authentication of the user by the input credentials.

6. Conclusions

We aim to provide information about individual components and how they work together in applications, operating systems, servers, data stores, and many other places for a complete picture of performance. With the help of the infrastructure condition monitoring function, it is possible to: monitor the level of resource use (CPU, RAM, HDD); analyze ways of data access and performance of production activities; and risk and impact assessment. In the current conditions, business priorities are often at odds with the constant pressure of growing cyber threats.

The pandemic with its lockdowns shifted the perimeter of protection of financial institutions to the homes of users, which required the expansion and strengthening of information security requirements. In particular, the regulator is going to provide banks with methodical recommendations on strengthening the security of online banking operations, online operations with cards, mobile applications and messenger chatbots.

It is not enough for financial institutions themselves to know the theory, they must be able to practically detect threats of cyberattacks and be able to defend against them. For this, it will help to use world best practices, tuned business processes, teamwork and the introduction of modern technologies. This will minimize the likelihood of intrusion into the operations of the bank or payment system, will allow stopping intruders in time, eliminate harmful activity and quickly restore the financial service.

Cognitive models have been developed to determine the level of safety of the computer network, information security system and banks. The suggested models allow to identify the most important threats, in terms of studying this problem and to analyze the relative change in the level of safety of the systems under study. The structural and topological analysis of the built fuzzy cognitive maps has been carried out, the results of which testify to their sufficient density, complexity and democracy. Concepts that have the highest structural significance have been identified and scenario modeling has been carried out, as a result of which, with the maximum positive impact of these concepts, it is determined that the level of safety of the computer network security will increase by 65%, that of the information security system by 32% and that of banks by 2%.

The results of this study give an opportunity to forecast the state of bank cybersecurity, which in turn contributes to the implementation of the necessary mechanisms to prevent, protect and control access at the appropriate levels of network infrastructure.

Author Contributions: Conceptualization, O.S. and I.M.; methodology, I.Y.; software, M.K.; validation, O.S. and I.M.; formal analysis, V.N.; investigation, I.Y.; resources, V.N.; data curation, O.S.; writing—original draft preparation, I.M.; writing—review and editing, M.K.; visualization, V.N.; supervision, I.Y.; project administration, M.K.; and funding acquisition, I.Y. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Kosko, B. Fuzzy cognitive maps. International journal of man-machine studies. *Int. J. Man-Mach. Stud.* **1986**, *24*, 65–75. [CrossRef]
2. Bauer, S.; Bernroider, E.W.; Chudzikowski, K. Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. *Comput. Secur.* **2017**, *68*, 145–159. [CrossRef]
3. Shamala, P.; Ahmad, R.; Zolait, A.; Sedek, M. Integrating information quality dimensions into information security risk management (ISRM). *J. Inf. Secur. Appl.* **2017**, *36*, 1–10. [CrossRef]
4. Hassani, H.; Huang, X.; Silva, E. Digitalisation and big data mining in banking. *Big Data Cogn. Comput.* **2018**, *2*, 18. [CrossRef]
5. Han, J.; Kim, Y.J.; Kim, H. An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective. *Comput. Secur.* **2017**, *66*, 52–65. [CrossRef]
6. Bauer, S.; Bernroider, E.W. From information security awareness to reasoned compliant action: Analyzing information security policy compliance in a large banking organization. *ACM SIGMIS Database DATABASE Adv. Inf. Syst.* **2017**, *48*, 44–68. [CrossRef]
7. Ramachandran, M.; Chang, V. Towards performance evaluation of cloud service providers for cloud data security. *Int. J. Inf. Manag.* **2016**, *36*, 618–625. [CrossRef]
8. Jasmin, M.; Hemalatha, S.B. RFID security and privacy enhancement. *Int. J. Pure Appl. Math.* **2017**, *116*, 535–539.
9. Srinivas, J.; Das, A.K.; Kumar, N. Government regulations in cyber security: Framework, standards and recommendations. *Future Gener. Comput. Syst.* **2019**, *92*, 178–188. [CrossRef]
10. Salahdine, F.; Kaabouch, N. Social engineering attacks: A survey. *Future Internet* **2019**, *11*, 89. [CrossRef]
11. Ijaz, S.; Shah, M.A.; Khan, A.; Ahmed, M. Smart cities: A survey on security concerns. *Int. J. Adv. Comput. Sci. Appl.* **2016**, *7*, 612–625. [CrossRef]
12. Jasmin, M.; Hemalatha, B. Security for industrial communication system using encryption/decryption modules. *Int. J. Pure Appl. Math.* **2017**, *116*, 563–568.
13. Kiwia, D.; Dehghantanha, A.; Choo, K.K.R.; Slaughter, J. A cyber kill chain based taxonomy of banking Trojans for evolutionary computational intelligence. *J. Comput. Sci.* **2018**, *27*, 394–409. [CrossRef]
14. Merhi, M.; Hone, K.; Tarhini, A. A cross-cultural study of the intention to use mobile banking between Lebanese and British consumers: Extending UTAUT2 with security, privacy and trust. *Technol. Soc.* **2019**, *59*, 101151. [CrossRef]
15. Moody, G.D.; Siponen, M.; Pahnila, S. Toward a unified model of information security policy compliance. *MIS Q.* **2018**, *42*, 285–311. [CrossRef]
16. Safa, N.S.; Von Solms, R. An information security knowledge sharing model in organizations. *Comput. Hum. Behav.* **2016**, *57*, 442–451. [CrossRef]
17. Goel, S.; Williams, K.; Dincelli, E. Got phished? Internet security and human vulnerability. *J. Assoc. Inf. Syst.* **2017**, *18*, 2. [CrossRef]
18. Singh, S.; Srivastava, R.K. Predicting the intention to use mobile banking in India. *Int. J. Bank Mark.* **2018**, *36*, 357–378. [CrossRef]
19. Lombardi, M.; Pascale, F.; Santaniello, D. EIDS: Embedded Intrusion Detection System using Machine Learning to Detect Attack over the CAN-BUS. In Proceedings of the 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference, Venice, Italy, 21–26 June 2020.
20. Sinclair-Desgagné, B. Measuring innovation and innovativeness: A data-mining approach. *Qual. Quant.* **2021**. [CrossRef]

21. Antonczak, L.; Burger-Helmchen, T. Being mobile: A call for collaborative innovation practices? *Inf. Learn. Sci.* **2021**, *122*, 360–382. [CrossRef]
22. Chhabra, R.N.; Prabhakaran, S. Sustainable response system building against insider-led cyber frauds in banking sector: A machine learning approach. *J. Financ. Crime* **2022**. [CrossRef]
23. Chesbrough, H. To recover faster from Covid-19, open up: Managerial implications from an open innovation perspective. *Ind. Mark. Manag.* **2020**, *88*, 410–413. [CrossRef]
24. Bogers, M.; Burcharth, A.; Chesbrough, H. Open innovation in Brazil: Exploring opportunities and challenges. *Int. J. Innov.* **2019**, *7*, 178–191. [CrossRef]
25. Yun, J.J.; Zhao, X.; Jung, K.; Yigitcanlar, T. The culture for open innovation dynamics. *Sustainability* **2020**, *12*, 5076. [CrossRef]
26. Yun, J.J.; Kim, D.; Yan, M.R. Open innovation engineering—Preliminary study on new entrance of technology to market. *Electronics* **2020**, *9*, 791. [CrossRef]
27. Nambisan, S.; Siegel, D.; Kenney, M. On open innovation, platforms, and entrepreneurship. *Strateg. Entrep. J.* **2018**, *12*, 354–368. [CrossRef]
28. Rauter, R.; Globocnik, D.; Perl-Vorbach, E.; Baumgartner, R.J. Open innovation and its effects on economic and sustainability innovation performance. *J. Innov. Knowl.* **2019**, *4*, 226–233. [CrossRef]
29. Leckel, A.; Veilleux, S.; Dana, L.P. Local Open Innovation: A means for public policy to increase collaboration for innovation in SMEs. *Technol. Forecast. Soc. Chang.* **2020**, *153*, 119891. [CrossRef]
30. Hameed, W.U.; Nisar, Q.A.; Wu, H.C. Relationships between external knowledge, internal innovation, firms' open innovation performance, service innovation and business performance in the Pakistani hotel industry. *Int. J. Hosp. Manag.* **2021**, *92*, 102745. [CrossRef]
31. Huggins, R.; Prokop, D.; Thompson, P. Universities and open innovation: The determinants of network centrality. *J. Technol. Transf.* **2020**, *45*, 718–757. [CrossRef]
32. Singh, S.K.; Gupta, S.; Busso, D.; Kamboj, S. Top management knowledge value, knowledge sharing practices, open innovation and organizational performance. *J. Bus. Res.* **2021**, *128*, 788–798. [CrossRef]
33. Hervas-Oliver, J.L.; Sempere-Ripoll, F.; Boronat-Moll, C. Technological innovation typologies and open innovation in SMEs: Beyond internal and external sources of knowledge. *Technol. Forecast. Soc. Chang.* **2021**, *162*, 120338. [CrossRef]
34. Sun, Y.; Liu, J.; Ding, Y. Analysis of the relationship between open innovation, knowledge management capability and dual innovation. *Technol. Anal. Strateg. Manag.* **2020**, *32*, 15–28. [CrossRef]
35. Sivam, A.; Dieguez, T.; Ferreira, L.P.; Silva, F.J. Key settings for successful open innovation arena. *J. Comput. Des. Eng.* **2019**, *6*, 507–515. [CrossRef]
36. Lee, M.; Yun, J.J.; Pyka, A.; Won, D.; Kodama, F.; Schiuma, G.; Park, H.; Jeon, J.; Park, K.; Jung, K.; et al. How to respond to the fourth industrial revolution, or the second information technology revolution? Dynamic new combinations between technology, market, and society through open innovation. *J. Open Innov. Technol. Mark. Complex.* **2018**, *4*, 21. [CrossRef]
37. Grimaldi, M.; Greco, M.; Cricelli, L. A framework of intellectual property protection strategies and open innovation. *J. Bus. Res.* **2021**, *123*, 156–164. [CrossRef]
38. Cedarbaum, J.G.; Powell, B.A.; Freeman, D.R.; Schloss, L.; Abrahamson, R. New York finalizes cybersecurity regulations for financial institutions. *J. Investig. Compliance* **2017**, *18*, 27–30. [CrossRef]
39. Aldasoro, I.; Gambacorta, L.; Giudici, P.; Leach, T. The drivers of cyber risk. *J. Financ. Stab.* **2022**, *60*, 100989. [CrossRef]
40. Najaf, K.; Mostafiz, M.I.; Najaf, R. Fintech firms and banks sustainability: Why cybersecurity risk matters? *Int. J. Financ. Eng.* **2021**, *8*, 2150019. [CrossRef]
41. Kandasamy, K.; Srinivas, S.; Achuthan, K.; Rangan, V.P. IoT cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. *EURASIP J. Inf. Secur.* **2020**, *1*, 8. [CrossRef]
42. Uddin, M.; Ali, M.; Hassan, M.K. Cybersecurity hazards and financial system vulnerability: A synthesis of literature. *Risk Manag.* **2020**, *22*, 239–309. [CrossRef]
43. Soni, V.D. Role of Artificial Intelligence in Combating Cyber Threats in Banking. *Int. Eng. J. Res. Dev.* **2019**, *4*, 7.
44. Maharjan, R.; Chatterjee, J.M. Framework for Minimizing Cyber Security Issues in Banking Sector of Nepal. *LBEF Res. J. Sci. Technol. Manag.* **2019**, *1*, 82–98.
45. Ali, L. Cyber crimes-A constant threat for the business sectors and its growth (A study of the online banking sectors in GCC). *J. Dev. Areas* **2019**, *53*, 267–279. [CrossRef]
46. Yun, J.J.; Zhao, X.; Park, K.; Shi, L. Sustainability condition of open innovation: Dynamic growth of alibaba from SME to large enterprise. *Sustainability* **2020**, *12*, 4379. [CrossRef]
47. Tajudin, M.M.; Musa, N.C. Issues and trends in open innovation amongst Malaysian fintech start-ups. *Int. J. Acad. Res. Bus. Soc. Sci.* **2018**, *8*, 1949–1964. [CrossRef]
48. De Groote, J.K.; Backmann, J. Initiating open innovation collaborations between incumbents and startups: How can David and Goliath get along? *Int. J. Innov. Manag.* **2020**, *24*, 2050011. [CrossRef]
49. Urbinati, A.; Chiaroni, D.; Chiesa, V.; Frattini, F. The role of digital technologies in open innovation processes: An exploratory multiple case study analysis. *RD Manag.* **2020**, *50*, 136–160. [CrossRef]
50. Cepeda, J.; Arias-Pérez, J. Information technology capabilities and organizational agility: The mediating effects of open innovation capabilities. *Multinatl. Bus. Rev.* **2019**, *27*, 198–216. [CrossRef]

51. Scuotto, V.; Beatrice, O.; Valentina, C.; Nicotra, M.; di Gioia, L.; Briamonte, M.F. Uncovering the micro-foundations of knowledge sharing in open innovation partnerships: An intention-based perspective of technology transfer. *Technol. Forecast. Soc. Chang.* **2020**, *152*, 119906. [CrossRef]
52. Tidd, J.; Bessant, J. Innovation management challenges: From fads to fundamentals. *Int. J. Innov. Manag.* **2018**, *22*, 1840007. [CrossRef]
53. Brockman, P.; Khurana, I.K.; Zhong, R.I. Societal trust and open innovation. *Res. Policy* **2018**, *47*, 2048–2065. [CrossRef]
54. Zhu, X.; Xiao, Z.; Dong, M.C.; Gu, J. The fit between firms' open innovation and business model for new product development speed: A contingent perspective. *Technovation* **2019**, *86*, 75–85. [CrossRef]
55. Mosteanu, N.R. Artificial Intelligence and Cyber Security–A Shield against Cyberattack as a Risk Business Management Tool–Case of European Countries. *Qual. Access Success* **2020**, *21*, 148–156.
56. Masucci, M.; Brusoni, S.; Cennamo, C. Removing bottlenecks in business ecosystems: The strategic role of outbound open innovation. *Res. Policy* **2020**, *49*, 103823. [CrossRef]
57. Gomber, P.; Kauffman, R.J.; Parker, C.; Weber, B.W. On the fintech revolution: Interpreting the forces of innovation, disruption, and transformation in financial services. *J. Manag. Inf. Syst.* **2018**, *35*, 220–265. [CrossRef]