Список литературы:

1 Постановление Правления Национального Банка РК «Об утверждении Правил определения размера вреда, причиненного транспортному средству» от 28.01.2016 г. №14. URL: https://adilet.zan.kz/rus/archive/docs/V1600013460/28.01.2016.

2 Закон РК «О порядке рассмотрения обращений физических и юридических лиц» от 12.01.2007 г. №221. URL: https://adilet.zan.kz/rus/docs/Z070000221_.

3 Комментарий к Уголовному кодексу Республики Казахстан. Общая и Особенная части / Под общ.ред. И.Ш. Борчашвили. Изд. 2-е. – Алматы: Жеті жарғы, 2015. – 1120 с.

4 Телибеков Б.А. Телибекова И.М. К вопросу о квалификации мошенничества в сфере страхования // Международный научный журнал «Актуальные проблемы современности»: Карагандинский университет «Болашак» – Баспа. – 2012. – №4 (84). – С. 155-160.

5 Сайт: www.http:e-polis.analitics//Обман в сфере страхования//Аналитика страхового рынка.

6 Галагуза Н.Ф., Ларичев В.Д. Преступления в страховании: предотвращение, выявление, расследование (отечественный и зарубежный опыт). – М., 2000. – 250 с.

7 Ким Ю. Мошенничество в страховании. URL: http://wfin.kz.

8 Уголовный кодекс Республики Казахстан от 03.07.2014 г. №226-V. URL: https://online.zakon.kz/Document/?doc_id=31575252&.

9 Сайт: http://egid.info/ins/inszarubech//Проблемы мошенничества в страховании за рубежом.

10 Уголовный кодекс Российской Федерации от 13.06.1996 №63-ФЗ.URL: http://www.consultant.ru/document/cons_doc_LAW_10699/0e17c9f5bd23686e1c53864f8783a3ca9fed2e60/.

11 Федеральный закон «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» от 29.11.2012 №207-ФЗ.URL: http://www.consultant.ru/document/cons_doc_LAW_138322/.

12 Конституция Республики Казахстан от 30.08.1995 г. URL: https://online.zakon.kz/Document/?doc_id=1005029&.

.

ACTUAL ISSUES PROTECTION WEB RESOURCES

Hozhyi O., senior forensic expert of the department of computer-technical and telecommunication researches, Cherkasy scientific research forensic center MIA of Ukraine
Ptashkin R., deputy head of the department of computer-technical and telecommunication researches, Cherkasy scientific research forensic center MIA of Ukraine

The rapid evolution of information technology is gradually transforming the world. Open and free cyberspace expands the freedom and opportunities of people, enriches society, creates a new global interactive market for ideas, research and innovation, stimulates responsible and efficient government and active involvement of citizens in governance and local issues, ensures publicity and transparency, promotes prevention of corruption. But the development of information technology causes new threats to personal or even national security [1].

The development of the global Internet contributes to the spread of illegal collection, storage, use, destruction or distribution, personal data, illegal financial transactions, theft and fraud on the global network. Cybercrime is becoming transnational and can cause significant harm to the interests of both the individual and society or the state.

Using modern technology, even interstate relations and political confrontation are often continued on the Internet in the form of cyberattacks or even "cyberwar": vandalism, propaganda, espionage, and direct attacks on computer systems, networks or individual servers.

In general, the term "cyberattack" Ukrainian laws define as targeted (intentional) actions in cyberspace, which are carried out using electronic communications (including information and

communication technologies, software, software and hardware, other technical and technological means and equipment) and aimed at achieving one or a combination of the following goals: violation of confidentiality, integrity, availability of electronic information resources processed (transmitted, stored) in communication and/or technological systems, obtaining unauthorized access to such resources; violation of security, sustainable, reliable and regular mode of operation of communication and / or technological systems; use of the communication system, its resources and means of electronic communications for cyberattacks on other objects of cyber defense [2].

In terms of cybersecurity, as a direction to protect the vital interests of man, citizen, society and state in the use of cyberspace, special attention should be paid to certain resources of the global network - official websites of government agencies and structures, financial and business centers, etc. [2]. Such information sources in most cases form the basis for the formation of public opinion and public reaction to certain events. Unlawful interference with the work of official information resources in most cases has a clear purpose - to post false information in order to mislead the public and society, which in everyday life relies on information from the Internet.

The issue of protection of web-resources or web-servers in general is given a lot of attention - information protection is the main activity of whole companies (McAfee, Comodo, Symantec, ESET, etc.), and research in cyber security is the basis of such international organizations and communities like COSIC, Mozilla, W3C, etc. [3-5].

However, the issue of security on the Internet can’t be completely settled, because every day there are errors in the security system of software used for the functioning of web-resources. In addition, the software is periodically updated to correct detected errors and modify functionality, but, unfortunately, correcting some errors leads to others. This fact is the reason for the need for constant monitoring of web security and measures to support security systems.

Therefore, considering the cyber security of the web segment, it is logical and consistent to organize security systems at all levels of the information resource - from http-server to content management system code (hereinafter - CMS) - and create a system of interaction between these levels. It is the possibility of interaction between different levels of the overall structure of the web resource that makes it possible to create a comprehensive and logically complete system of protection of Internet sites.

During the study of the problem of interaction between http-server and CMS software, a huge gap was identified - popular http-servers in their functionality do not contain simple and logical solutions to implement interaction with CMS and response to notifications of unauthorized or non-standard access [7].

The NGINX software, which is the most popular http-server among the Ukrainian segment of the Internet, was subject to detailed research [8]. Vital functions are functions of performing certain actions as a response to a notification from the CMS to events or a series of events of unknown nature and/or those that have signs of possible (potential) cyberattacks that threaten the security of the system as a whole and create a breach. electronic information resources.

As a result of research, among the features of the software NGINX identified functionality that allows you to check the elements of the file system and their properties, such as the existence of files and their access modes [7,6]. These features allow you to organize a basic connection between the http-server and the CMS - in response to abnormal modes of operation or detection of gaps in the security system, internal CMS algorithms can create certain label files with the necessary properties, and web-server software will respond to these labels. That is, at the content management system level, in the event of an emergency - entering an incorrect password more than N times, requesting a non-existent partition or file, sending knowingly incorrect data, etc. - the system creates a tag file corresponding to the user's IP address, and initiates a repeat request. The software of the http-server at the next request of the same user notices existence of a file-label and carries out the necessary action - blocking of request or its redirection, etc.

As an example of the positive experience of applying the above approach, we can cite the official website of the Cherkasy forensic center (ndekc.ck.ua) and some information and analytical systems used in the Expert Service of the Ministry of Internal Affairs of Ukraine. Therefore, the internal codes of content management systems are organized in such a way that in case of detection of signs of threat to the security of the resource, in a specially designated directory creates a label file. Each time a user requests a server, NGINX checks the existence of a label file before performing its basic functions. The existence of such a file is a direct signal that the current request of the user may compromise the security system and in order to prevent the threat - blocked (HTTP status 403).

As additional functionality of the security system, it is possible to implement the entry in a special file of information about the request and the state of the server at a certain time, the content of internal variables, and so on. But these basic functions allow to connect different levels of the general functional unit and to organize complex protection.

It has also been found that file system features are almost mandatory for most software used to organize http servers. That is, this approach can be easily imported and implemented in any modern web-server.

The work investigates the functionality of software used to organize the work of web servers, and developed and proposed algorithms that allow to organize comprehensive protection systems at several levels of web resource, which in turn improves algorithms to prevent breaches of confidentiality, integrity, availability of electronic information resources and breaches of security, sustainable, reliable and regular operation or gaining unauthorized access to them.

References:

1. On the decision of the National Security and Defense Council of Ukraine of January 27, 2016 "On the Cyber Security Strategy of Ukraine" URL: https://zakon.rada.gov.ua/laws/show/96/2016 (access date 05.02.2022);

2. On the basic principles of cyber security of Ukraine URL: https://zakon.rada.gov.ua/laws/show/2163-19 (access date 05.02.2022);

3. COSIC Computer Security and Industrial Cryptography URL: https://www.esat.kuleuven.be/cosic/about-us/ (access date 05.02.2022);

4. Web Security MDN URL: https://developer.mozilla.org/en/docs/Web/Security

5. W3C Security Activity URL: https://www.w3.org/Security/;

6. Derek DeJonghe: NGINX Cookbook Advanced Recipes for High Performance Load Balancing: O'Reilly Media, Inc ISBN 978 1-491-96893-2;

7. NGINX: documentation URL: https://nginx.org/ru/docs/ (access date 05.02.2022);

8. Usage Statistics and Market Share of Web Servers, February 2022. URL: https://w3techs.com/technologies/overview/web_server (access date 05.02.2022).

ВОПРОСЫ СОВЕРШЕНСТВОВАНИЯ ПЕРЕЧНЯ КОРУПЦИОННЫХ УГОЛОВНЫХ ПРАВОНАРУШЕНИЙ В УГОЛОВНОМ КОДЕКСЕ УКРАИНЫ И УГОЛОВНОМ КОДЕКСЕ РЕСПУБЛИКИ КАЗАХСТАН

Чуб Ю.С.
факультет права и предпринимательства
ООО «Харьковский университет»

В Уголовном кодексе Украины (далее – УК Украины) ст. 12 «Классификация уголовных правонарушений» определяет разделение уголовных правонарушений по их степени тяжести, а именно уголовные проступки и преступления (нетяжкие, тяжкие и особо тяжкие) [1]. В соответствии с Законом Украины «О предотвращении коррупции» коррупцией считается использование лицом, указанным в части первой статьи 3 настоящего Закона,предоставленных ему служебных полномочий или связанных с ними