Автоматика. Энергетика. ИКТ

DOI 10.52209/1609-1825_2022_4_396 UDC 004.056.5

Analysis of Existing Goals of Network Attacks and Methods of Attacks on Websites

[1]***BARAKOVA Aliya,*** *doctoral student, balia_79@mail.ru,*
[2]***USSATOVA Olga,*** *PhD, Docent, uoa_olga@mail.ru,*
[1]*NPJSC «Al-Farabi Kazakh National University», Kazakhstan, Almaty, Al-Farabi Avenue, 71,*
[2]*Institute of Information and Computational Technologies, Kazakhstan, Almaty, Shevchenko Street, 28,*
**corresponding author.*

Abstract. *All existing targets of network attacks are considered. An analytical study of the percentage of targets of network attacks and attacks on WEB sites is carried out in order to identify the most critical area for protection. The article also includes comparative analysis of cyberattacks by state and data on which areas of threat were most affected by the attack. The relevance of the study lies in the fact that with the development of websites, organizations are faced with a new technology where the foundations of information security have not yet been formed. At the same time, websites, namely information within its framework, become the desired object of fraudulent operations and illegal actions for identity theft, which can be used for authentication on various resources and platforms.*

Keywords: *network attack, methods of network attacks, information security, goals of network attacks, attack rating, the level of information security, globalization.*

Introduction

According to the results of the year 2021, the do mestic information security market has grown by 25%. In short, this growth is due to three reasons. Firstly, the topic of information security is becoming more and more relevant, including due to objective reasons: the number of threats and the activity of cybercriminals in general are growing year by year. The problem of cyber security is becoming more and more clear and close to the management of various companies and, accordingly, the principle of inability to implement certain business risks is becoming more and more important. Obviously, building practical security of this kind goes in league with increasing the budgets involved.

Second, critical information security cyber security, as a concept that began several years ago with surveys, categorization and design, has finally

reached the period of actual implementation. And this, in turn, ensures the growth of turnover of protection manufacturers and their integration.

Thirdly, we cannot say that the COVID-19 pandemic had no impact on the cyber security market. In reality, however, there has been more talk on the subject than practical impact. By the end of the first quarter of 2020, a situation began to emerge that raised a number of concerns: the total number of pilot projects has dropped dramatically. And it is completely understandable why this happened – in the updated conditions (lockdown, hasty transition to a remote format of work) these projects have become objectively more difficult (and sometimes even impossible) to carry out on the sites of companies.

Websites and web applications are just as susceptible to security breaches as physical homes, stores and government offices. Unfortunately, cybercrime happens every day, and serious security measures are needed to protect websites and web applications from being hacked [1].

This is exactly what makes web-security-a system of security measures and protocols that can protect your Web site or Web application from hacking or infiltration by unauthorized personnel. This integral division of information security is vital to the protection of Web sites, Web applications, and Web services. Anything applied over the Internet must have some form of web security to protect it.

Given the events of 2020 and early 2021, the shift to a remote work format has become most urgent, and the pace continues to gain momentum. Greater responsibility has fallen on employees responsible for setting up corporate networks and servers. All of this has put companies' data at risk of compromise.

According to forecasts by experts of American IT-company HP Inc., in 2021 the negative impact on security of IT infrastructures of many large organizations around the world will continue to increase.

Uncontrolled web vulnerabilities can lead to corporate data leaks, loss of access to accounts and personal accounts of important services, financial documents, and personal data of employees and customers. Web resources are a key element in the corporate environment because they contain a lot of valuable information that affects the core functions of a company's infrastructure management.

Now it is hard to imagine any company without the use of web resources, which are the basis for the promotion of products and services in the market. What security threats can be expected? In the following article, we offer a list of the most popular web vulnerabilities.

Research methodology

According to the Web Application Security Consortium, the OWASP working group has published a draft of the new Top 10 Web Application Security Risks 2021 list. The list has been maintained by OWASP since 2003 and was last updated in 2017 [2].

OWASP (Open Web Application Security Project) is an international non-profit organization that focuses on analyzing and improving software security [1]. This community has developed a list of the ten most dangerous vectors of attacks on web applications – OWASP TOP-10:

From figure 1 shows that the main purpose of network attacks, namely, such as information destruction, installation of malicious software, information theft and misinformation associated with the disclosure, modification of information to gain unauthorized access to the rights of the owner who has access to the use of computer resources. It is also worth noting purposes such as forced inactivity of the network, the purpose of which is a distributed denial of service and even such non-obvious as link spam, the purpose of which is to increase the citation index of the site [3].

The percentage of attacks on Web sites shown in figure 2.

Our primary goal in researching website attacks was to determine which attacks are most popular with attackers and what their motives might be, as well as to identify the main sources of threats for different industries. This data provides insight into what needs to be addressed when securing web applications.

Cyberattacks are the actions of cybercriminals that target computer systems, databases, infrastructure, and website visitors.

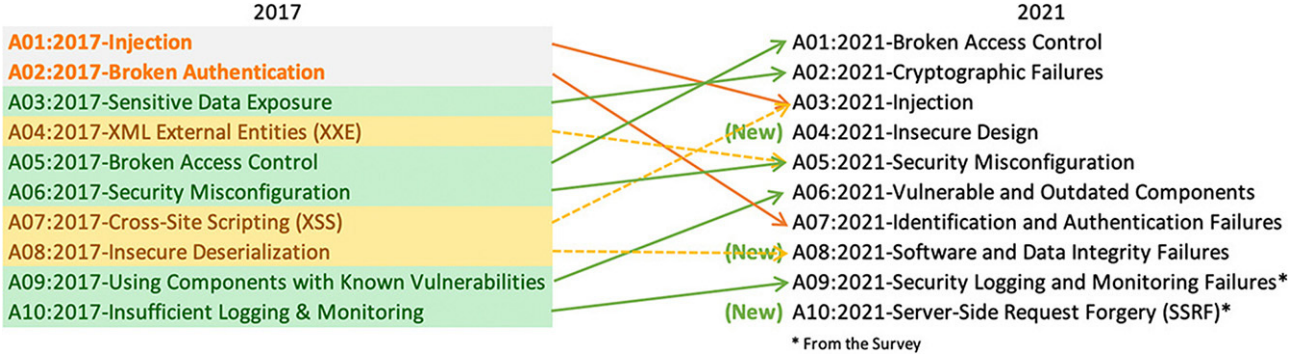

Figure 1 – List of the ten most dangerous attack vectors for web applications

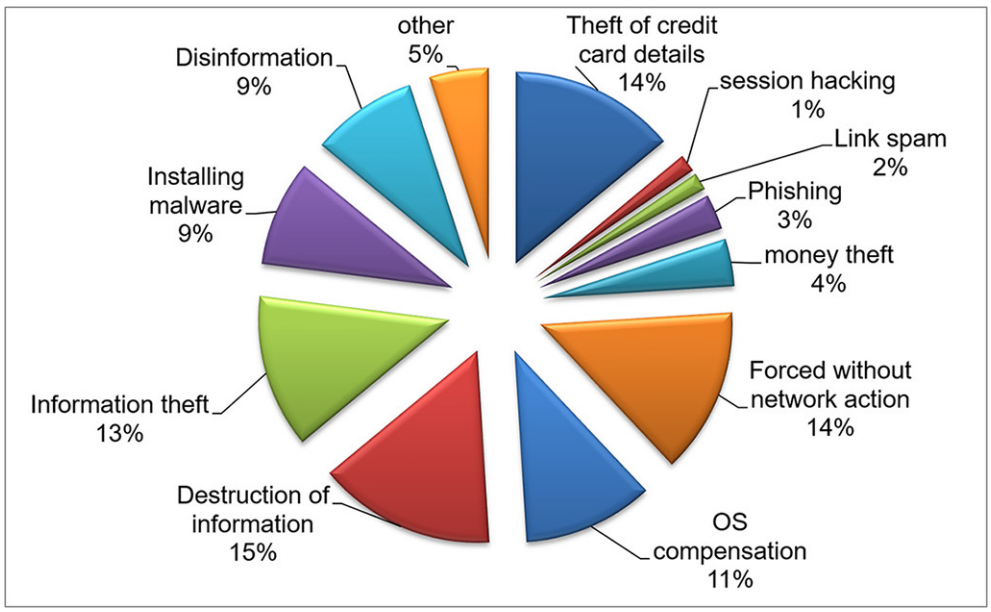

Figure 2 – Types of attacks

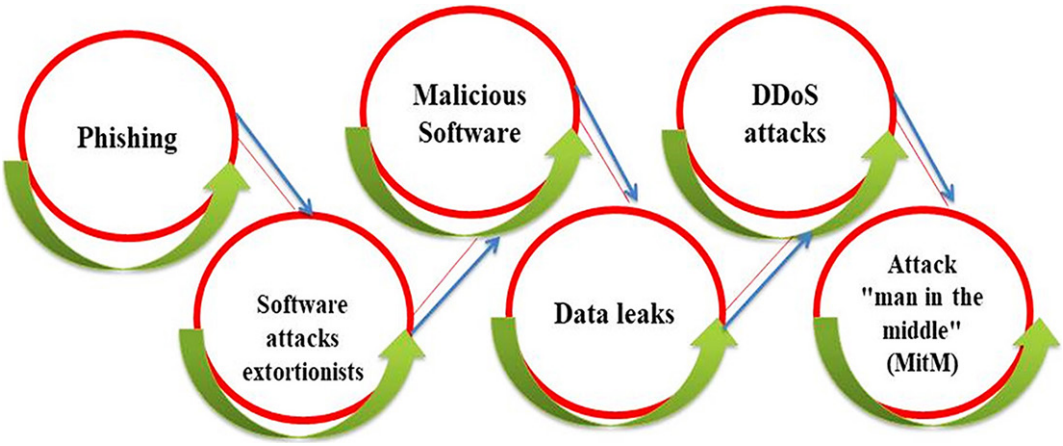

Figure 3 – The most popular types of cyberattacks in 2021

1. Phishing

Phishing is an attack that basically uses email as a vector and tricks people into downloading malware to their devices. About 75% of organizations experienced phishing in 2020 [4].

Many phishing attacks use seemingly unsuspicious links and files to deceive. Hackers also use psychological tricks and know who to pretend to be to get their way.

In 2020, there were many phishing emails related to COVID-19. Attackers allegedly sent out information on behalf of the World Health Organization, playing on our fear. Other cybercriminals used click bait headlines related to business, credit, and politics.

2. Ransom ware attacks

Ransom ware is malware that blocks users from accessing their software and demands that they pay a ransom. Usually ransom ware spreads through spam or social engineering [4].

3. Malware

Malware stops or significantly slows down the operation of your devices. Spyware, viruses, worms, ransom ware, or Trojans are all used by cybercriminals. Malware arrives on devices via email attachments with malicious code or file-sharing programs that distribute dangerous material disguised as music or images [4].

4. Data Leaks

A data leak occurs when a user's sensitive information becomes vulnerable. In 2020, many companies reported data breaches, and the trend is expected to continue in 2021 [4].

5. DDoS attacks

DDoS attacks occur when an attacker directs a large volume of traffic to a system or server, forcing it to stop or suspend operations. Given that IT downtime costs anywhere from $300,000 to $1 million per hour, such antics can cost a company money. In 2020, Google reported that it suffered a 2.5Tbps DDoS

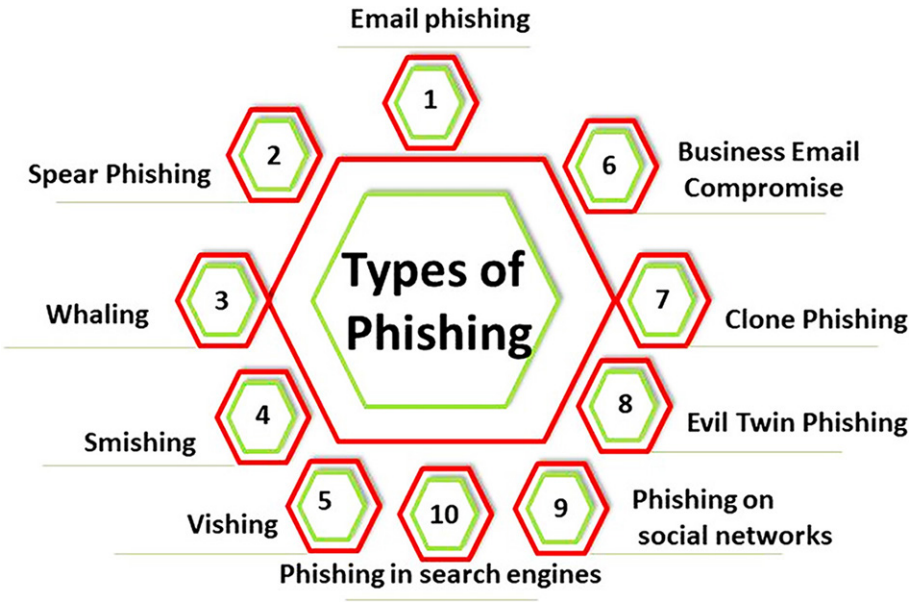

Figure 4 – Types of phishing

attack, the largest attack to date, affecting 180,000 Web servers [4].

6. Man-in-the-middle (MitM) attack

Mediator attacks occur when an attacker intercepts and alters electronic communications. An example would be a fake Wi-Fi hotspot that looks and works like the real thing, but intercepts your information. With the growing trend of remote working and digital communications, it has become increasingly important for companies to use end-to-end encryption for messaging and video conferencing. In response to criticism at the beginning of the pandemic, Zoom implemented end-to-end encryption to protect businesses during video calls.

Other types of attacks that hackers may also actively use in 2022 [5]:

- SQL injection – getting unauthorized access to information using a structured query language;
- Zero-day exploits – quick exploitation of security flaws;
- brute-force attacks, or brute-force – breaking a password by trying all possible variants of the key;
- DNS tunneling – turning domain name systems into hacker weapons.

There are the following ways to combat these types of attacks [6]:

1. Using antivirus tools and regularly updating their signatures. Can solve the problem with Trojans, viruses, mail worms, but will not solve the problem of sniffers and go-betweens.
2. Encryption of transmitted data. The problem does not completely solve the sniffers problem, however, the adversary intercepts data that cannot be freely read. It takes time to decrypt them.
3. Use of anti-sniffers (e.g. AntiSniff or PromiScan).
4. Use of firewalls.
5. Use of anti-rootkits.

Research results

The rating of the cyber threat is not clear, so you can't be sure it's the same as the rating of the security system. Global Cyber Threat Exposure Index 2020 (CEI – Cybersecurity Exposure Index).

As every country gets used to the new, unprecedented order of things in post – COVID 19 reality, the need for cyber security to secure digital infrastructure is becoming increasingly urgent.

Cybercrime can take many forms:

- from device-specific attacks aimed at gaining unauthorized access, stealing data and extorting money by blocking access to files or computer systems;
- to attacks on cloud infrastructure, the ultimate goal of which is to compromise virtual machines and use them as weapons.

The study indicates the most recent data on which countries are most vulnerable, least vulnerable, and those with an average, intermediate, value [7].

Table 1 presents the Cyber Threat Exposure Index (CEI – cyber security Exposure Index) by country from 0 to 1. It shows: the higher the score, the more vulnerable a country is to cyber attacks and, therefore, the lower its level of cyber security.

Kazakhstan, unfortunately, ranks 51st with a score of 0.579, demonstrating a very high level of exposure to cyber threats (consequently, a very low level of cyber security).

The study provides the latest data on which countries are most vulnerable, least vulnerable and those with an average, intermediate, value.

The most attacked industry

The share of targeted cyber attacks over the past year exceeded the share of mass attacks, and the most attacked sectors were government agencies, industry, medicine, education, and the financial sector [8].

Table 1 – Global Cyber security Impact Index 2020 Chart

Top 10 countries			Kazakhstan 51 places			Number of countries		
Finland	1	0.110	Egypt	48	0.548	Morocco	75	0.748
Denmark	2	0.117	Kenya	48	0.548	Pakistan	76	0.755
Luxembourg	3	0.124	Albania	49	0.566	Bangladesh	77	0.759
Australia	4	0.131	Panama	50	0.569	Nepal	78	0.762
Estonia	5	0.134	Ukraine	50	0.569	Bolivia	79	0.783
Norway	5	0.134	Kazakhstan	51	0.579	Libya	80	0.793
Japan	6	0.138	Lebanon	51	0.579	Venezuela	81	0.807
United States	7	0.145	Bosnia and Herzegovina	52	0.583	Palestine	82	0.855
Austria	8	0.162	Jordan	53	0.586	Ethiopia	83	0.866
Switzerland	9	0.172	Colombia	54	0.590	Myanmar	84	0.910
New Zealand	10	0.179	India	55	0.597	Afghanistan	85	1.000

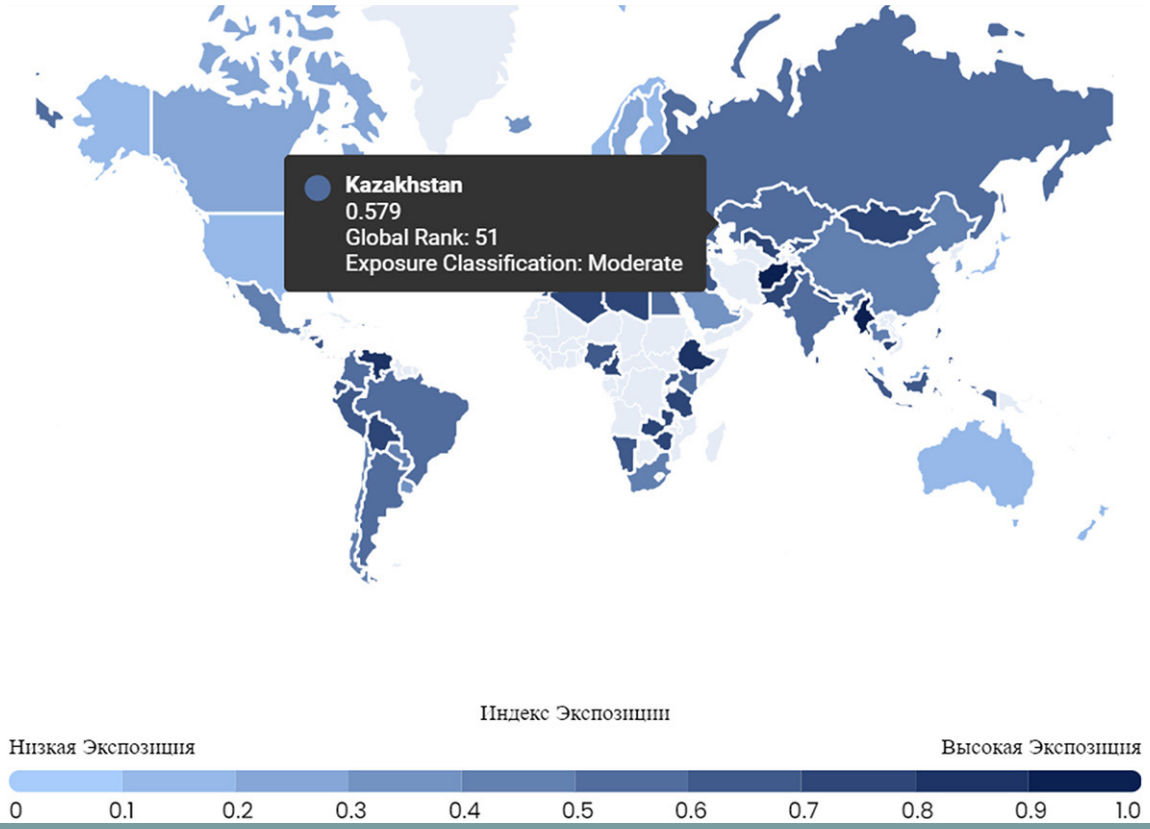

Figure 5 Cybersecurity Impact Index in Kazakhstan

Table 2 – Distribution of countries by level of exposure to cyber threats: The numbers in the table denote the number of countries

Region	Very tall	High	Average	Short	Very low
Europe	0	22	10	21	8
North America	0	3	4	1	1
South America	1	3	5	1	0
Asian-Pacific area	3	11	8	7	3
Africa	1	11	3	1	0
All countries	5	30	30	31	12

Table 3 – Priority sectors for hackers in 2021

№	Organization	Increase in attacks on
1	Organizations from the fields of education and research	75%
2	Organizations from the state and defense sphere	47%
3	Communication organizations	51%
4	IT service providers	67%
5	Organizations from the healthcare sector	71%
6	Organizations from the healthcare sector	75%

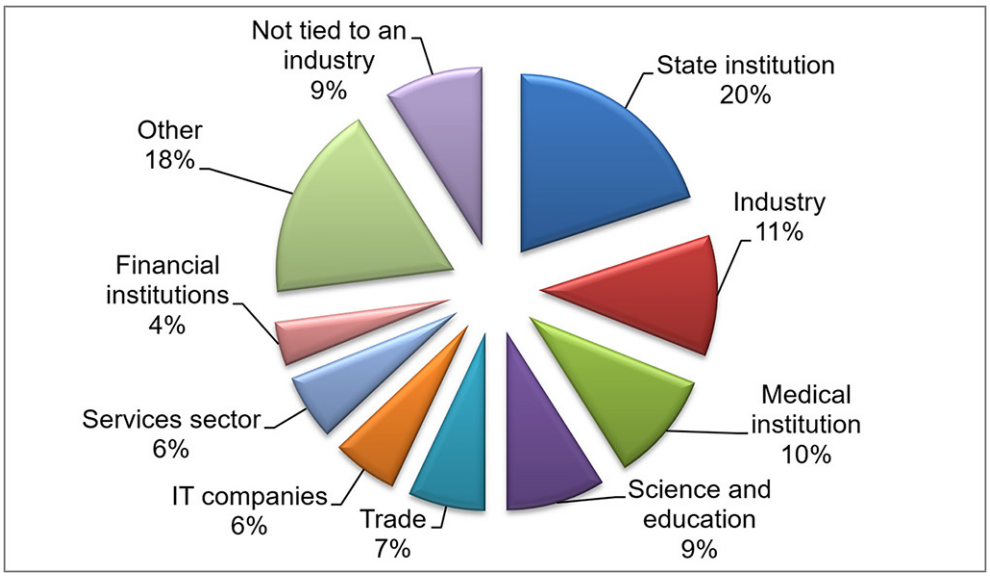

Figure 6 – Categories of victims among organizations

Conclusion

In this article we looked at what attacks mean and how to protect your site from attacks. It is important to remember that such malicious actions can disable even the safest and largest web resources. This will have serious consequences in the form of huge losses and loss of customers. That is why securing your resource against attacks is an urgent task for all commercial structures and government agencies.

The pandemic also continues to affect different areas of life. Cybersecurity has not been spared. Now developers are looking for new protection options or improving old ones. It is clear that the COVID-19 situation is not the reason for the increase in cyber attacks, but just another opportunity for mass confusion, which cybercriminals take advantage of [9].

Thus, we considered the main network attacks and ways to combat them [10]. This area is the most evolving, as there is a constant rivalry between attackers and data security organizations. Despite the possible use of comprehensive measures to protect your computer, the most reliable way to protect your computer is to use trusted electronic resources, reading emails from trusted sources. i.e. the greatest protection from attacks can be provided by the user himself by taking precautions.

REFERENCES

1. Прохоренко В., Чу К.-К.Р., Ашман Х. Контекстно-ориентированная модель защиты веб-приложений // Прикладная математика и вычисления. 2016. Том 285. С. 59-78.
2. Проект OWASP обновил список рисков безопасности web-приложений / 13 сентября, 2021. С-1 URL: https://www.securitylab.ru/news/524358.php (дата обращения: 17.01.2022).
3. Дафа-Аллах А., Эльханг А.М. Предлагаемая модель безопасности для веб-приложений и сервисов // Международная конференция по связи, управлению, вычислительной технике и электронике 2017 (ICCCCEE). – 2017. С. 1-6.
4. Дипа Г., Тилагам П.С. Защита веб-приложений от уязвимостей, связанных с внедрением и логикой: подходы и проблемы // Информационные и программные технологии. 2016. Том 74. С. 160-180.

5. Верма А.К. Классификация атак SQL-инъекций с использованием нечеткого заражения // Достижения в области интеллектуальных систем и вычислений. 2018. Том. 518. С. 463-469.
6. Буглиези М., Кальзавара С., Фокарди Р. Формальные методы веб-безопасности // Журнал логических и алгебраических методов в программировании. 2017. Том 87. С. 110-126.
7. Глобальный индекс воздействия кибербезопасности 2020 / PasswordManagers.co, URL: https://infogram.com/global-cybersecurity-exposure-index-2020 passwordmanagersco-1h7k23z7dqqv6xr (дата обращения: 02.02.2022).
8. Актуальные киберугрозы: II квартал 2021 года / Дата публикации 30 августа 2021, URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021-q2/ (дата обращения: 02.02.2022).
9. Аль-Хурафи О.Б., Аль-Ахмад М.А. Обзор атак на уязвимости веб-приложений // 4-я Международная конференция по передовым приложениям и технологиям в области компьютерных наук 2015 (ACSAT). – 2016. С. 154-158.
10. Сяо Х., Ян Р., Е Р., Ли К., Пэн С., Цзян Ю. Обнаружение и предотвращение атак с внедрением кода в приложения на основе HTML5 // Третья Международная конференция по передовым облачным технологиям и большим данным 2015. – 2016. С. 254-261.

Желілік шабуылдардың мақсаттары мен веб-сайттарға жасалатын шабуыл әдістерін талдау

[1]***БАРАКОВА Алия Шаризатқызы,** докторант, balia_79@mail.ru,*
[2]***УСАТОВА Ольга Александрқызы,** PhD, доцент, uoa_olga@mail.ru,*
[1]«Әл-Фараби атындағы Қазақ ұлттық университеті» КеАҚ, Қазақстан, Алматы, Әл-Фараби даңғылы, 71,
[2]Ақпараттық және есептеуіш технологиялар институты, Қазақстан, Алматы, Шевченко көшесі, 28,
**автор-корреспондент.*

***Аңдатпа.** Желілік шабуылдардың барлық мақсаттары қарастырылған. Желілік шабуылдар мен веб-сайттарға шабуылдардан қорғаудың ең маңызды саласын анықтау мақсатында аналитикалық зерттеудің пайыздық мөлшерін жүргізеді. Мақалада сондай-ақ мемлекеттер бойынша кибершабуылдардың салыстырмалы талдауы және шабуыл қай қауіп-қатерге ең көп әсер еткені туралы мәліметтер бар. Зерттеудің өзектілігі веб-сайттардың дамуымен ақпараттық қауіпсіздік ұйымдар негіздері әлі қалыптаспаған жаңа технологиямен бетпе-бет келеді. Сонымен бірге веб-сайттар, атап айтқанда олардың ішіндегі ақпарат, әртүрлі ресурстар мен платформаларда аутентификация үшін пайдаланылуы мүмкін алаяқтық операциялар мен жеке деректерді ұрлау үшін заңсыз әрекеттердің қалаған объектісіне айналады.*

***Кілт сөздер:** желілік шабуыл, желілік шабуыл әдістері, ақпараттық қауіпсіздік, желілік шабуыл мақсаттары, шабуылдардың рейтингі, ақпараттық қауіпсіздік деңгейі, жаһандану.*

Анализ существующих целей сетевых атак и методов атак на веб-сайты

[1]***БАРАКОВА Алия Шаризатовна,** докторант, balia_79@mail.ru,*
[2]***УСАТОВА Ольга Александровна,** PhD, доцент, uoa_olga@mail.ru,*
[1]НАО «Казахский национальный университет имени Аль-Фараби», Казахстан, Алматы, пр. Аль-Фараби, 71,
[2]Институт информационных и вычислительных технологий, Казахстан, Алматы, ул. Шевченко, 28,
**автор-корреспондент.*

***Аннотация.** Рассматриваются все существующие цели сетевых атак. Аналитическое исследование процентного соотношения целей сетевых атак и атак на веб-сайты проводится с целью выявления наиболее критичной области для защиты. Статья также включает сравнительный анализ кибератак по государствам и данные о том, какие области угрозы были наиболее затронуты атакой. Актуальность исследования заключается в том, что с развитием веб-сайтов организации сталкиваются с новой технологией, где основы информационной безопасности еще не сформированы. В то же время веб-сайты, а именно информация в их рамках, становятся желанным объектом мошеннических операций и незаконных действий для кражи личных данных, которые могут быть использованы для аутентификации на различных ресурсах и платформах.*

***Ключевые слова:** сетевая атака, методы сетевых атак, информационная безопасность, цели сетевых атак, рейтинг атак, уровень информационной безопасности, глобализация.*

REFERENCES

1. Prokhorenko V., Choo K.-K.R., Ashman H. Context-oriented web application protection model // Applied Mathematics and Computation. 2016. Vol. 285. pp. 59-78.
2. The OWASP project has updated the list of web application security risks / September 13, 2021. C-1 URL: https://www.securitylab.ru/news/524358.php (accessed: 17.01.2022).
3. Dafa-Allah A., Elhang A.M. Proposed security model for web based applications and services // International Conference on Communication, Control, Computing and Electronics Engineering 2017 (ICCCCEE), – 2017. pp. 1-6.
4. Deepa G., Thilagam P.S. Securing Web applications from injection and logic vulnerabilities: Approaches and challenges // Information and Software Technology. 2016. Vol. 74. pp. 160-180.
5. Verma A.K. Classification of SQL injection attacks using fuzzy tainting // Advances in Intelligent Systems and Computing. 2018. Vol. 518. pp. 463-469.
6. Bugliesi M., Calzavara S., Focardi R. Formal methods for Web security // Journal of Logical and Algebraic Methods in Programming. 2017. Vol. 87. pp. 110-126.
7. Global Cybersecurity Impact Index 2020 / PasswordManagers.co, URL: https://infogram.com/global-cybersecurity-exposure-index-2020 passwordmanagersco-1h7k23z7dqqv6xr (accessed 02.02.2022).
8. Current cyber threats: II quarter of 2021 / Publication date August 30, 2021, URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021-q2/ (accessed: 02.02.2022).
9. Al-Khurafi O.B., Al-Ahmad M.A. Survey of Web Application Vulnerability Attacks // 4th International Conference on Advanced Computer Science Applications and Technologies 2015 (ACSAT). – 2016. pp. 154-158.
10. Xiao X., Yang R., Ye R., Li Q., Peng S., Jiang Y. Detection and Prevention of Code Injection Attacks on HTML5-Based Apps // Third International Conference on Advanced Cloud and Big Data 2015. – 2016. pp. 254-261.