СЕКЦІЯ 7
«ІНФОРМАЦІЙНА БЕЗПЕКА. ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ, АВТОМАТИЗОВАНІ КОМПЛЕКСИ, ВИМІРЮВАЛЬНІ СИСТЕМИ, ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ ТА ОПТИМІЗАЦІЯ»

УДК 007:621.391

K.Krasovska, Ph.D. candidate
Taras Shevcenko National University of Kyiv, katerina.krasovska@gmail.com

CYBERSECURITY IN BANKING SECTOR. LONG-TERM PERSPECTIVE

Nowadays, cybersecurity is growing risk area for all businesses. Over the past year it has become obvious that there are number of gaps in cybersecurity protection in the banking sector.

An increasing amount of banking takes place online. Banks can offer increased access and convenience to customers because of this digitization; however, this has also opened the door to increased online security risks.

Cyber-attacks can take on many forms, based on the number of recent attacks, it is fair to estimate that many banks are unprepared to deal with major cybersecurity attacks, the most vivid example was the attack of virus Petya which appeared in July 2017 and showed the terrible weakness of Ukrainian critical infrastructure and financial sector as its part. In order to protect we need to create cybersecurity strategy and implement its components all over the country, including banks and financial institutions [1].

An effective cybersecurity strategy will involve devising a combination of defence, assurance and resilience. Although outsourcing cybersecurity can be of huge benefit, there needs to be a radical change of mind-set across the banking operational infrastructure in tackling cyber-threats comprehensively. Cybersecurity should be applied as a reported metric – with an expectation of a certain standard on all levels, departments and projects. It is not as simple as signing a contract with a cybersecurity firm or buying their suite of tools [2]. A standardised, systematic approach should be set in place so that each attack is not treated with an ad hoc procedure but with a pre-determined action plan that has pre-allocated roles and responsibilities in the event of cyber-attacks.

Banks have invested significant amounts of cybersecurity spending over the past few years. However, the risk exposure has been growing at a faster pace than this investment. In other words, the gap between the investments in technology, labour and processes designed to mitigate cybersecurity vulnerabilities and relevant threats is widening.

Today, the intense competitiveness of financial services demands a constant search for cost-effective ways to improve performance and deliver new, innovative products and services to meet customer demands while retaining loyalty and trust. However, as financial services organizations forge new initiatives to drive business growth they are navigating a landscape marked by numerous challenges.

The underground financial fraud community has become increasingly organized, facilitating an expanded reach. Trojans targeting financial institutions have become one of the most prevalent threats on the internet today. As reported in the 2014 Symantec State of Financial Trojans report, the number of financial Trojans dropped by 53 percent in 2014. Android banking Trojans, such as the Android.iBanking Trojan, specialize in stealing banking information by intercepting SMS messages and continue to make the rounds[3].

Internet banking is at the core of banking – in five years, three of every four customer interactions will be online or mobile. Financial firms know they must move to mobile platforms or risk losing an entire generation of consumers to new, digital-native startups. But location-independent devices open a new set of security vulnerabilities, such as:

- Untested or insecure applications on mobile devices that may leak data or be vulnerable to misuse or attack.
- Inadequate authentication on devices and networks, granting unauthorized users access to data stores.
- Inconsistent protection of information on employee devices, customer devices, and company-owned devices used in branches and elsewhere.

To prevent and predict cyberattacks, banks need to introduce and develop the following protection methods and technologies [3].

1) Strong authentication and certificate management across devices, applications and users, including multi-level access control by identity and role and expansion of customer access controls.

2) Data protection solutions on shared devices, for example tablet computers used by staff and customers at branch offices.

3) Two-factor authentication options for high-value or high-sensitivity transactions, or available as a customer benefit.

Advanced authentication offers much greater protection than traditional security and anti-fraud approaches. A key advantage is that it is individualized for each user, and as a result resists the industrial-style automation that characterizes mass attacks. More than just identity management, advanced authentication methodologies monitor users' attributes and behaviors to keep imposters from accessing infrastructure and data.

Automation of security response and mitigation processes has lagged behind monitoring and alerting, but is due for a change. Once feeds, log data and human intelligence are combined into a sophisticated threat detection and discrimination mechanism, the stage is set for automated response. For example, upon identifying a bad actor by IP, URL or any other security control, an automated solution could not only block the activity and send an alert, but also isolate the affected system from the network, image the system for forensics, rebuild it to a known good state and bring it back online.

Financial firms collect enormous volumes of security information, including endpoint and network device logs, asset databases, user data and much more. Modern data-mining and visualization techniques, accelerated by rules-based engines and machine-learning algorithms, have the potential to identify high-risk outliers with sensitivity unknown today. Traditionally a labor intensive process, cybercrime analysis will increasingly leverage the use of Big Data [4]. The use of powerful, real-time analytics across multiple data sets – both structured and unstructured – will vastly improve the quality and speed of real-time cyber threat analysis while greatly reducing overall cost.

Confronted with stringent regulations and fragmented line-of-business operations and pressured by increased competition and changes in consumer expectations and behavior, financial services firms need to adopt new strategies in order to innovate and modernize. Financial institutions are looking to take advantage of mobile, cloud, social and other technical trends in order to reignite growth and build customer trust, but must contend with evolving and increasing complex cyber threats. IT Security plays a strategic role in providing the cover that financial services firms need in order to conduct business efficiently and securely. By forging strong security and risk management programs, IT Security empowers financial firms to innovate and compete with confidence.

List of references

1. Namestnikov Y. Cybercriminals vs financial institutions in 2018: what to expect [Electronic resource] / A.Gostev, D.Bestuzhev // Kaspesky Security Bulletin. – 2017. – Mode of access: https://securelist.com/cybercriminals-vs-financial-institutions/83370/

2. Anderson, Ross Why Information Security is Hard – An Economic Perspective [Text] / R.Anderson // 17th Annual Computer Security Applications Conference, December 10-14, 2001: Proceedings. – 2001. – p. 1-8

3. Bank for International Settlements and Board of the International Organization of Securities Commissions: Guidance on Cyber Resilience for Financial Market Infrastructures [Electronic resource] – Mode of access: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD535.pdf . – Last access: 2018.

4. FinTech Futures: Clever banking with artificial intelligence [Electronic resource] – Mode of access: https://www.bankingtech.com/2016/06/clever-banking-with-artificial-intelligence/ . – Last access: 2018

УДК 004:021

Sinkevych O.V., Master of Information Technology, PhD student
IT Department, Ukrainian National Forestry University, oleksiy1694@gmail.com

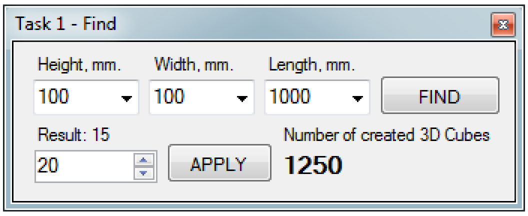
SOFTWARE AND ALGORITHMIC SUPPORT FOR WORKING WITH CELLULAR AUTOMATA

The primary objective of this work is the allocation of a fixed size timber on 3D cubes, which then will be used for distribution in 2D neighborhood von Neumann. For the distribution of lumber, it is necessary to take into account a number of rules, among which:

- It is necessary to divide the stack on a certain number of lumber, which will be divided into 3D cubes of the same size.
- The number of 3D cubes is limited and is determined by the cutoff density that is given in advance.
- The cut density should be sufficiently small to ensure that there are enough 3D cubes in the depth of the lumber.

In order to comply with the above rules it was decided to cut the lumber according to the scheme of uniform section with identical parts. The selected lumber has the following dimensions: height and width of 100 mm, and length 1 m.

Further, according to the developed software application, the form of which is shown in Figure 1, the calculation of the number and size of 3D cubes was performed. Consequently, with such dimensions of the lumber can be built 3D cubes, which can have 15 different sizes of external facet. If we take the largest dimension of the facet, which is 100 mm, then we will have only 10 cubes, which of course is not enough.


Task 1 - Find

Height, mm. 100
Width, mm. 100
Length, mm. 1000
Result: 15
20
Number of created 3D Cubes 1250

Fig. 1 – View of the software application that is used to calculate the number of required 3D cubes

When selecting the size of facet at 0.25 mm, we get 640 million 3D cubes, the calculation of which, even on powerful computers take long. That is why it was decided to select 3D cubes, the outer edges of which have a size of 20 mm. With such dimensions of external facet, the total number of 3D cubes will be 1250 pieces. After calculation of the required 3D cubes were made the timber section of a given size. This process is fully automated and was achieved by using developed software application that uses capabilities of the SolidWorks API.

The following parameters that will be assigned to 3D cubes include: Height, length and width are given according to the size of created 3D cubes, for example, 20 mm; Wood species; Initial temperature and humidity. If they are different, then it is necessary to uniform distribution along the length of a given timber. The rest of the initial parameters are transmitted to the airspace surrounding the stack. Air space similarly will be presented as an array of 3D cubes of the same size. This representation will allow us to calculate a mathematical model that serves to change the parameters of the drying agent in space and time.

Consequently, when we having 3D cubes, it is necessary to make their transformation in order to represent them in the form of 2D squares. This step is very important and necessary, because with this transformation we will be able to use cellular automata.

To represent cellular automata, we can use one of the two most popular 2D nodes, namely 2D Moore's area and 2D Von Neumann Fields. If we talk about the Moore countryside then it represents a set of eight cells on a square parquet, having a common vertex with this cell. In turn,