**WEBSITE**

**Development of a system for detecting fraudulent activities in online payments**

A project undertaken as part of BSc (Hons) Business Information Systems Degree, Westminster International University in Tashkent

**Student:** Laylo Abdukhalilova

**Email:** [labdukhalilova@students.wiut.uz](mailto:labdukhalilova@students.wiut.uz)

**Course:** Business Information system

**Submission date:** 7/04/2023

**Supervisor:** Shirin Primkulova

Table of Contents

[Glossary 4](#_Toc136987062)

[Introduction 5](#_Toc136987063)

[Problem Overview 6](#_Toc136987064)

[Project objectives 7](#_Toc136987065)

[Business objectives 7](#_Toc136987066)

[Technical objectives 8](#_Toc136987067)

[Academic objectives 8](#_Toc136987068)

[Project Scope 9](#_Toc136987069)

[Methodology Business 10](#_Toc136987070)

[Literature Review 10](#_Toc136987071)

[Online shopping 10](#_Toc136987072)

[Analytical analysis of existing systems on the market 12](#_Toc136987073)

[Bank transfers 13](#_Toc136987074)

[Cybersecurity in online transaction 14](#_Toc136987075)

[Brief analysis of the regulatory framework for information security in Uzbekistan 16](#_Toc136987076)

[Brief Overview 18](#_Toc136987077)

[Observation 19](#_Toc136987078)

[Solution 21](#_Toc136987079)

[SWOT analysis 22](#_Toc136987080)

[Strengths 22](#_Toc136987081)

[Flaws 22](#_Toc136987082)

[Possibilities 22](#_Toc136987083)

[Threats 23](#_Toc136987084)

[Porter's Five Forces 23](#_Toc136987085)

[Buyers 23](#_Toc136987086)

[Suppliers 24](#_Toc136987087)

[Current competitors 25](#_Toc136987088)

[New competitors 26](#_Toc136987089)

[Substitute products 26](#_Toc136987090)

[PESTL Analysis 27](#_Toc136987091)

[Political factors 27](#_Toc136987092)

[Economic forces 27](#_Toc136987093)

[Social factors 29](#_Toc136987094)

[Technological factors 30](#_Toc136987095)

[Legal factors 30](#_Toc136987096)

[Environmental factors 31](#_Toc136987097)

[Monetization 31](#_Toc136987098)

[Subscription monetization 32](#_Toc136987099)

[Methodology computing 33](#_Toc136987100)

[Creation of a fraud detection system for online payments and its implementation 33](#_Toc136987101)

[Creation of the user interface of the system. Types of user interfaces and stages of their creation 36](#_Toc136987102)

[System implementation 38](#_Toc136987103)

[Algorithms for fraud detection 51](#_Toc136987104)

[Integration 55](#_Toc136987105)

[Statistics of traffics 55](#_Toc136987106)

[Diagrams 57](#_Toc136987107)

[Concept Map 57](#_Toc136987108)

[UML diagrams 58](#_Toc136987109)

[Project schedule 59](#_Toc136987110)

[Critical Self Evaluation 60](#_Toc136987111)

[Psychological assessment 60](#_Toc136987112)

[Academic Grade 61](#_Toc136987113)

[Conclusion 61](#_Toc136987114)

[Reference List 63](#_Toc136987115)

# Glossary

Client’s data theft– The eCommerce industry is full of cases where criminals have stolen the information about inventory data, personal information of customers, such as addresses and credit card details.

Cyberattack - is an unauthorized attempt to exploit and damage computer systems, steal data, or disrupt business processes.

Network security - actions to protect computer networks from various threats, such as targeted attacks or malware.

Unique malicious URLs - when a user clicks on an attachment, they are automatically redirected to a fraudulent URL.

Unique malicious objects - are divided into viruses and worms, Trojans, suspicious packers and malicious tools.

Bad Bots - programmed to perform a task that will hurt company or website visitors.

Spams - unnecessary e-mails, promotional letters, etc., sent by individual companies via the Internet or e-mail.

Proxy - server is an additional link between user and the Internet. A certain intermediary that separates a person from the visited site. Creates conditions under which the site thinks that the proxy is a real person. Just not the user.

SQL attacks - SQL injection is a method of using user data through the input field of web pages.

Malicious data, when received by a server or application, can be used to manipulate user and company data.

Web server - is software that is managed by a hosting provider so that visitors can browse the web on site.

The user interface (UI) is the point at which people interact with a computer, website, or application.

# Introduction

In the era of globalization, everything familiar and necessary becomes accessible, comfortable and requires less and less time at the request of the general public.

One of the most advanced digital versions of habitual activities has become shopping. To be more precise online shopping.

The idea of ​​creating the first online store came from Jeff Bezos in 1994 in the United States.  Traveling from New York to Seattle, he thought about how much interest in the Internet has grown. The Internet is no longer an e-mail system, people began to work on the net, look for information, get acquainted with the news.

Since trading via the Internet is a remote way of trading, the issue of payment methods needs to be adjusted. It required cooperation with banks.  Thus, the first electronic payment system was developed. Currently, goods can be paid for with electronic money, cash on delivery, through terminals.

But even today, this does not always end successfully due to cybersecurity, or, to be more precise, its absence. This is a serious problem on the Internet. E-commerce sites record important customer data such as name, phone number, address, and bank details. If strict cybersecurity measures are not put in place on these sites, buyers' data could fall into the wrong hands, which could then damage their bank account. Most of the big players in online trading certainly use best-in-class security measures to protect their clients' data, but the same cannot be said for the countless smaller sites that may not have the expertise and budget to do so. Online shopping is too convenient to be bothered by these issues. But if ecommerce sites can solve these problems, they will certainly improve the customer experience and therefore lead to more sales. Customers, in turn, will have full confidence in payment systems, peace of mind for their earned money and safe purchases even in the newest small online stores.

However, as mentioned above, with the development of technology, cybercriminals are becoming more sophisticated in their fraudulent activities, which makes it difficult to protect users from such attacks. To overcome this problem, the development of a system for detecting fraudulent activities in online payments has become a vital necessity for both businesses and customers. This system of graduation project uses advanced information technology algorithms and techniques to analyze user behavior on the Internet and detect any suspicious activity that may indicate a fraudulent attempt. In this topic, we will delve into the development of such a system and its potential for protecting users' online transactions from malicious attacks.

In other words, in this project, careful work was carried out to analyze the vulnerabilities of online transactions, identify the most dangerous types of attacks and implement functions to combat them in the project website, which online shoppers can use to provide security in the payment system to their customers.

# Problem Overview

While the rise of e-commerce has improved online transactions, it has attracted the attention of scammers at the same pace. E-commerce cybercrime statistics show that the online transaction industry is one of the most vulnerable when it comes to cybercrime.

Attacks result in significant financial losses, market share, and reputational damage.  According to statistics, 60% of small online e-commerce stores that have been subjected to cybercrime do not conduct their business for more than six months.

In a 2021 article, Forbes reports that as a result of the pandemic, which changed the world, led to the massive development of digital technologies, it also brought with it quite a few problems. One of which is online fraud. Some have become scammers from losing their jobs, others from lack of funds during the pandemic for treatment, food, housing or other needs, others simply went crazy spending the whole day at home. But this is not a reason to engage in robbery. The losses were enormous.

Lost money from 2019 to 2020 has increased significantly. In Singapore alone, reported fraud increased by over 65% in 2020 and over $210,000,000 was lost.

Therefore, it is very important to take strong security measures and hire a reliable team. This will allow entrepreneurs to run business without worrying about being shut down by cybercriminals.

Security issues in e-commerce are not something an online business can ignore. In practice, this should be a priority for most online stores so that their customers can enjoy a fast and secure shopping experience. The better the security protocols, the better the brand will be able to maintain its reputation and gain customer trust.

# Project objectives

This project has several goals, which can be divided into three main categories.

## Business objectives

This includes the mission of the project itself.

• Market research and identification of the main problems of weak cybersecurity

• Analysis of competitors, their working conditions, pros and cons of their systems

• Identification of all necessary features that must be implemented in the website for convenient use

• Provide companies, small businesses, online stores with a website that will help them increase the level of security during online transactions of customers in their online stores.

• Help to increase the sales and reputation of start-up online stores with a secure payment system

• Provide users with a clear, user-friendly design

• Provide buyers of online stores with a secure payment

• Study ways to monetize this type of service and implement them in my project

## Technical objectives

• Developing a system to detect fraudulent activities in online payments

• Developing a website using professional services, streamlined code editor Visual Studio Code

• Developing a user-friendly user interface in a website with complex functionality

• Implement a website security system against the most common types of fraud, which will be shown in detail below

• Implement a blacklist of IP addresses and suspicious IPs

• Improve the payment system, as security is one of the main criteria for online shopping

## Academic objectives

• Detection of various types of fraud in online payments

• Review of alternative methods that have been used for fraud detection

• Apply knowledge of programming languages ​​HTML, CSS, JS, MySQL

• Study the bases of such programming languages ​​as PHP, Apache, OpenServer to use them in system development

• Explore the online payment and cybersecurity industry

• Analyze the root causes of problems and find solutions to them

# Project Scope

The above has detailed cybersecurity issues in online transactions. Therefore, in this project, in order to eliminate these problems, a website is proposed to protect users' personal data from all-round scammers.

The project is presented as a website due to the fact that it will function inside applications or websites of online stores. This is done for the convenience of users so that they do not have to download a separate application to secure their data.

Website includes:

1. Login and password page

2. Site panel

3. Information about the site

4. List of IP addresses

5. Warning page

6. Sections 4 types of fraud:

SQL injection section

Bad bots

Proxy

Spam section

Database for site implementation:

1. Log chart that keeps track of what is happening in the system

2. Table fixing the authorization status in the system

3. Schedule for tracking incoming and outgoing Internet traffic

4. Whitelist IP addresses and files

5. Main ban schedule

And another thing that will be described in detail in the methodology computing section.

And other functions that will be described in detail in the methodology computing section.

Secondary research was conducted to analyze the industry and competitors. SWOT and PESTLE analyzes were carried out for better analysis and development of the project.  Several types of monetization have been studied that will bring profit to the project.

# Methodology Business

## Literature Review

### Online shopping

The importance of e-commerce and online shopping.

Thanks to the many cons, more and more people these days are choosing online shopping over brick-and-mortar shopping. In recent years, the decision-making process of the buyer has changed dramatically. If a few years ago people still did not trust online stores one by one, now the time pressure is pressing, people are making online purchases more and more often.

Taking advantage of this, online stores expand and improve their services.

Digital journalist Tim Borovkov offers some of the top reasons people choose online shoppers.

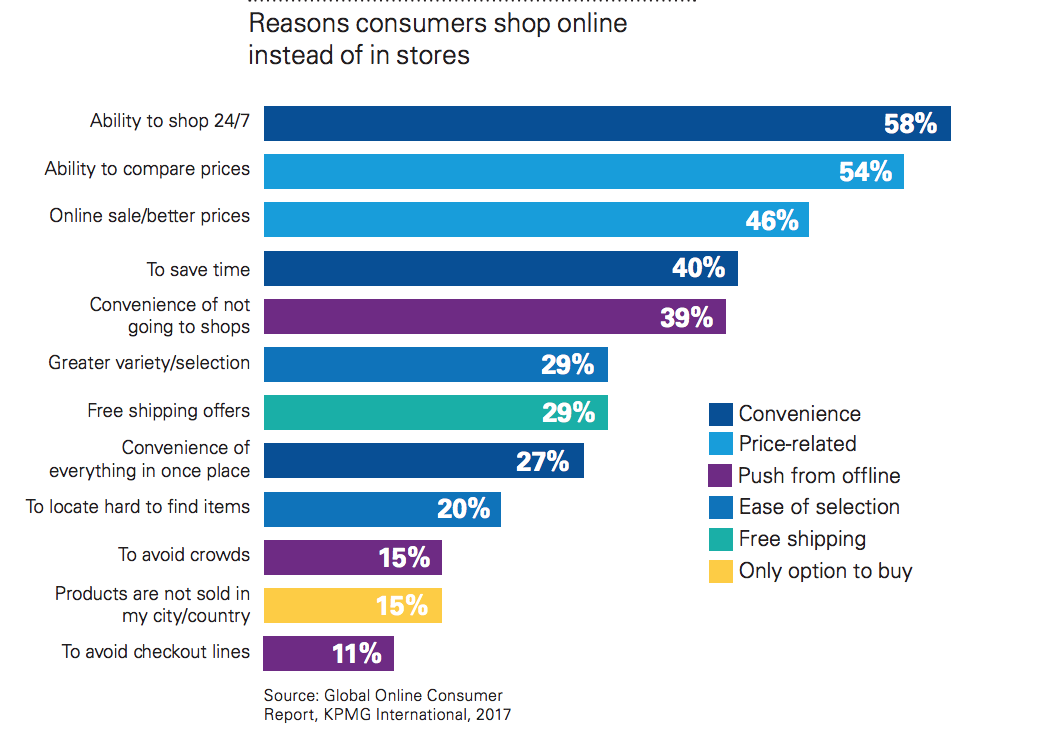
1. Convenience. This includes a lot of entertainment. Online stores are open around the clock. Buyers do not spend on gasoline. They save time and money.

2. Price comparison. Although online stores invest in the development of their software, they invest much less than physical stores. Therefore, purchases are higher, prices are lower.

3. The crowd. In online services, everyone will pay attention. No one will crowd and push.

4. Users can deliver a gift, product anywhere in the country, sitting at home.

This is a small part of comforts of using online stores.

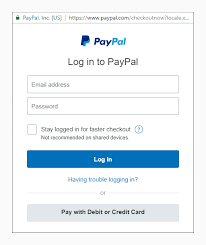


### Analytical analysis of existing systems on the market

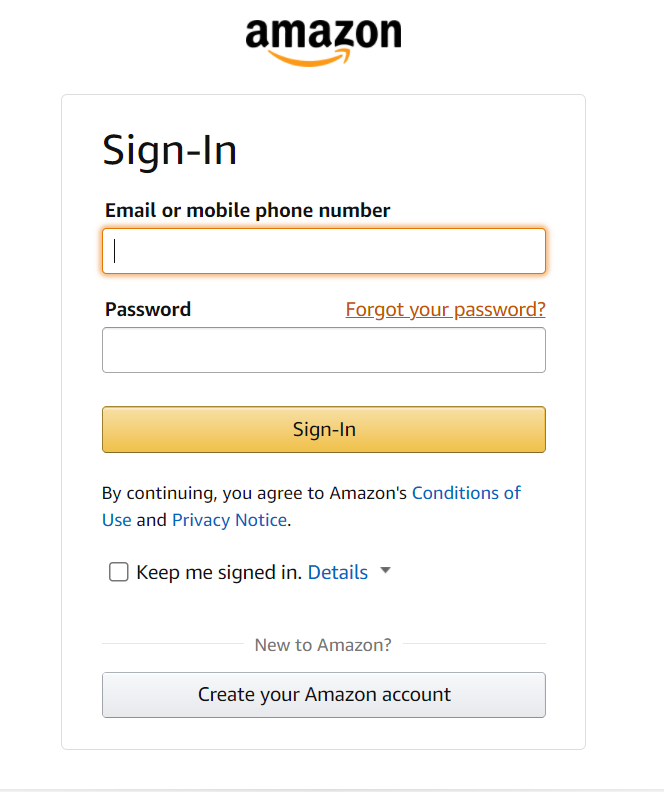
Most modern online payment services are simpler, faster and more secure. The most popular payment gateways or online payment systems are PayPal, Square, Stripe, Amazon Pay, Apple Pay, Authorize.net, etc.

List of some of the most popular online payment services:

PayPal is one of the most popular payment methods. This allows users to create a PayPal account where they can pay a fee for every cash transaction.



Amazon Pay is another popular online payment system. It is a digital payment processing service that allows customers to pay online using their Amazon payment methods on third-party websites. Amazon Pay uses data stored in your Amazon account to complete the transaction.



### Bank transfers

Customers do not always have a credit card, but they always have a bank account. The main advantage of bank transfers is that customers do not need to disclose any financial details to merchants in order to purchase goods or services.

All payment methods listed above have a high level of security

### Cybersecurity in online transaction

According to the 2016 Financial Industry Cybersecurity Reports, cybercrime is the second leading source of economic crime in global financial institutions (SecurityScoreboard, 2016).

According Ashfrod (2019) this includes fraud, large-scale break-ins, robberies.

In February 2016, Bangladesh's central bank was compromised by hackers who exploited vulnerabilities in SWIFT, the global financial system's main electronic payment messaging system. The attempt took place in the theft of 1 billion dollars. Fortunately, most transactions were blocked, however 101 million dollars still disappeared. For the financial world, this robbery was a disturbing blow and it became clear that systemic cyber risks in the financial system were grossly underestimated.

International Monetary Fund reveals, in consonance with papers compiled on cybersecurity risks by global organizations such as the International Monetary Fund, the Bank for International Settlements, the Economic Cooperation Organization, and the World Bank, the focus is generally on the broader framework of cybersecurity. The fact is that the types of cyberattacks multiply from day to day, so cyber security requires a wider study. No technical support promises 100% security, as with the development of the internet, virtual crime is also growing. Such an impact may negatively affect the financial performance of organizations that support online transactions.

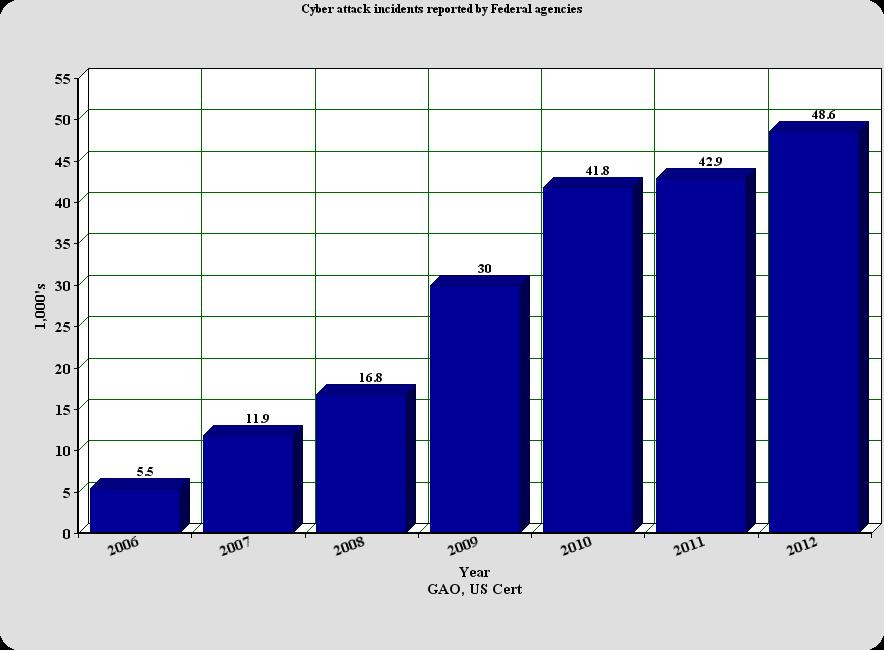


Eling & Lehmann (2018) also argue that the threat of cyberattacks is imminent. Even the best security systems need to be constantly updated and require a large investment to do so.

According to a new 2023 vedantu.com article, online transaction fraud can be divided into two types.

1. Risks like identity theft, viruses, and hacking come with data storage and transactions.

2. Risks of intellectual property and privacy threats, including the possibility of copying information by unauthorized online sellers, phishing using fake websites and misleading advertising messages.



Confirming to spot.uz, there are several factors that hinder the development of online stores in Uzbekistan. Under 'public trust' they describe the problems of online payments.

“The third problem is distrust on the part of the population. It is still unusual for us to pay online. For some it's scary, some don't know, and so on.  Low level of public confidence in online payments.'  - Shukhrat Kurbanov (CEO of GlobUz) and Nodira Gulyamova (founder of several online stores in the USA).

### Brief analysis of the regulatory framework for information security in Uzbekistan

Any CISO (eng. Chief Information Security Officer) - the head of the information security department, starting to work on organizing the work of the unit, developing an internal regulatory framework for information security, is puzzled by the question - what existing documents should be taken as a basis. In this article, we will try to briefly analyze the existing documents on this topic.

To streamline the types of regulations, we suggest using a conditional hierarchy. At the highest level, in terms of legislation, IS problems are mentioned in the Criminal Code, in chapter XX (1), it will not be superfluous to familiarize yourself with the document, but it is hardly applicable in practical work for CISO.

In practice, laws are at the highest level of the regulatory framework. From them one can draw a general view of the problem, some general definitions. Here are perhaps the main ones that mention information security:

• Law “On Informatization”. Articles 19 and 20 define the goals of protecting information systems, as well as the obligations of individuals and legal entities for their protection of such systems, which contain, among other things, confidential information.

• The Law “On Principles and Guarantees of Freedom of Information”. Here it is worth paying special attention to articles 11 to 15, which describe in sufficient detail what information and how (in the legal sense) is protected.

• The Law "On Telecommunications" is more about operators and providers, but many theses can be useful.

• Law “On Personal Data”, enters into force on October 1, 2019.

• Law on Cyber Security, effective date 17 July 2022.

• The Law “On the Protection of Information in the Automated Banking System”. Despite such an applied name, many theses can be used and adapted in the development of standards. The financial industry in general is almost always at the forefront of information security, in this case this is confirmed by the adoption of such a law, in which ABS security issues are highlighted separately.

At the end of 2017, a rather voluminous document was approved and at the beginning of 2018 appeared in the public domain, published by the Center for Information and Public Security (now SUE "Cyber Security Center") - "Requirements for ensuring information security of state and economic administration bodies, local government". The document aims to bring together the requirements of many standards, including the ISO 27000 series, into a single document, selecting the most important of them and providing them with more specific requirements and explanations. Those. the information security administrator in the state agency has a single document, the starting point of all work to ensure information security.

According to cybersecurity experts Kaspersky Security Network, Uzbekistan is subject to 8 percent of all Internet attacks affecting Central Asia, and 85 percent are in Kazakhstan. The state response to the insecurity of cyberspace as a result of cybercrime takes many forms, including important bilateral regional cooperation and multilateral cooperation through the SCO.

In 2005, Uzbekistan joined the Computer Security Incident Response Team (CERT), an international information security system that currently includes 27 countries. CERT members work together to develop technical recommendations and legislative initiatives, identify attacks on information infrastructure, and promote the exchange of expert knowledge.

According to Sputnik.Uz research, 71% of cyberattacks are financially motivated (followed by intellectual property theft and then espionage)

Law "On Cybersecurity"

April 15, 2022 President of the Republic of Uzbekistan Mirziyoyev Sh.M. signed the Cyber Security Law, which will come into force on July 17, 2022 (hereinafter referred to as the Law) The adoption of the Law is of strategic importance in the fight against cybercrime and, of course, it is not surprising that the authorized body, in accordance with Article Law, the "elite" of the law enforcement system was appointed - the State Security Service of the Republic of Uzbekistan.

The following positive aspects of the Law are clearly articulated principles, namely:

• legality;

• priority of protecting the interests of the individual, society and the state in cyberspace;

• a unified approach to regulating the sphere of cybersecurity;

• priority for the participation of domestic manufacturers in the creation of a cybersecurity system;

• openness of the Republic of Uzbekistan to international cooperation in ensuring cybersecurity.

President Shavkat Mirziyoyev at a meeting on April 14, 2022 announced the need to turn Uzbekistan into a regional IT center. The Development Strategy of New Uzbekistan for 2022-2026 sets a goal to increase the volume of IT services by 2.5 times and the export of the industry to $500 million, the President instructed to increase the volume of domestic IT services by 50% by the end of this year and bring exports to 100 million dollars.

Since the beginning of the year, a huge number of IT specialists and companies, including international ones, have been relocated to Uzbekistan. Uzbekistan attracts the attention of big players and the only reason why they are not here yet is the lack of clear, transparent and understandable rules for them. Corporations like Google, Amazon, Facebook are accustomed to operating in jurisdictions with English law or where it is recognized.

The current legislation of Uzbekistan does not provide corporations with the opportunity to use the legal structures and mechanisms that they widely use in other countries. Therefore, in order to attract such companies, some countries, such as the UAE, Kazakhstan, have begun to create territories with a special legal regime and a regulatory "sandbox", and this has begun to bear fruit. Taking into account the large-scale work done by the President over the past six years, Uzbekistan has every chance to become not just a regional IT hub, but an international one, adopting the successful experience of other countries.

However, the adoption of Laws such as “On Cyber Security” can drastically slow down the inflow of investments, large players who study the country and its laws in detail before entering the market will not make a decision in favor of Uzbekistan.

If the state wants to continue development in the direction in which it has been determined, then it is necessary to make appropriate changes to the Law “On Cybersecurity”, taking into account the opinion and interests of the business community, which should also be more often involved in the development of such regulatory legal acts.

### Brief Overview

This includes distrust of people due to bad experiences in the past, negative feedback from word of mouth, distrust of new unknown technologies, preference for the traditional physical payment method.

It is also said that it is impossible to get rid of the threats of cyber-attacks completely. With the development of the Internet, types of attacks are also developing.

Storing personal data can increase the risk of hacker theft and damage to the website from viruses and hacking. Two specific risks are mainly discussed: viruses that delete data and hacks that steal personal information. Online shopping websites can also be affected, resulting in damage and loss of time. Therefore, incorporating cybersecurity measures is extremely important for both buyers and online stores.

Under all studies carried out for the project and statistics, it is important to invest in the development, updating and implementation of cybersecurity in online payment systems.

### Observation

Indeed, online shopping is becoming commonplace. If earlier the adult generation was skeptical about online shopping, now the number of customers among them is increasing. People see beautiful videos, pictures of products with a profitable price on social networks and immediately click on the order button. A few successful purchases motivate people to make more purchases. Therefore, this industry is sure to develop all over the world, with many amenities for people.

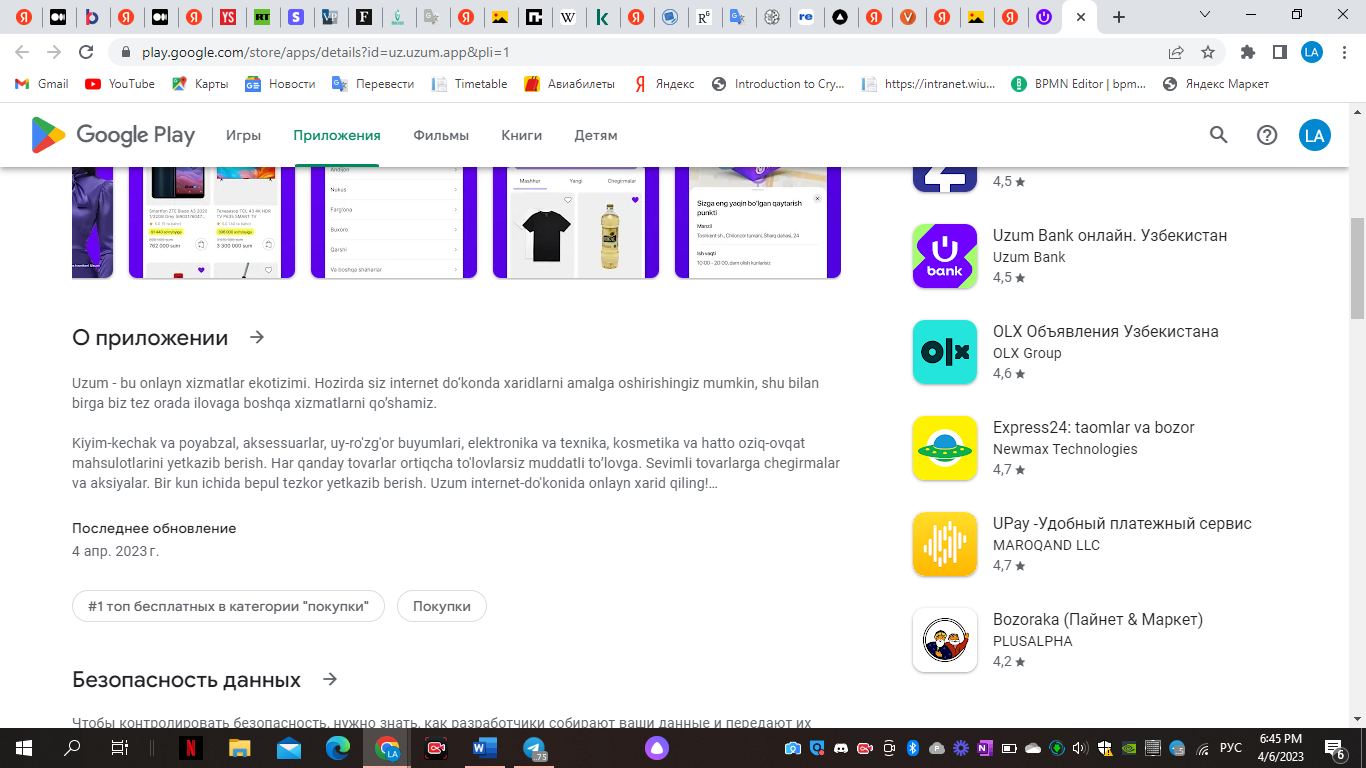
But there are also some downsides to online shopping. This is trusting them with personal information about cards and bank accounts.

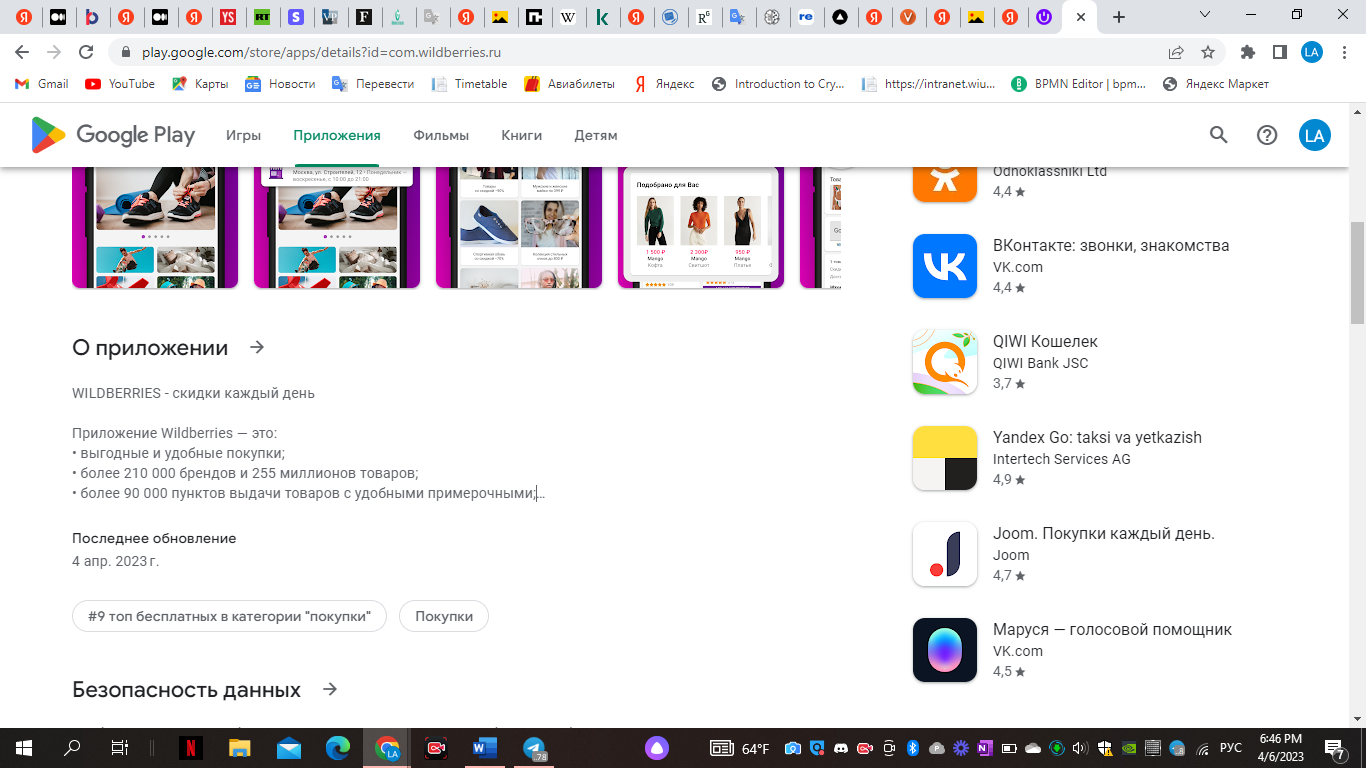
In keeping with many reports, online transactions are still a problem for both organizations and the public.

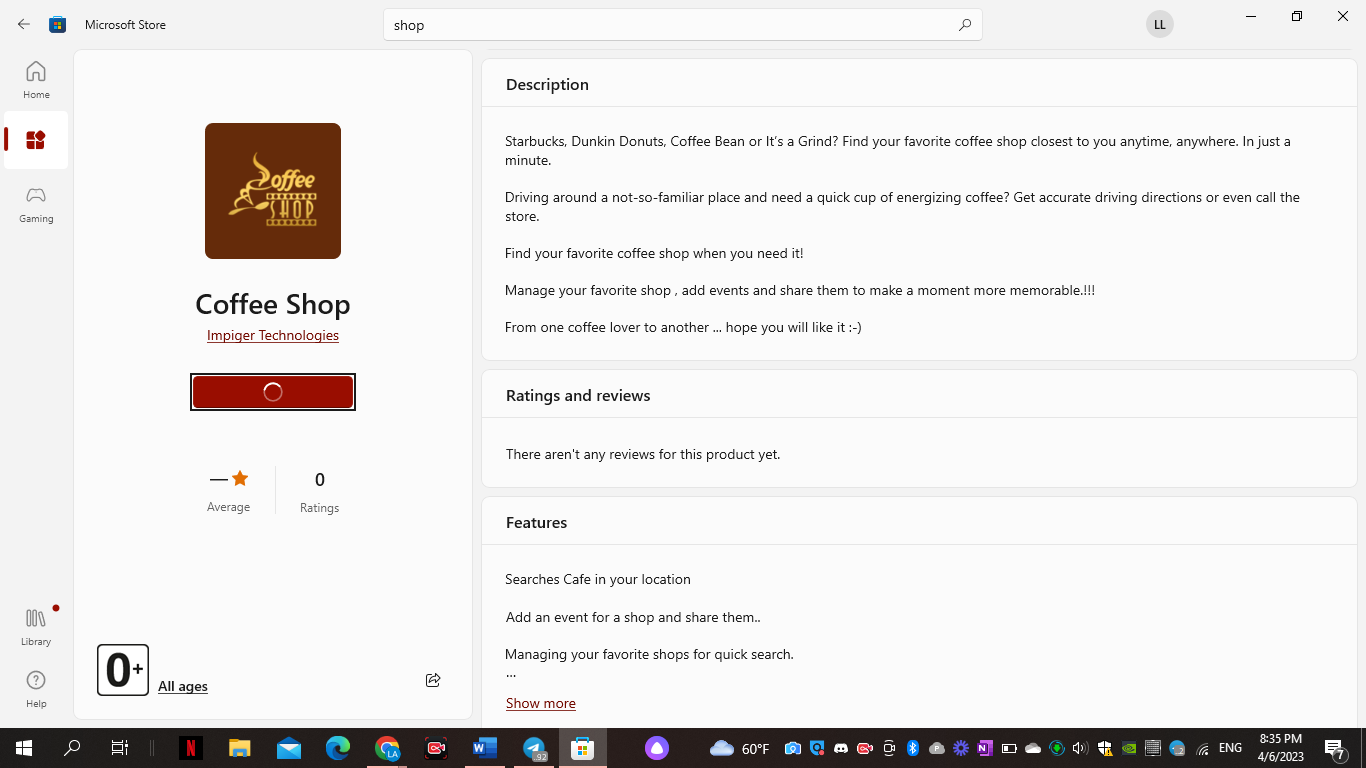
According to the facts and research carried out for this project, online payments are becoming an integral part of people's lives. General public can't get far with the traditional physical method. People have a need to pay, to transfer money from one end of the earth to another in a matter of seconds. The reason may be different situations. Paying for online courses, transferring finances to relatives, a new purchase and many other options. People still have to use online transactions.

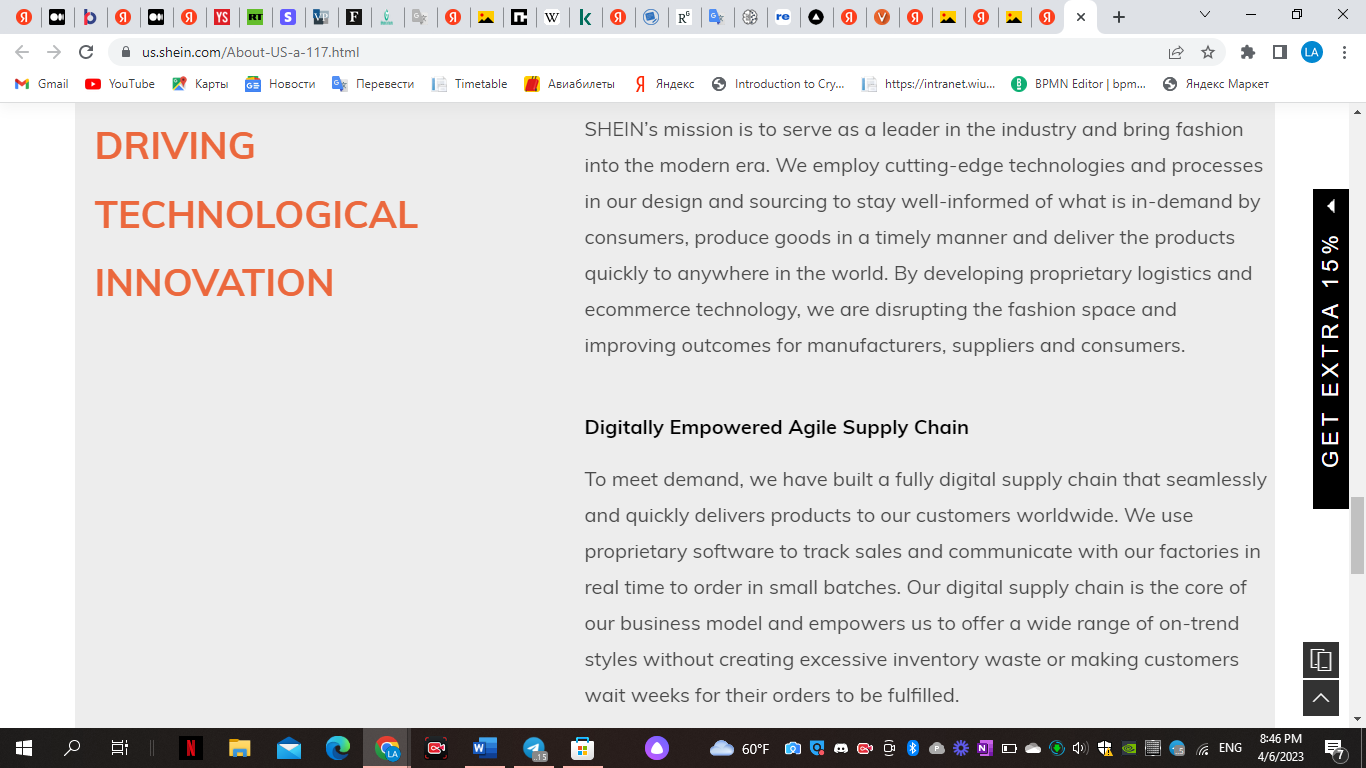
But they can be very vulnerable. Especially on sites, where store keep personal information about buyers. I recently witnessed a conversation on this topic. The guys expressed their dissatisfaction with how many applications of fast food restaurants and other establishments store information about their card in their database. This causes constant anxiety among users. With their thoughts, they think, are their finances safe on the card?, no one will steal their money from the card?, how safe are these sites?

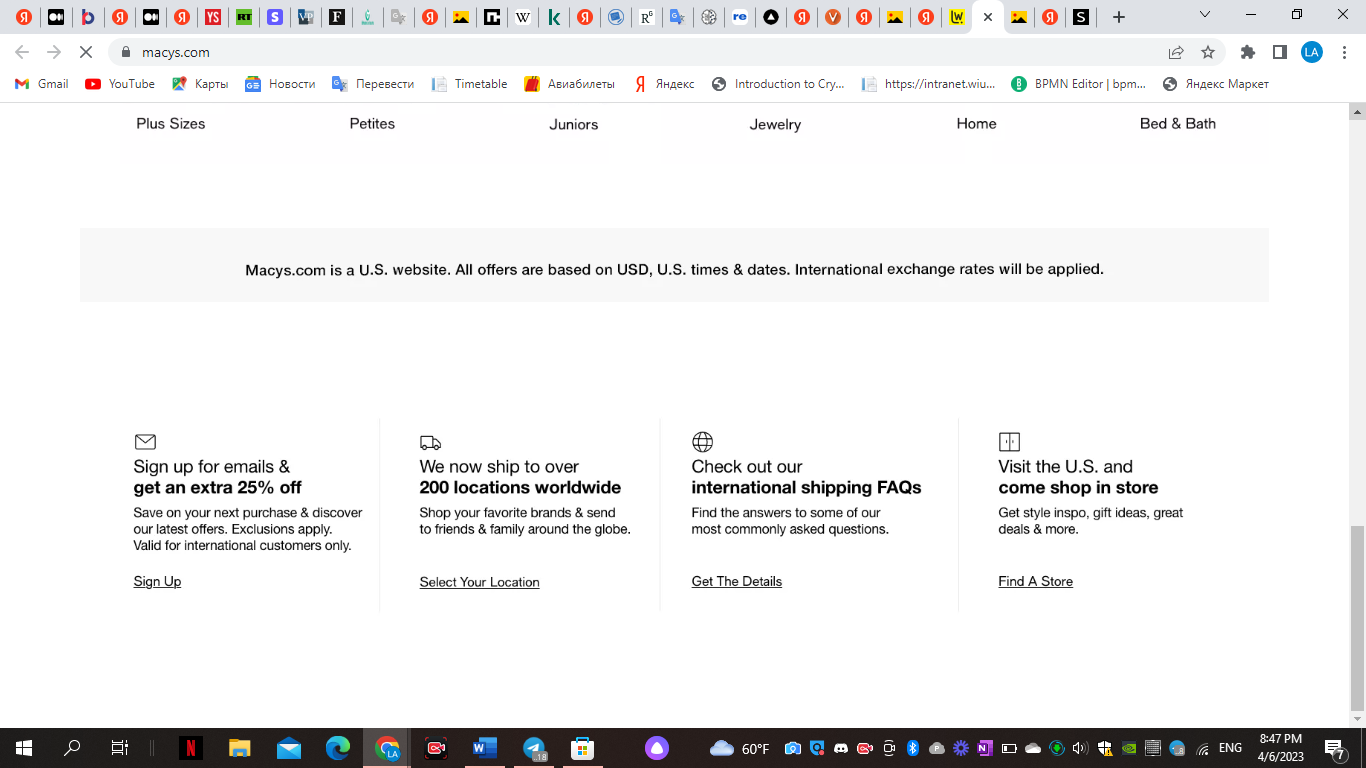
Many online stores are only busy advertising their other services. They do not emphasize to users how secure their payment system is, which is an integral part of online shopping. In the description, they attach more importance to the quality of their products, assortment, price, logistics, coupons. Here are some examples:











Therefore, it is extremely important to inform users about how secure the site or application of stores is during online payments. This will help to imbue even greater confidence in the quality, safety, and innovativeness of stores. In addition, it will save store websites from negative spam and other pests, viruses, scammers.

### Solution

This thesis project proposes a solution to this problem. With the development of the Internet, online stores, cyberattacks, developers should not abandon the constant development of cybersecurity systems. I present a cyber security system against cyberattacks during online payments. The system mainly focuses on protecting the personal information of customers on the payment pages of online stores from four popular types of fraud. They are SQL attacks, Proxy - Servers, Spams, Bad Bots.

In the future, it is planned to develop in website new types of protection against other types of fraud.

# SWOT analysis

## Strengths

In order to improve cyber security measures and protect buyers' sensitive information during online transactions, the project meets the urgent needs of the e-commerce industry.

Detection of fraudulent activities in online payments can be achieved using advanced algorithms and information technology techniques to improve the security of online shopping.

By instilling more trust and peace of mind in payment systems, this project will improve the online customer experience.

Ensuring strong growth in cybersecurity at the expense of the system in the country and beyond. This increases the level of trust among users, helps the development of small businesses through innovative implementation, positively affects the country's economy through bold purchases and the development of small businesses.

## Flaws

Small businesses may find it difficult to enter the market due to financial investments.

Regular updates and improvements are needed to keep up with the ever-changing tactics of cybercriminals despite the reliability of the system.

The website provides protection against the four most popular online scams and is focused on protecting against these scams only.

And there are many ways to cheat. Therefore, website should have to be update with each new type of fraud.

## Possibilities

Improving the security of online transactions through the project can attract more customers to online shopping.

The need for safer online shopping has created a favorable market for this type of system.

In addition to e-commerce, banking and finance, as well as other industries that depend on online transactions, can use an adaptable system.

The project can serve as a start-up and attract investors and lucrative contracts.

## Threats

The collection and storage of personal data by the system may lead to legal and ethical complications.

There may already be companies on the market offering similar platforms that can compete with the system.

Consumer knowledge can determine the success of a project in terms of cyber security and secure online shopping.

The future of the website also depends on the feedback of users. Many users may think that there are no threats in online transactions, that all payments are secure. Therefore, ignoring them at the expense of an uninformed service can lead to a lack of necessary reviews.

# Porter's Five Forces

Buyers (customers)

Representatives of online stores.

Representatives of online stores that will implement this project in their online store can act as clients.

The bargaining power of buyers is high as there are many websites offering similar services. Customers have a wide range of options, which puts pressure on pricing and customer experience. But still, many beginner online stores do not think about cybersecurity during online payments in the very first place. That is why project should be tried to be the first to offer them this service. Therefore, the level of customer search is average.

Users of online shops.

Also, buyers of online stores can remain regular customers of online stores because of their security system. This is also a dependent factor. But as a special role does not directly affect into the implementation of the project. Rather, project will improve the relationship between online stores and their customers.

If the relationship between this project and online stores is directly dependent on each other, then the decision of buyers is influenced not only by the security system during online transactions, but also by the product of online shop itself, its quality, price, delivery and other factors, which are not dependent on this security system.

And the server will primarily be used by representatives of online stores. Therefore, the dependence on the customers of the shops of the project payment system is not high.

However, the demand of the general public for high cybersecurity in online stores influences the decisions of representatives of online stores to implement security systems in their payment systems. Demand creates supply. This motivates online stores to use the development of a system for detecting fraudulent activities in online payments website service.

## Suppliers

The bargaining power of the providers on this website is relatively low as the main content is produced in-house. However, if some third-party software is required to operate the website, then the vendors' bargaining power in this regard can be high.

The suppliers of this product are comprehensive applications, software, hardware, frameworks, websites with which this cybersecurity system was created.

The development environment was the well-known giant of its field Visual Studio Code. An environment for experienced developers with a convenient set of functionalities, which in addition allows its users to add third-party plugins. Plus, Visual Studio Code is free to use.

The importance of this development environment is essential to the functioning of the website.

In its turn, MySQL has been chosen as the database manager.

MySQL is still the most popular database management system in the Internet giants. There are a huge number of examples from well-known companies and popular Internet services: Facebook, Github, Wikipedia, Google, Youtube, LiveJournal, PayPal, Twitter, Booking.com, AirBnB, DropBox, Uber, LinkedIn, Alibaba.

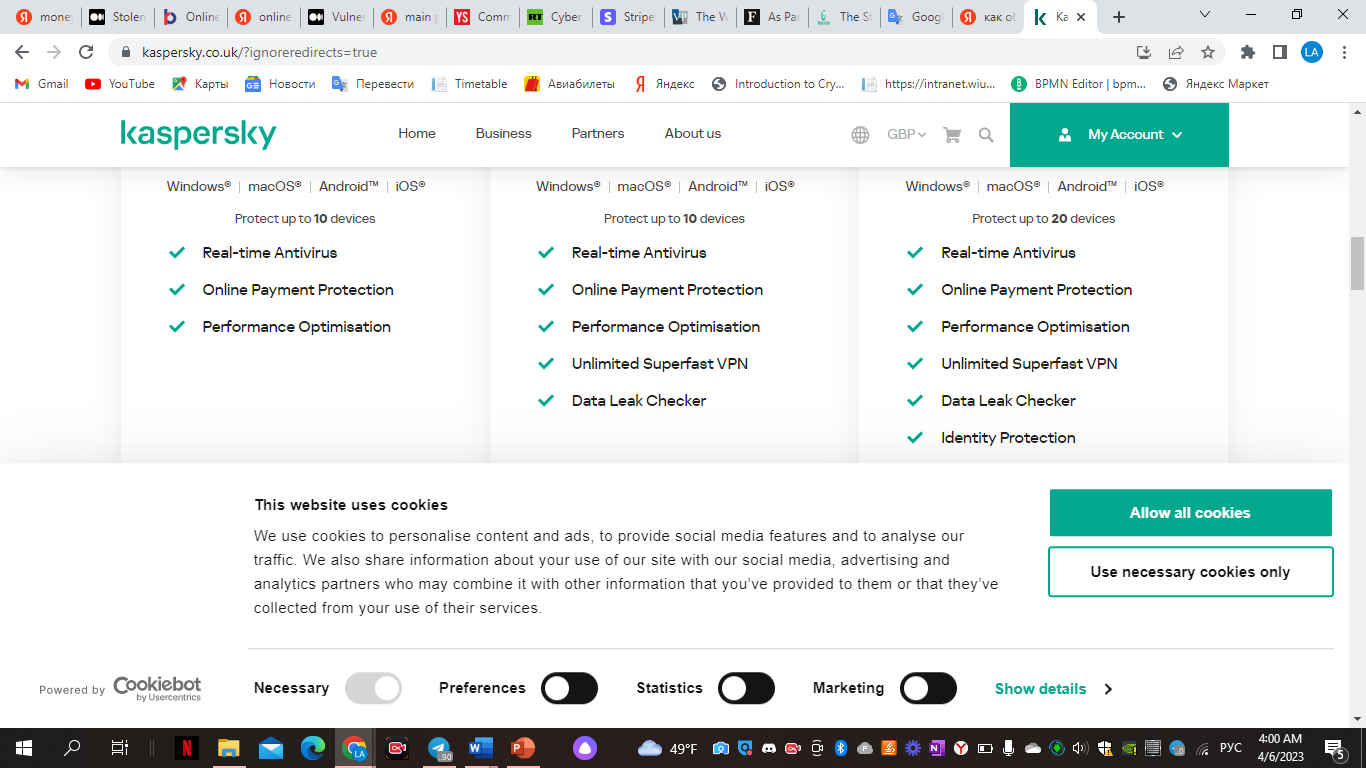
In the world of business development, database management systems are changed only when there is a very great need, and therefore rarely anyone has already come across this feature in practice. But replacing MySQL with other systems is possible. It is more difficult if the database is overloaded. Therefore, the level of dependence here is medium.

In the future, suppliers will include technology vendors providing updated cybersecurity solutions, as well as a team of web developers and website designers who will update the project. The help of marketeer is also required, as the project is looking for clients in a narrow circle, namely applications with online transactions with vulnerable weak or no cyber security, which will be offered the service of introducing a new system.

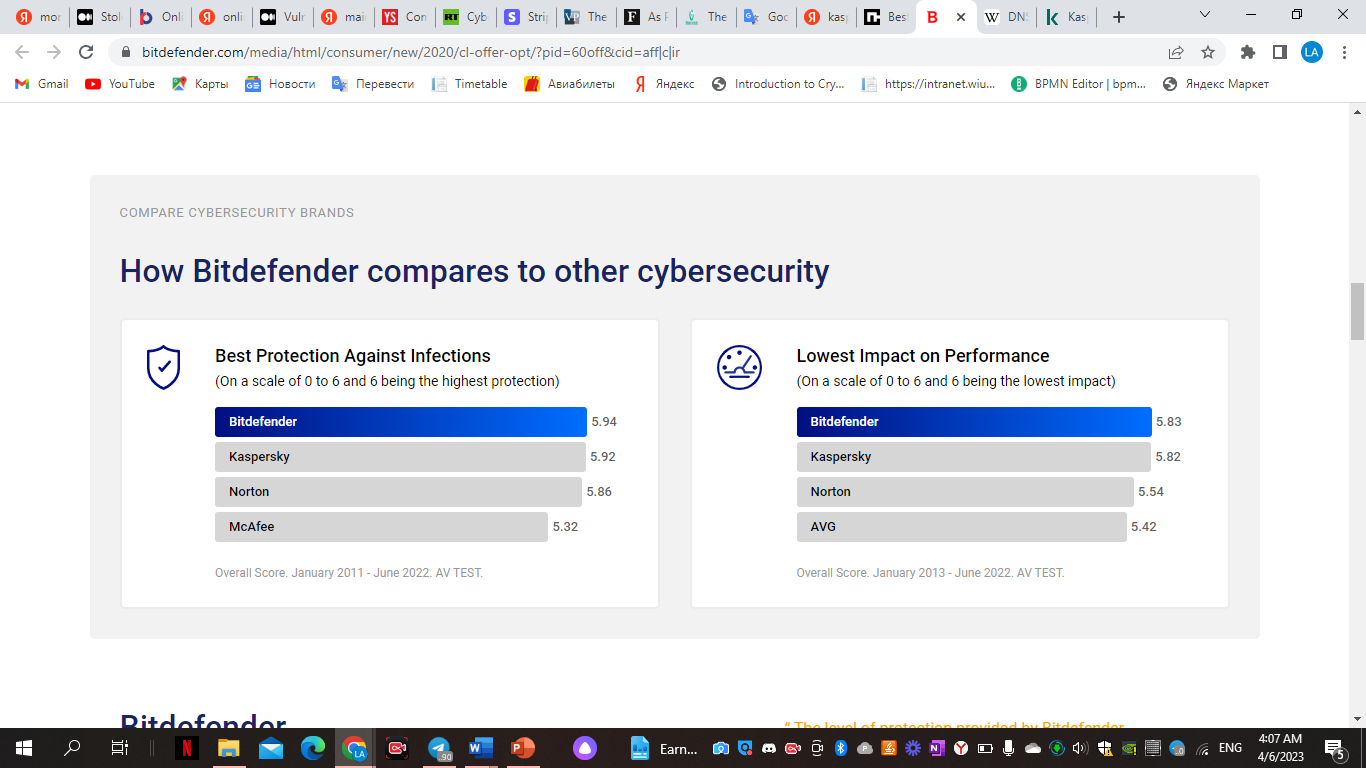
## Current competitors

The competition for this site is high. There are several companies that offer similar services and they are all competing for the same target audience. This makes it difficult for this website to differentiate itself and stand out in the market.

One of the main competitors is Kaspersky (https://www.kaspersky.co.uk/) which is a feature rich website that promises cyber security against many kinds of threats. Their statistics for the year show that they have eliminated 687 million cyberattacks\*, achieved blocking of 114 million unique malicious URLs\* and neutralization of 64 million unique malicious objects\*.



From 2021 to 2022, Bitdefender has become the leader in cybersecurity. It offers additional features besides safe online banking. These are anti-phishing projection, safety from all new and existing threats, fast, anonymous and secure while surfing the web.



In turn, our website only offers cyber security features during online transactions, protecting customer data from the 4 most dangerous types of fraud. In the future, it is planned to introduce the fight against other types of fraud.

## New competitors

The market is always at the risk of new competition. The industry's saturation makes it challenging to establish oneself in the market at present.

New competitors may include startups or small online stores with innovative cybersecurity solutions or unique value propositions.

It will be more difficult if a number of new online stores implement their security systems already during the development of their applications.

## Substitute products

Other options could be utilizing different payment methods or exploring comparable products or services through a physical store.  
  
This website faces a serious threat from substitute products. The website risks becoming outdated if a new technology or platform with similar features emerges. To address the threat of substitute products, a website's innovation and adaptation to new technologies is paramount.

# PESTL Analysis

## Political factors

• E-commerce transactions regulation is a critical task that is performed by governments, which can affect the way online payment fraud detection systems are designed and implemented.

• The level of awareness and investment by governments in cybersecurity measures can affect the success of these systems.

• Data protection and privacy laws can influence functionality and feasibility of the systems as they vary across different legal frameworks and countries.

• Reviewing the tax laws, trade agreements, consumer protection laws, data privacy laws, and cybersecurity laws of operating countries is crucial. An e-commerce business is susceptible to political factors that can technically either create opportunities or pose a threat.

## Economic forces

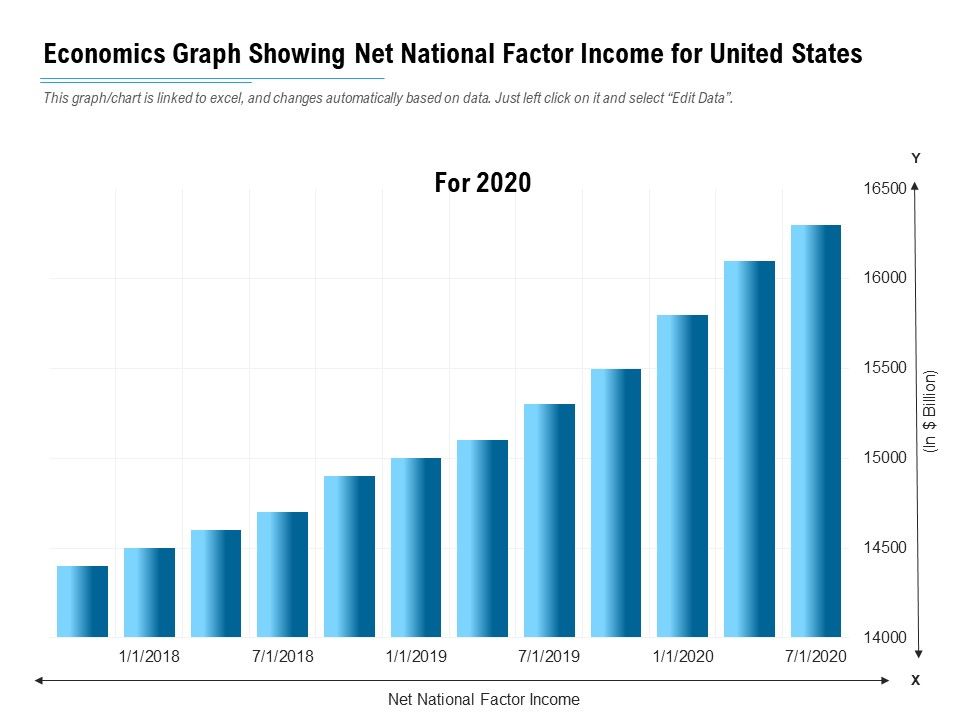
• E-commerce expansion worldwide escalates the probability of deceitful actions that may result in major financial losses for businesses and customers.

• Implementing an online payment fraud detection system can be expensive and vary based on organization size and complexity.

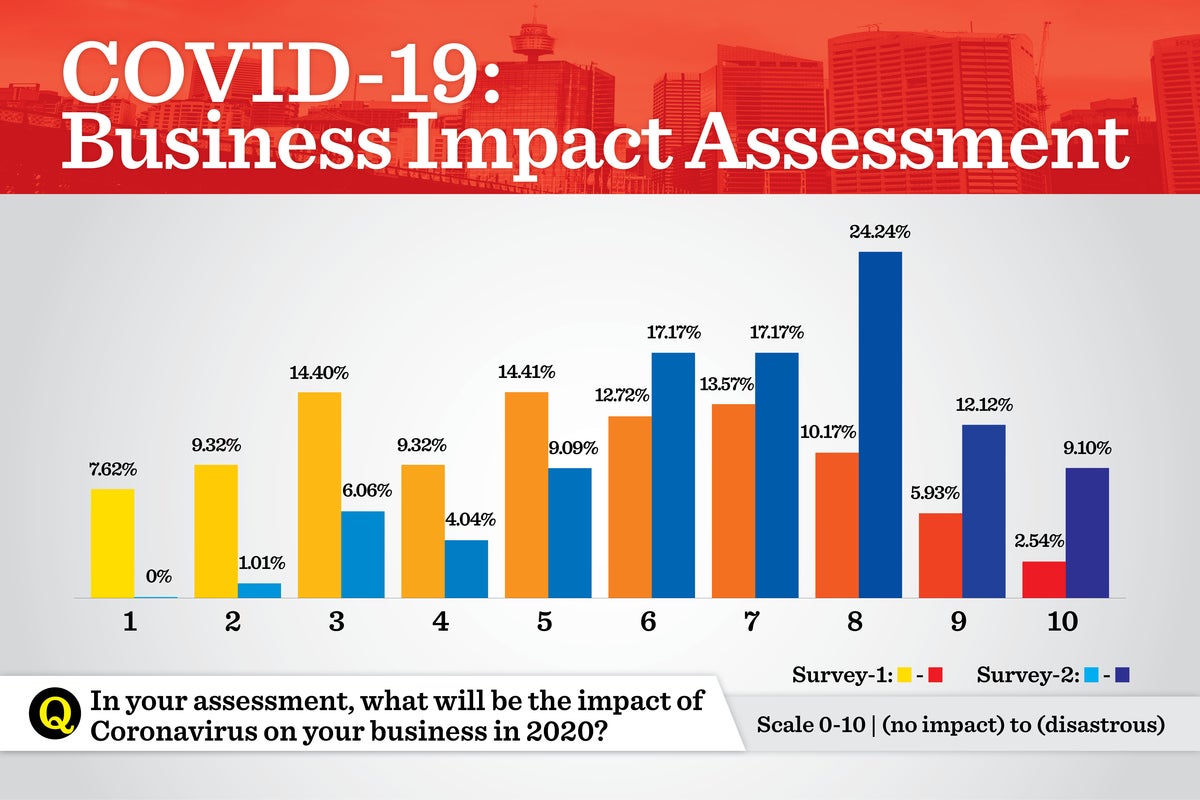
• A cybersecurity system can improve the level of demand among the population of the country, which will encourage users of online stores to confidently make more purchases online. The development of small business in countries leads to the development of the country's economy.  In this case, online stores also belong to small businesses, which are gradually expanding.

• Entering the global market. The biggest advantage of online payments is that entrepreneurs will be able to organize their business worldwide and receive payments easily. Electronic payment method allows to accept payments from anywhere in the world.  Most people want to try something new and prefer the best choice, so shopping abroad is on the rise. Thus, digital payments allow to make transactions both within the country and abroad. People can expand their business around the world and make an online transaction.

Statistics on how well online stores affect the country's (USA) economy:



[Impact of Coronavirus (COVID-19) on eCommerce Businesses by Nick Loggie Medium](https://medium.com/@logz05/impact-of-coronavirus-covid-19-on-ecommerce-businesses-fae2082db9ee?source=post_internal_links---------3----------------------------)



The impact of online transactions on the country's economy

## Social factors

Social factors take into account all the characteristics of the population, such as age, gender, nation, interests, lifestyle, problems and solutions. People have desires, expectations, needs. Businesses, in turn, should comply with them in order to provide the best offer for the demand of their customers.

• Online transactions are increasingly integral to consumers, hence trust in payment systems is pivotal in the triumph of e-commerce.

• A secure payment system may increase consumers' tendency to shop online.

• The reliability factor could significantly impact the future of e-commerce.

• The pandemic has a positive effect on the loyalty of customers who have learned online shopping and online payments, and now their number is only growing.

• Reduced transaction costs.

Previously, shoppers had to visit the store with a sufficient amount of cash or use receipts to purchase groceries.  But today, digital payments save customers time and effort. They can shop online and even pay electronically. The online payment process reduces the transaction cost of the traditional payment method.  People don't need to hire staff, especially as a cashier and payroll processing costs.

There is usually no or very small charge for card swiping or online payment.  In the long term, electronic payments can save both individuals and businesses transaction fees.

## Technological factors

• Artificial intelligence and machine learning algorithms can help detect fraudulent activity in online payments.

• Constant innovation is needed to develop countermeasures that can effectively combat the increasingly sophisticated attacks by cybercriminals.

• The penetration of the Internet, mobile devices, social networks, cloud computing, artificial intelligence, blockchain and online payment systems in the specific industry and market where the cybersecurity website will be maintained should be considered.

## Legal factors

• Following cybersecurity guidelines is imperative for businesses to avoid legal recourse and financial repercussions.

• The presence of legal regulations concerning e-commerce transactions could influence the effectiveness and functionality of systems designed to prevent online payment fraud.

• Leakage of banking information or theft of buyers' money by fraudsters can also cause major legal damage.

• Strong intellectual property rights can provide competitive advantage and innovation, and patent infringement can lead to legal action and fines.

## Environmental factors

• Energy consumption, carbon footprint, waste management, recycling and sustainability of e-commerce activities need to be considered.

# Monetization

Having studied all the methods of monetization on the Internet, one thing is clear. Many standard methods of monetization do not fit the security system in online payments.

This website is not an informative, entertaining blog, so using ads to monetize this website is not the best way to go. This will only repel users in such a serious category of purchase.

The website is commercial. It is worth monetizing his services.

In fact, the right approach to monetization will bring good profits for cybersecurity systems.

For example, Microsoft, which last year released the OneCare universal anti-virus package and has already captured 15% of the US market in six months of online sales.

As practice shows, it is very difficult to convince the manager to spend money on something that he does not need now. It should also be remembered that IT budgets in the CIS companies are extremely low (compared to Western ones) and tend to be further reduced. Usually, information security becomes part of the information technology budget, respectively, this item of expenditure for the first persons is not a priority.

In addition, cybersecurity risks, even if they are beautifully described and calculated, are not significant for company leaders, that is, everyone always thinks that such problems will never affect them.

How to sell website services correctly?

First, find a problem (what to sell)

To begin with, it should be clearly understood what we want to spend the organization's money on. It is necessary to identify the existing problem and formulate it in terms understandable at the household level. It is a certain problem and subsequently the proposed technical solution that will become the main point in making a decision. In this case, the leakage of consumer information is a threat and a problem for representatives of online stores.

Next, need to find the owner of the problem, who is experiencing this and offer a solution.

## Subscription monetization

Project product is SaaS (Software as a Service). SaaS is a software subscription license. This is how Figma, Slack and Dropbox work.

Subscription apps earn 2-3 times more per user compared to products that use an advertising monetization model.

Subscribing to SaaS products reduces user risk. For example, Microsoft Word used to have to be purchased once and forever. It was an expensive purchase. Now people can use it for a monthly fee - this way users feel less obligations and make it easier to decide on a deal.

How does it work?

The system will offer monthly subscriptions to IT representatives of online stores. In the future, they can install several types of subscriptions, such as Premium, Pro, and so on. More expensive subscriptions will offer cyber security services against the largest type of cyberattacks.

Monthly fees will be charged for services from online stores, for which the website will provide cyber security during monetary transactions.

# Methodology computing

## Creation of a fraud detection system for online payments and its implementation

Rationale for choosing a programming language

When developing a fraud detection system in online payments, it is designed using the following programming languages:

• PHP

• Apache

• HTML, CSS, JS

• Open Server

• MySQL

PHP is an open source server-side scripting language that many developers use for web development. It is also a general-purpose language that developers can use to create many projects, including graphical user interfaces (GUIs). The first version of PHP was launched 26 years ago. This is now version 8, released in November 2020, but version 7 remains the most widely used. PHP runs on the Zend engine, which is the most popular implementation. There are other implementations like parrot, HPVM (Hip Hop Virtual Machine) and hip hop created by Facebook.

PHP is mainly used to create web servers. It works in the browser and can also work on the command line.

Why was PHP chosen to develop this system?

PHP has some of the advantages that have made it so popular and has been the go-to language for web servers for over 15 years now. Here are some of the benefits of PHP:

• Cross-platform: PHP is platform independent. Developers don't need to have a specific OS to use it because it runs on any platform, be it Mac, Windows or Linux. A Mac was used to develop this system.

• PHP is open source. The source code is available to anyone who wants to use it. This is one of the reasons why one of its frameworks, Laravel, is so popular.

• Easy to learn: PHP is not difficult to learn for beginners. Since there was no deep study of this language in the WIUT curriculum, it was easy to master the basics of the language on my own.

• PHP is synchronized with all databases: it is easy to connect to all databases, relational and non-relational. So, it can instantly connect to MySQL, Postgress, MongoDB or any other database. This project uses MySQL.

• Supportive Community: PHP has a very supportive online community. The official documentation contains guides on how to use the functions and users can easily solve problem if it gets stuck.

Apache

Giovana Hernandez of SUMO Logic security analytics platform says in her report that Apache is the most widely used web server software and powers 67% of all websites in the world. Developed and maintained by the Apache Software Foundation, Apache is open source software and is available for free.

In addition, Apache can be customized to suit the needs of different environments using extensions and modules.

Many WordPress hosting providers use Apache.

So, a web server like Apache does a lot of things:

• It receives a user request to access a web page.

• It performs several security checks on the user's HTTP request and translates it into a web page.

• It can ask the server to run additional modules when creating a document for the user.

• It then serves the requested document to the user.

• Starting the Apache web server on the user's computer.

If a user wants to run WordPress locally on their computer, they will need to run the same software as the user's WordPress hosting provider. This includes Apache (web server software), MySQL (database), and PHP (programming language).

HTML, CSS and Javascript

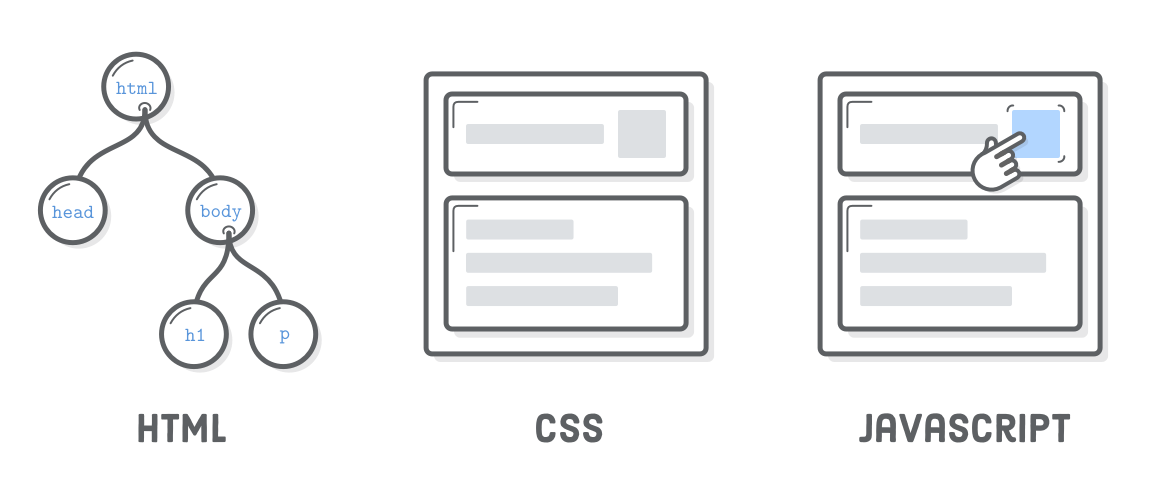
Hyper Text Markup Language (HTML), Cascading Style Sheets (CSS), and JavaScript are the languages ​​that run the web. They are very closely related, but they are also designed for very specific tasks.

For the project, HTML was used to add meaning to the raw content by marking it up.

CSS was used to format the marked-up content.

JavaScript was used to make this content and formatting interactive.

Here is how these three programming languages ​​are closely related to each other (which was dedicated to CIFS semester 2 on BIS)



*Source fiverr.com*

Database management system

The Oracle-supported MySQL system was used as the database management system.

MySQL is an important component of the open source enterprise stack called LAMP. LAMP is a web development platform using Linux as an operating system, Apache as a web server, MySQL as a relational database management system, and PHP as an object-oriented scripting language. A diagram of how the project was developed.

## Creation of the user interface of the system. Types of user interfaces and stages of their creation

The user interface (UI) is the point at which people interact with a computer, website, or application. The goal of an effective system user interface is to make the user's work simple and intuitive, requiring the minimum effort from the user to obtain the maximum desired result.

The user interface is created at interaction levels that appeal to the human senses (sight, touch, hearing, etc.). They include both input devices such as a keyboard, mouse, trackpad, microphone, touch screen, fingerprint scanner, electronic pen, and camera, as well as output devices such as monitors, speakers, and printers. Devices that interact with multiple senses are called "multimedia user interfaces". For example, everyday user interface uses a combination of tactile input (keyboard and mouse) and visual and auditory output (monitor and speakers).

Other types of user interfaces may include:

• Form-based user interface: used to enter data into a program or application, offering a limited selection of options. For example, the settings menu on a device is form-based.

• Graphical user interface: tactile user interface input with visual user interface output (keyboard and monitor).

• Menu-based user interface: A user interface that uses a list of options to navigate through a program or website. For example, ATMs use a menu-based user interface and are easy to use for everyone.

• Touch User Interface: User interface via tactile or touch. Most smartphones, tablets, and any touch screen devices use tactile input.

• Voice user interface: interaction between people and machines using sound commands. Examples include virtual assistant devices, voice control, GPS, and more.

The user interface is important in order to meet user expectations and maintain effective site functionality. A well-executed user interface promotes effective interaction between the user and a program, application, or machine through high-contrast visuals, clean design, and responsiveness. When designing the user interface for this site, it was important to consider the user's expectations in terms of accessibility, visual aesthetics, and ease of use. The optimal combination of effective visuals and effective response to increase the site's conversion rate as it anticipates user needs and then satisfies those needs.

The components of the IA system include three main types of organizational structures: hierarchical (level of importance), sequential (logical order of steps) and matrix (in which the user chooses the organization of the content that he sees).

On a site, these are navigation elements (buttons, tabs, icons), labels (terminology), search functions (search bar), and organization systems (categories).

Interactive design.

Identity elements are designed to turn passive readers into active participants by presenting examples of user input. Keeping the user in mind when creating the user interface will help improve interactivity and perform certain actions that satisfy the user's needs.

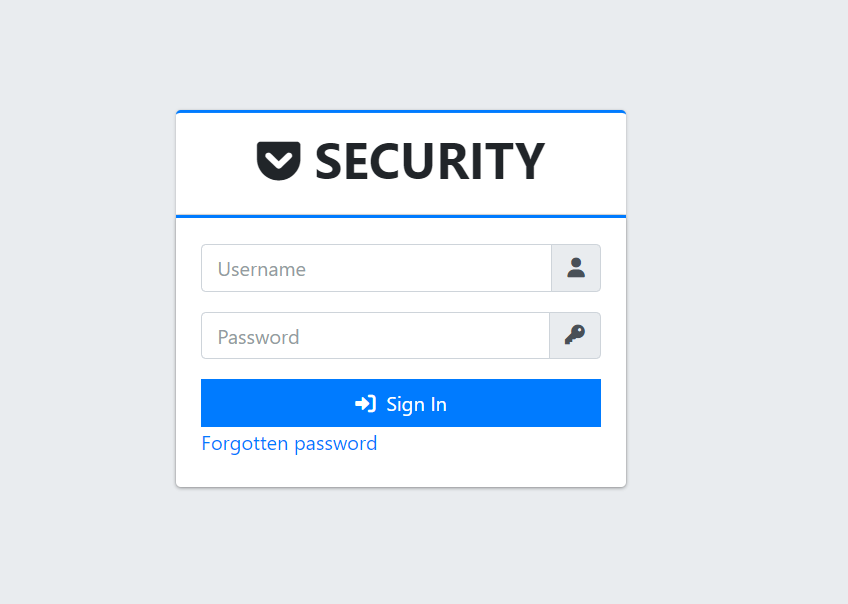
Visual design.

The importance of the aesthetic value of a site cannot be underestimated. Effective design uses color, contrast, font, video and photo elements to engage visitors and make it easier for them to read and interact with content rather than around it to create a logical, intuitive flow of features.

This system uses the right contrast, color, white space, typography, mobile optimization by studying the psychology of users of the most popular payment systems sites that have long built trust with their users. It was also taking into account modern trends in colors, website architecture and much more that make up the visual image.

## System implementation

In order to log in, users will need to enter their username and password for their account. This process is shown in figure below.



Login

Next figure shows the main page of the site, as well as the menu on the left side. The menu includes:

1. Site panel;

2. Site Information;

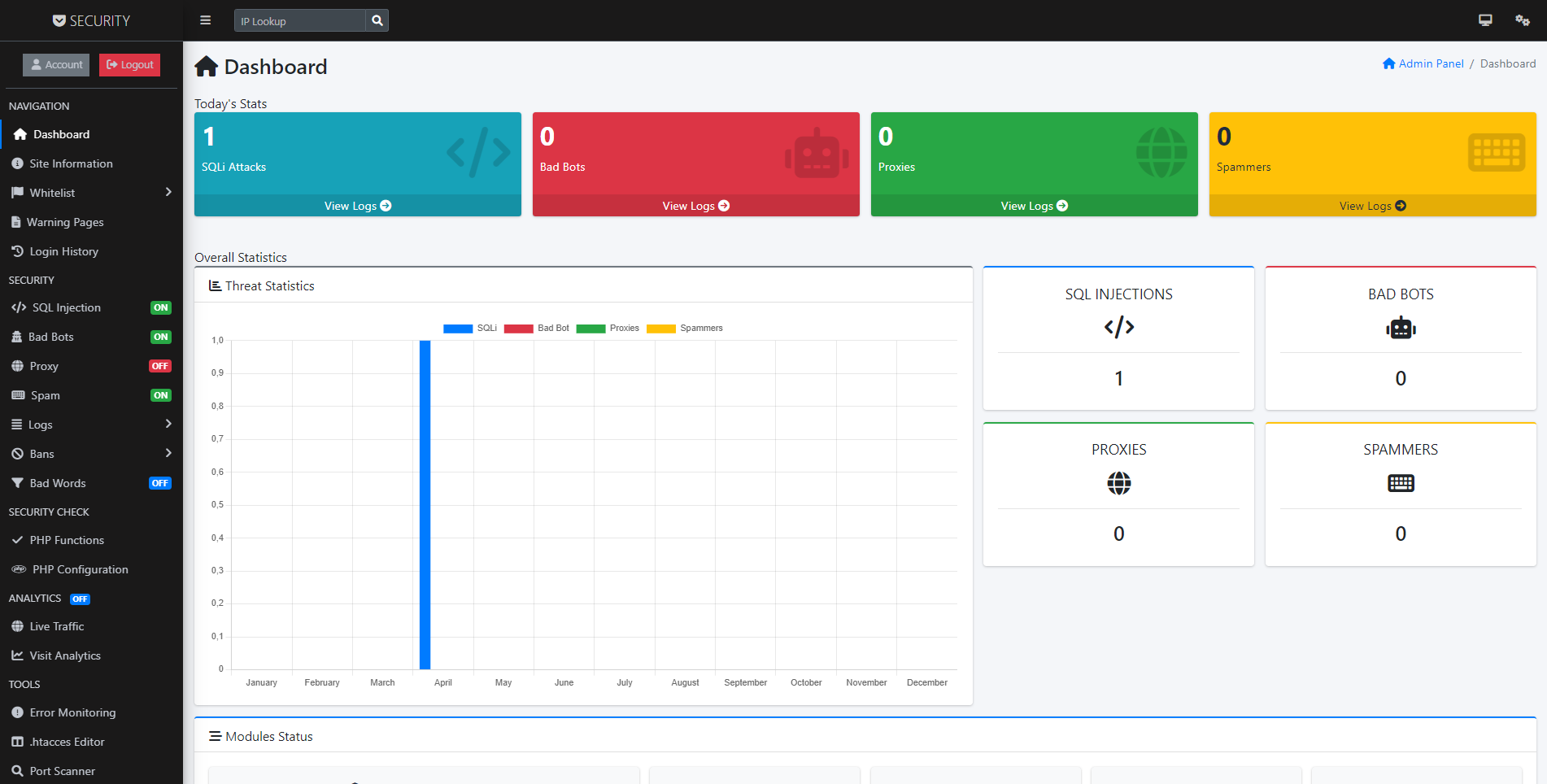
3. List of IP addresses;

4. Warning Pages;

5. Login History;

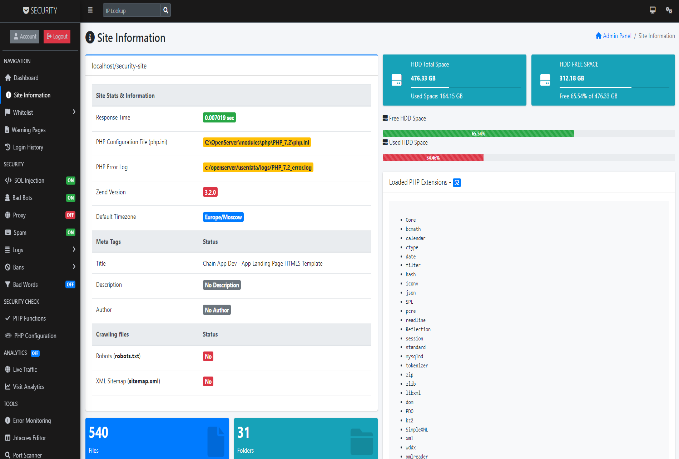
6. Security.

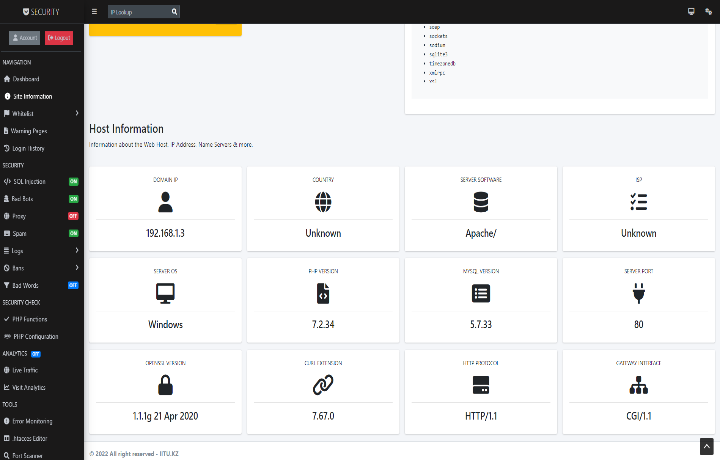
In the site panel section, users can see information about sources such as spammer, proxy distribution, bad bots, SQLi attacks statistics.



Site panel

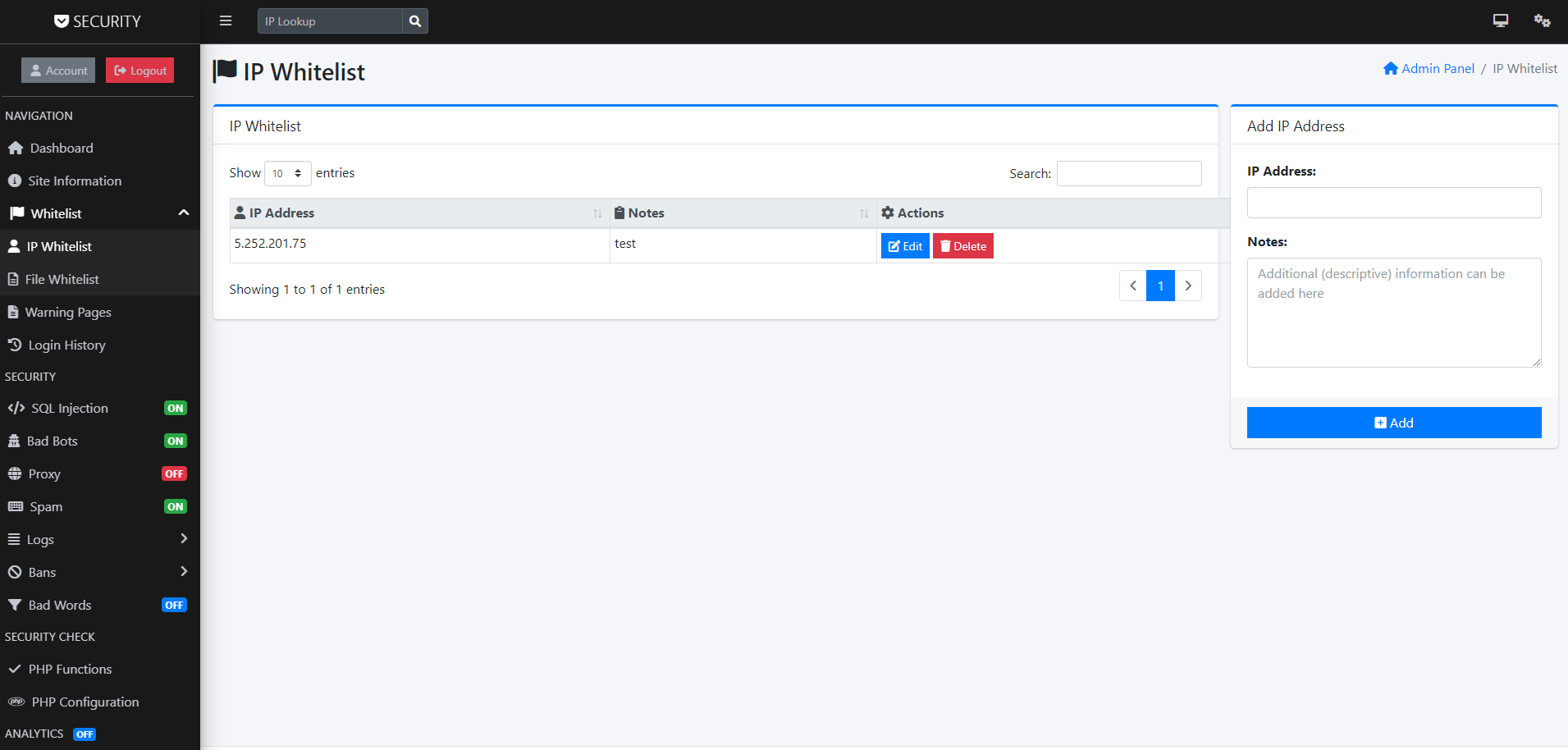
The next section is information about the site. In this section, users can get information about web host, IP address, name servers, country, http protocol, etc. These data are shown in figure below.





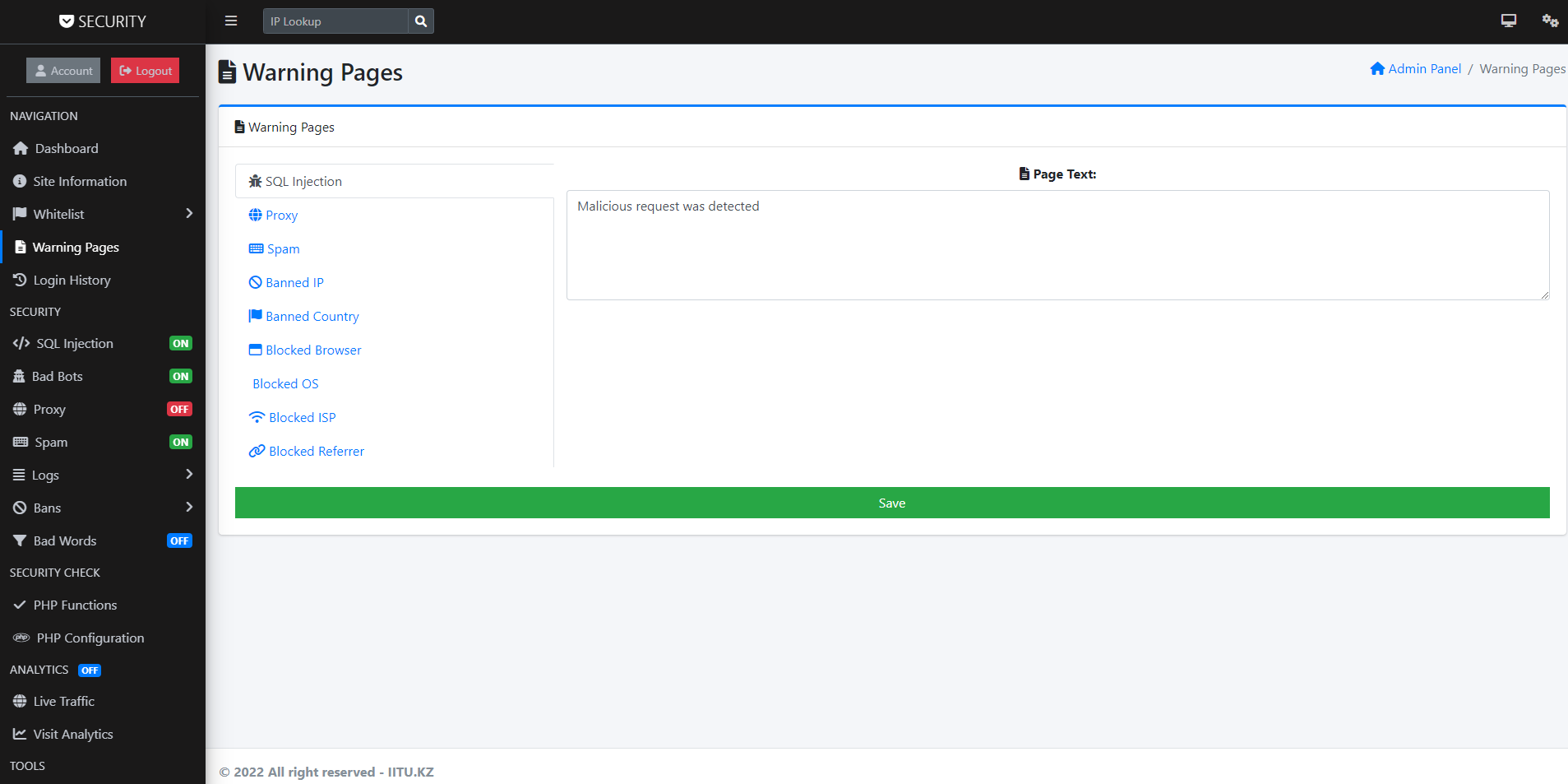
Site Information

Figure below shows a list of IP addresses. User can find other IP addresses here, edit and delete. User can also add an IP address.



List of IP addresses

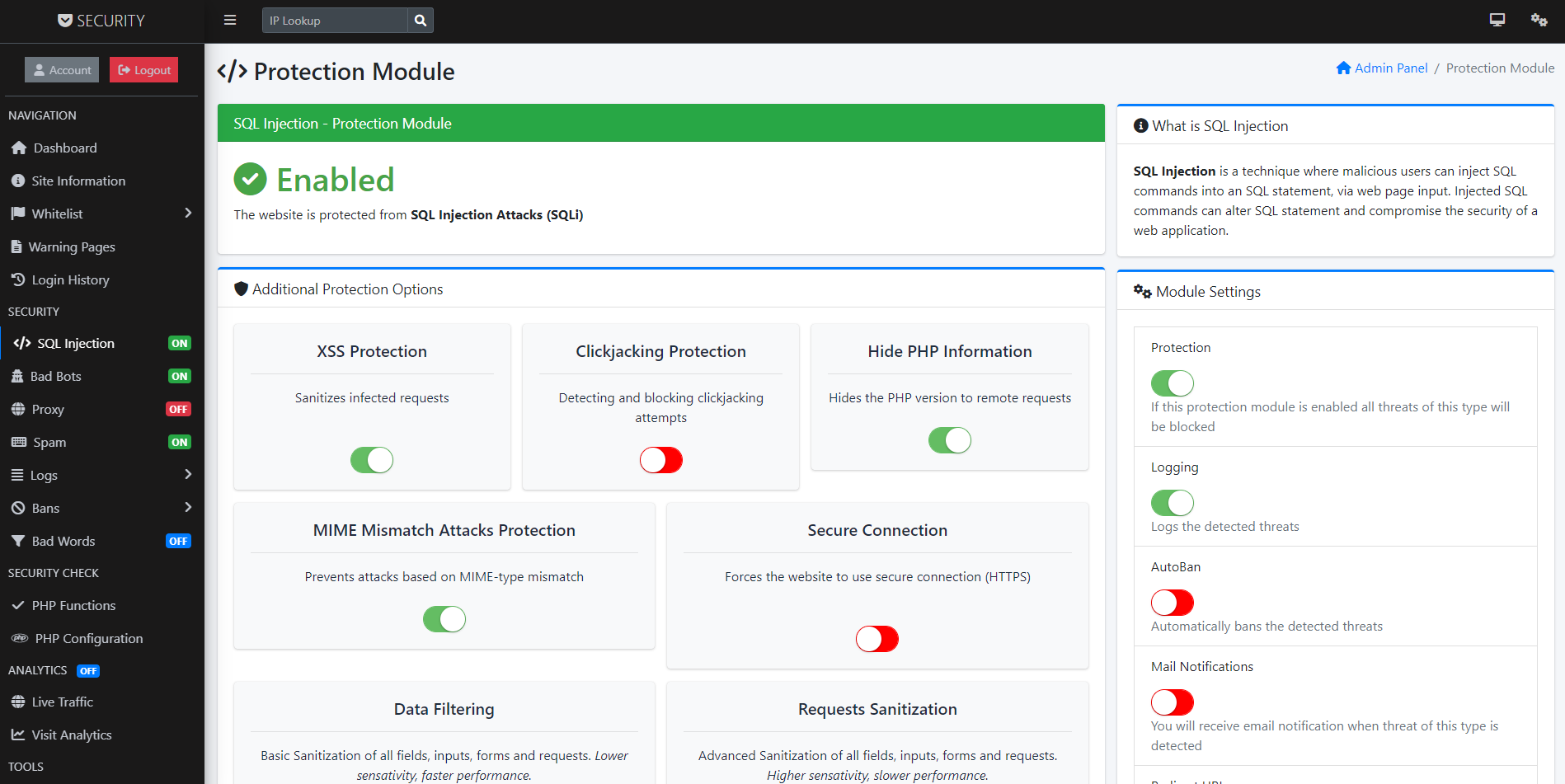
The "Warning Page" section shows information about proxies, spam, banned IPs, banned country, blocked browsers. It shows below.



Warning Pages

The next section is security. The security section itself is divided into several subsections such as: SQL injections, bad bots, proxies, spam, logs, bans and foul language.

SQL injection is a technique where attackers can inject SQL commands into an SQl statement through input from a web page. Embedded SQL commands can change the SQL statement and compromise the security of the web application.



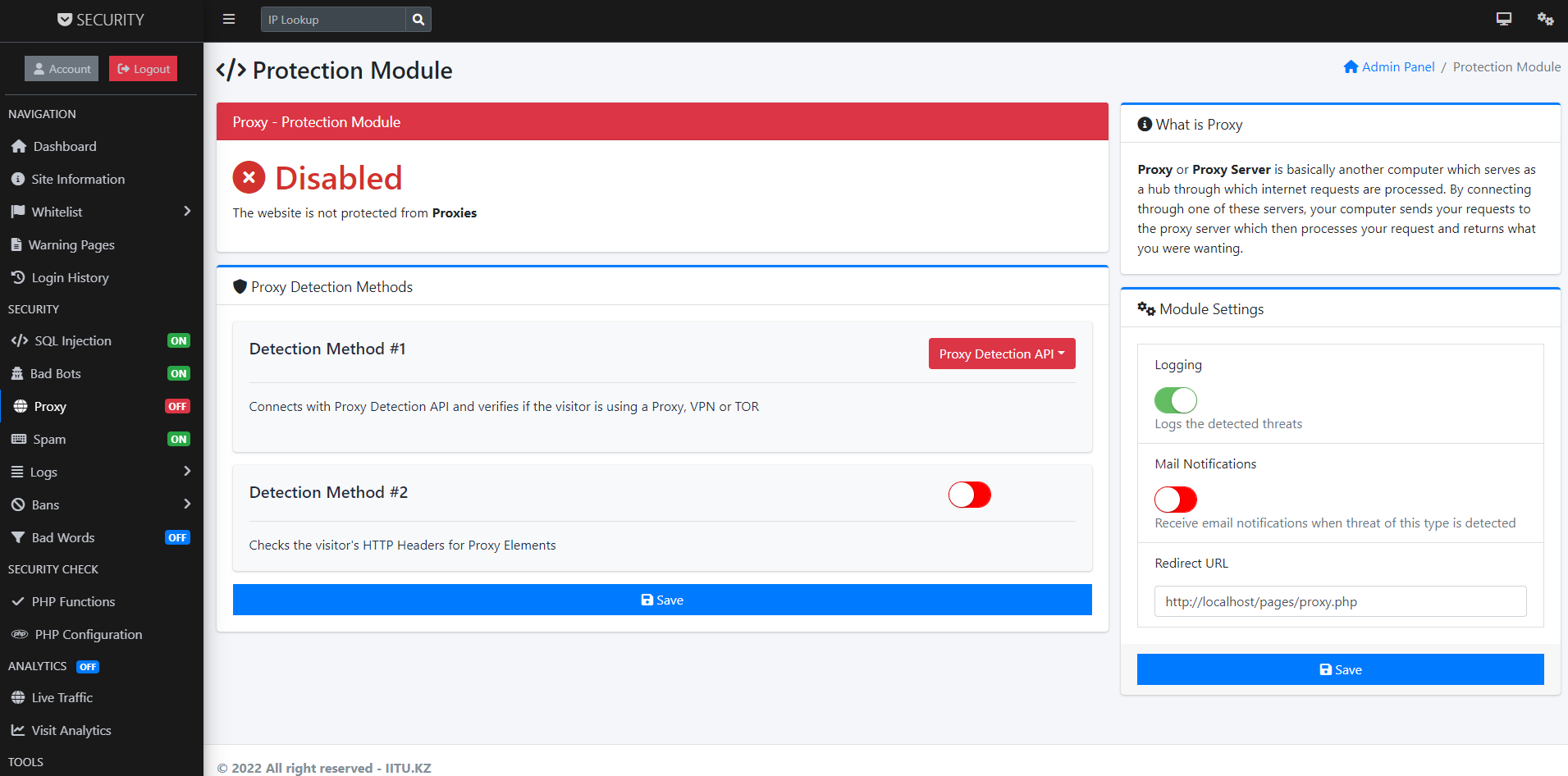
SQL injection section

Figure below shows the bad bots section. There are several protection options. These include: bad, fake and anonymous bots. These bots consume bandwidth, slow down user’s server, steal their content, and look for vulnerabilities to compromise their server.



Bad bots section

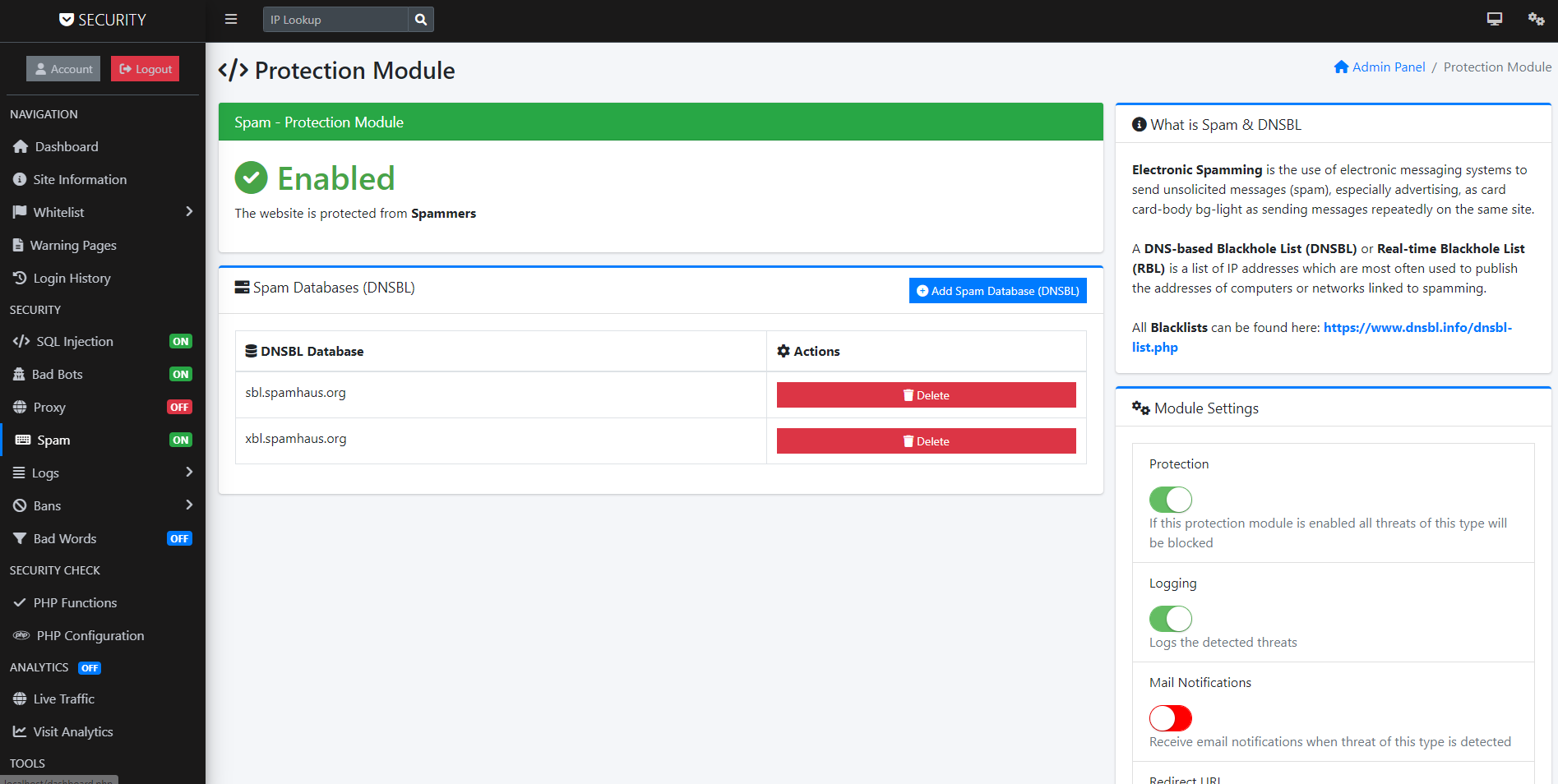
The next section is the proxy. A proxy server is another computer that acts as a hub through which Internet requests are processed. When user connect through one of these servers, his computer sends him requests to a proxy server, which then processes his request and returns what he wanted.



Proxy section

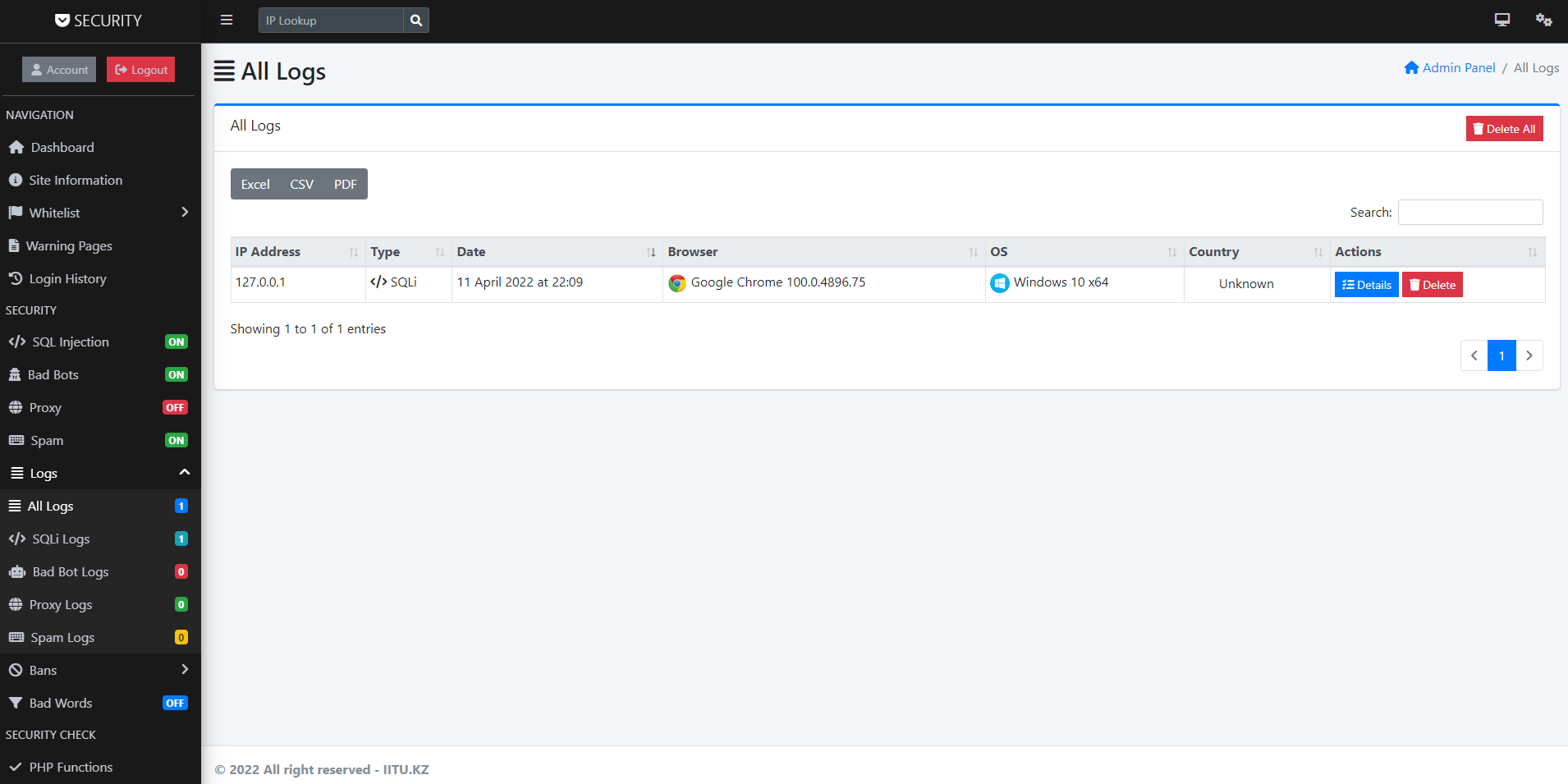
Figure below shows spam data, that is, this section contains spam databases. Electronic spam is the use of electronic messaging systems to send unsolicited messages (spam), especially promotional ones, in the form of a bg-light map-body map in the form of multiple messages sent to the same site.

DNS Based Blackhole List (DNSBL) or Real Time Blackhole List (RBL) is a list of IP addresses that are most commonly used to publish computer or network addresses associated with spamming.



Spam section

The next section is all logins. This section displays a list of all logins. That is, user can see the login information, the time and date of login, through which browser the login was made and the country. User can also delete this data.



Login subsection

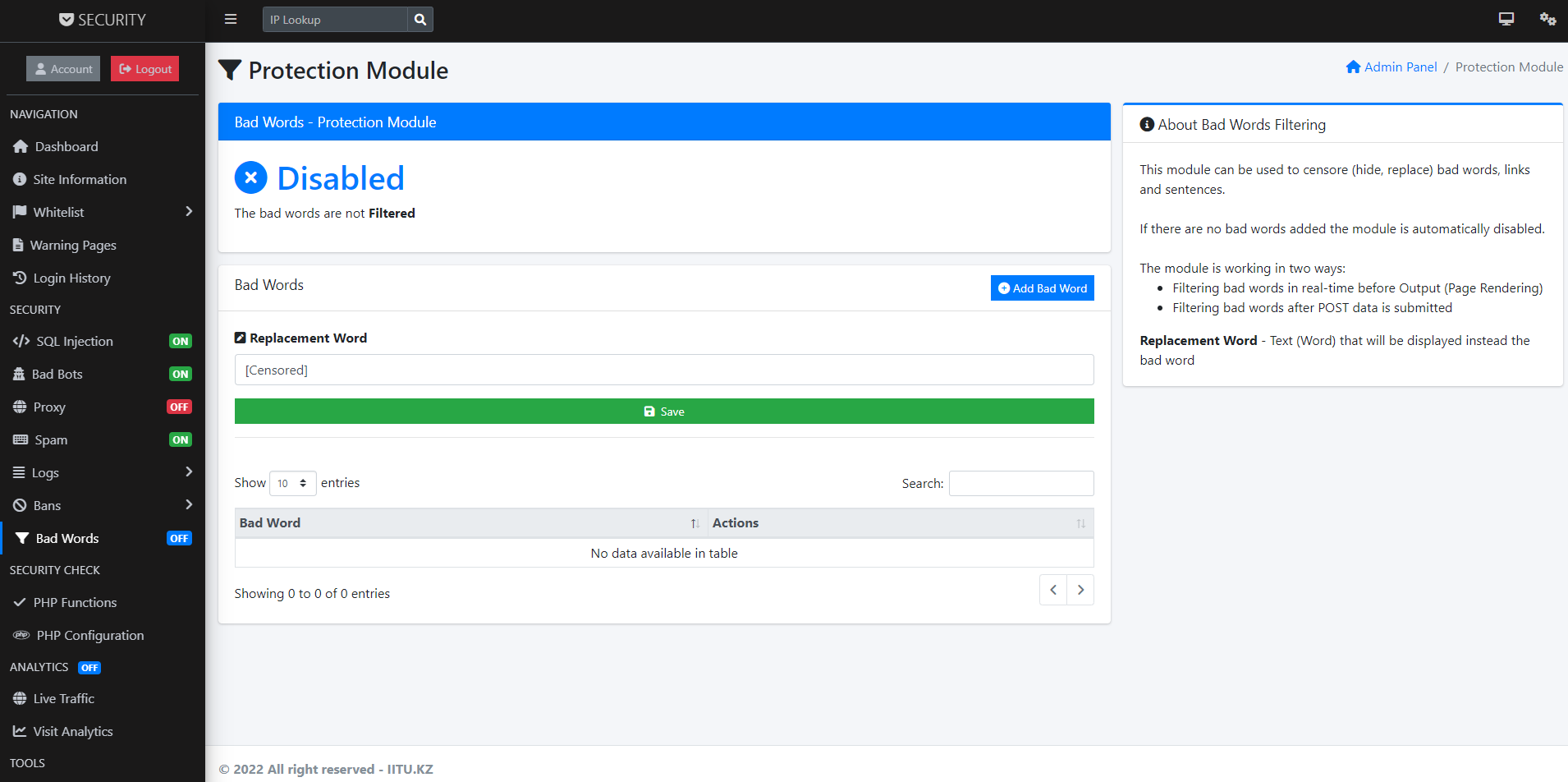
And the last section is - bad words, that is, filtering bad words. This module can be used to censor (hide, replace) bad words, links and sentences. If there are no bad words added, the module is automatically disabled.

The module works in two ways:

• Filtering bad words in real time before output (page rendering);

• Bad word filtering after POST data is sent.

Replacement word - the text (word) that will be displayed instead of the invalid word.



Bad words section

Next are shown the databases for implementing the site

Figure below - List of all tables in the database

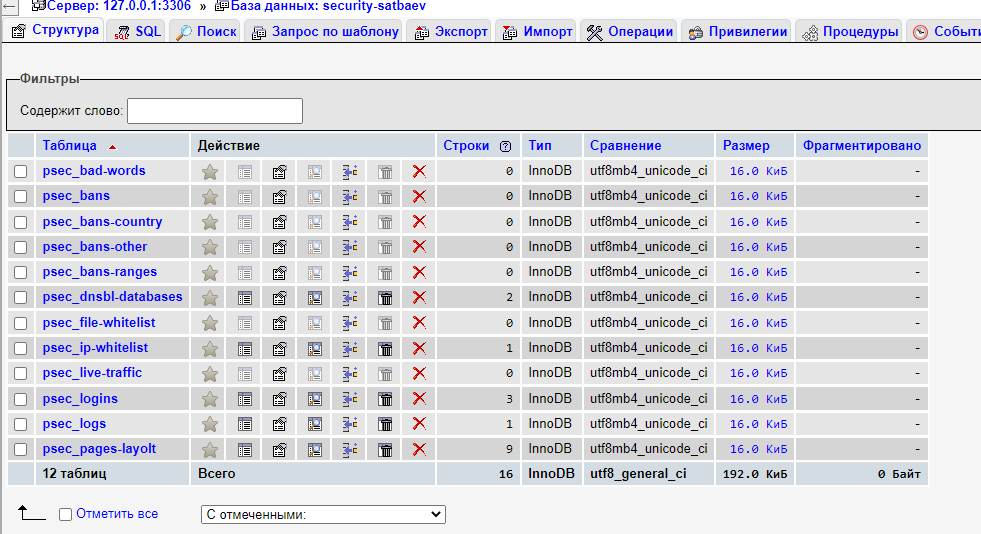


Figure below - Table of additional pages

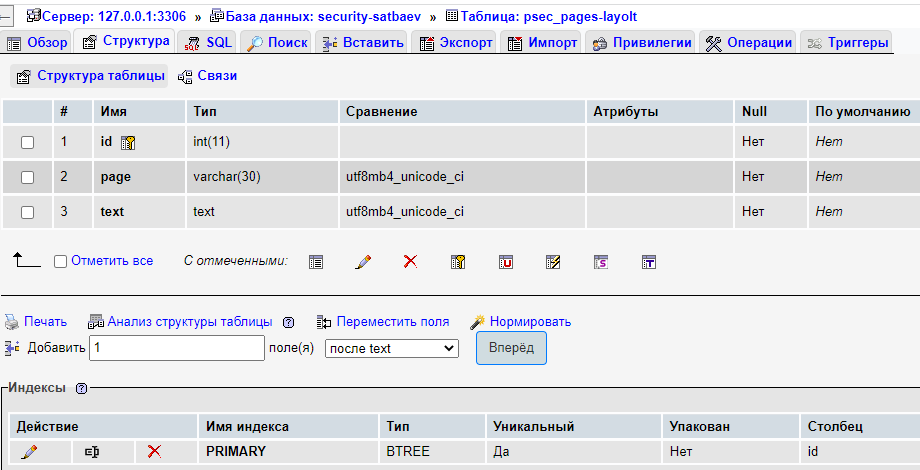


Figure below - Log diagram that tracks what is happening in the system

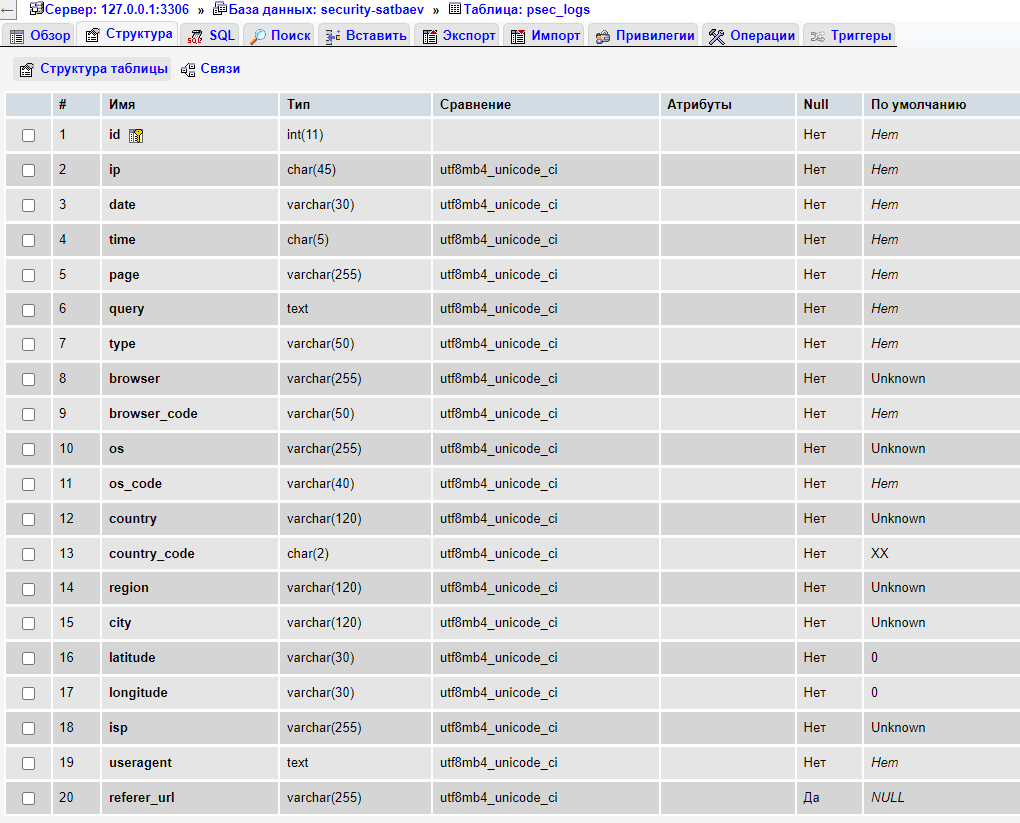


Figure below - Table fixing the authorization status in the system

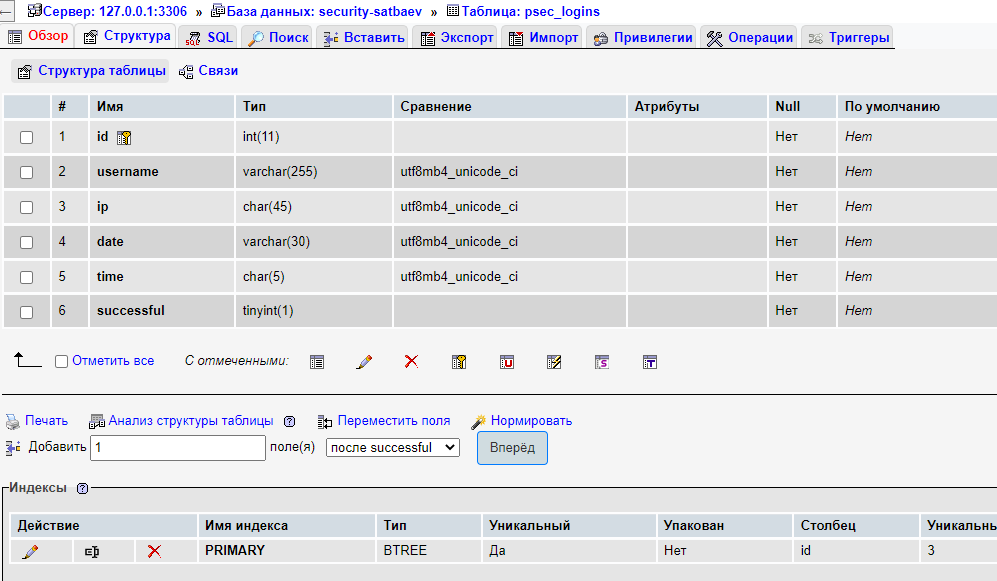


Figure below - Graph for tracking incoming and outgoing Internet traffic



Figure below - White list of IP addresses

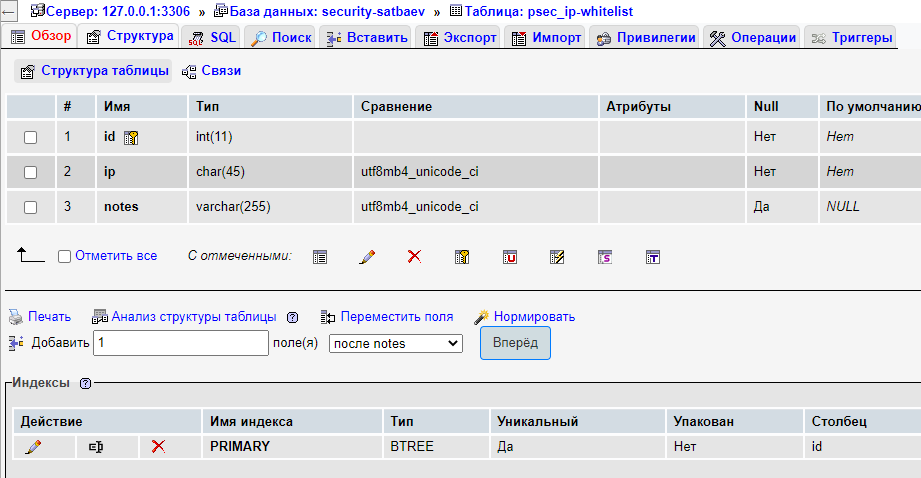


Figure below - White list of files

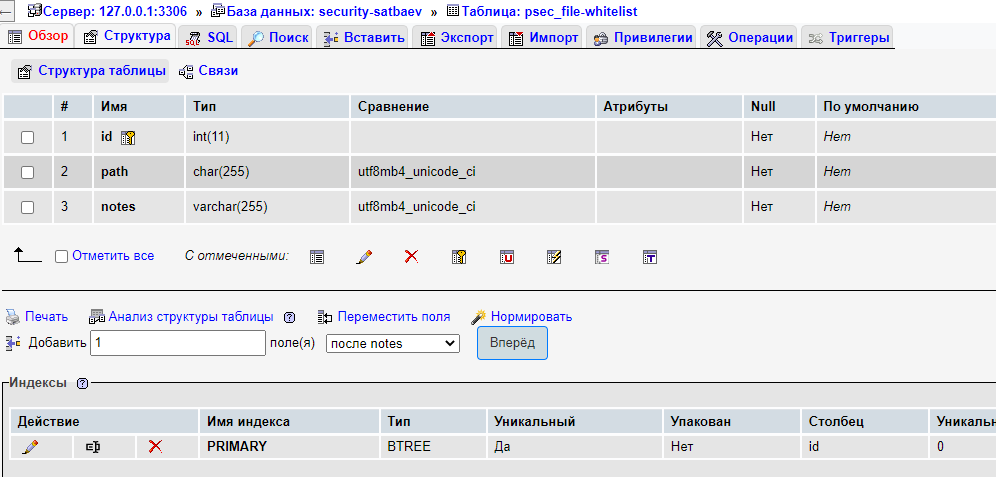


Figure below – Spam database storage table

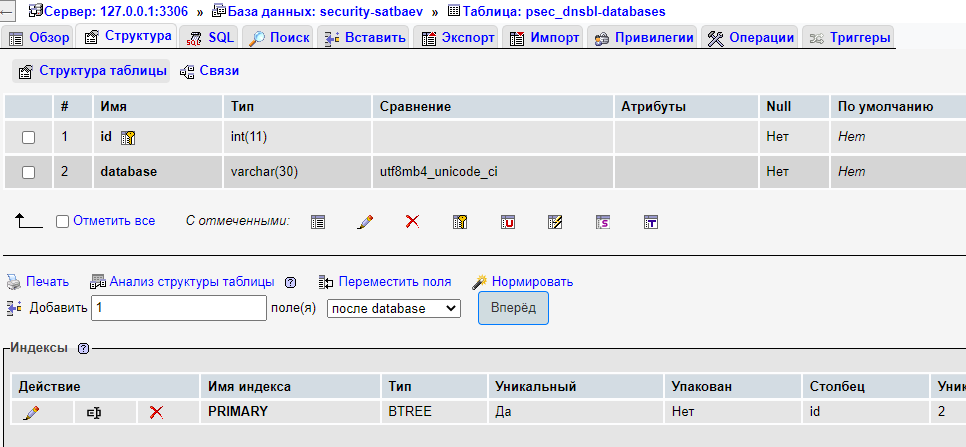


Figure below - Table that stores the range of IP addresses

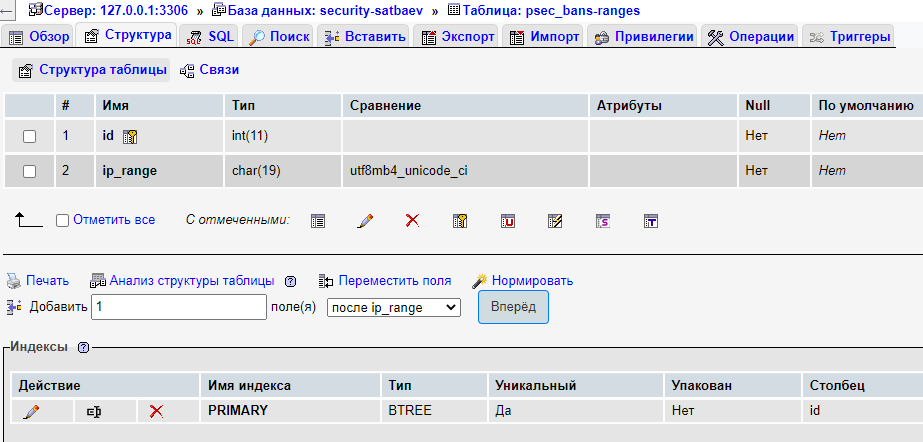


Figure below - Graph of the prohibition of activities in the system

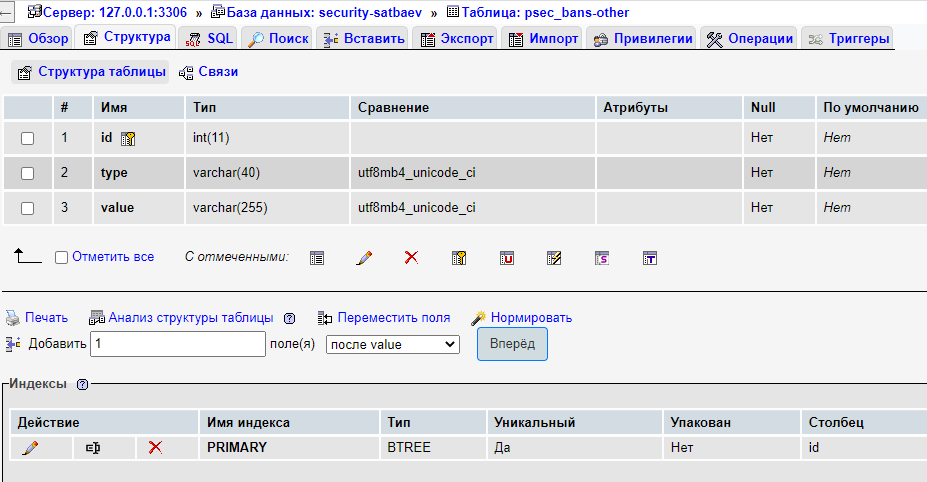


Figure below - Graph of blocking users by country

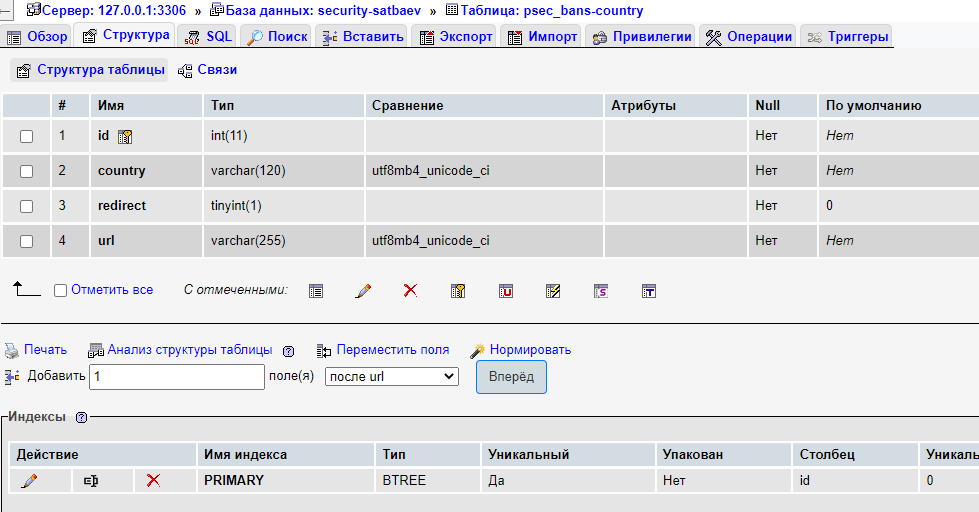


Figure below - Main ban chart

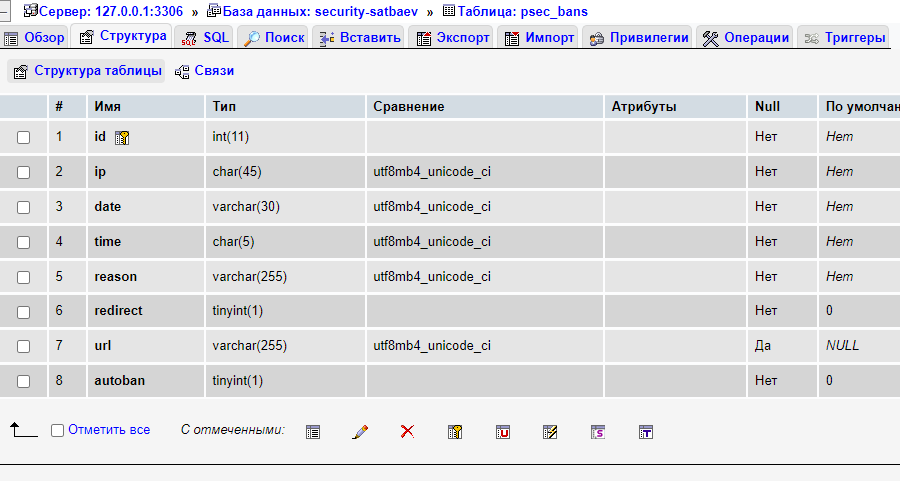
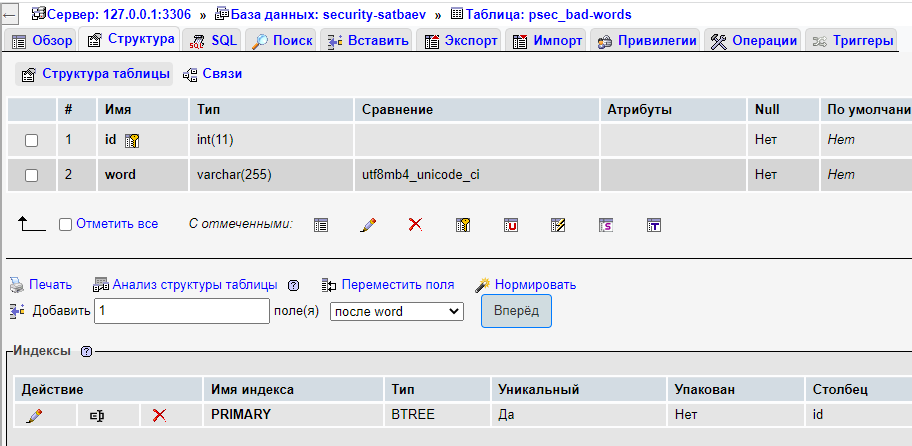


Figure below - Schedule for maintaining a list of obscene words in the system



## Algorithms for fraud detection

Bad words filter (modules bad-words.php)

This PHP code filters out bad words from the content and post data of a website. It first extracts the bad words from the database table named "psec\_bad-words". It then defines two functions, "bad\_words" and "badwords\_checker", to filter out bad words. The 'bad\_words' function replaces any bad word found in the content of a website with the value $settings['badword\_replace']. The "badwords\_checker" function checks the message data coming from the website for profanity and replaces it with $settings['badword\_replace'] if any. The $\_POST superglobal array is then passed through the "badwords\_checker" function to perform the filtering. Finally, the output of the functions is passed through the "ob\_start" function to filter the content of the website before it is sent to the user's browser.

badbots-protection.php

This code is a PHP script that implements protection against bad bots. The code checks if badbot\_protection is enabled (i.e. set to 1) and if so, creates an array of known bad bots.

The code then uses a foreach loop to loop through the array of bad bots and check for any bad bots in the user agent string. When a bad bot is detected, the code logs an event, blocks an IP address (if the autoban setting is enabled), sends an email notification (if the mail\_notifications and badbot\_mail settings are enabled), and redirects the user to the detected bad bot page. .

The code uses several functions not shown in the code snippet, including psec\_logging(), psec\_autoban(), and psec\_mail(). They likely handle the logging, autoban, and email notification features, respectively.

In general, the code provides a basic form of protection against known malicious bots by checking the user agent string against a predefined list of malicious bots and taking appropriate action if a malicious bot is detected.

ban-system.php

This is PHP code that implements various security measures to block access to a website based on various criteria.

1. The code checks if the user's IP address is in the list of banned IP addresses in the MySQL database. If the IP is banned, the user is redirected to the banned page and code execution is stopped.

2. The code then checks if the IP address belongs to the forbidden range of IP addresses in the database. If so, the user is redirected to the forbidden page.

3. If the site has country blocking enabled, the code checks the country of origin of the user's IP address using a third-party API. If the country is on the banned list, the user is redirected to the banned page.

4. The code checks if the user's browser is on the banned list in the database. If so, the user is redirected to the blocked page.

5. The code checks if the user's operating system is on the banned list in the database. If so, the user is redirected to the blocked page.

6. The code checks if the user's ISP is on the banned list in the database. If so, the user is redirected to the blocked page.

7. The code checks if the user's referrer URL is on the banned list in the database. If so, the user is redirected to the blocked page.

The code uses a MySQL database to store banned lists and redirects users to the appropriate pages based on criteria. It also uses a third party API to get the country of origin of the user's IP address. The code also uses caching of IP address information to reduce the number of API calls and improve performance.

core.php

This PHP code is used to retrieve information about a website visitor, including their IP address, browser and operating system information, referrer URL, page and path, date and time, and whether they are a bot search engine.

The code first checks various HTTP headers to determine the visitor's real IP address and then uses the library to get detailed information about their browser and operating system. It then formats and sanitizes the IP address and determines if it is IPv4 or IPv6.

The code also contains several functions for logging and handling security events, including automatically blocking IP addresses and sending notifications to website administrators.

fakebots-protection.php

This code is part of a PHP script designed to protect a website from fake bots. The code is activated if the site owner has enabled the "badbot\_protection2" setting.

If the script detects a fake bot, it sets the $type variable to "Fake Bot" and does the following:

If the database has the badbot\_logging setting enabled, the psec\_logging() function is called to log the detection of a fake bot to the site's database.

If the database has the badbot\_autoban setting enabled, the psec\_autoban() function is called to automatically ban the fake bot from accessing the site.

If the mail\_notifications and badbot\_mail options are enabled in the database, the psec\_mail() function is called to send an email notification to the website owner informing them that a fake bot has been found.

Finally, the code redirects the visitor to the website page "fakebot-detected.php".

life-traffic.php

This code is used to track live traffic on a website by recording visitor information such as IP address, country, device type, and browser information. It first checks if live traffic is enabled in the settings. If so, it looks up the visitor's country using the API and caches the result to a file. It then checks if the visitor is a bot by looking for certain keywords in the user agent string. It also detects the device type (computer, mobile device, or tablet) using the Mobile\_Detect library. Finally, it logs the visit by inserting visitor information and other data into a MySQL database table.

proxy protection.php

This is a PHP script that includes proxy protection measures for websites. The script checks if the visitor is using a proxy server to access the website, and if so, takes certain actions such as registering, email notifications, and redirecting the visitor to the specified page.

The script uses two methods to detect the use of a proxy. The first method involves API calls to various proxy detection services, including iphub.info, proxycheck.io, and iphunter.info, and comparing the results to see if the visitor is using a proxy. These API responses are cached using the visitor's IP address as a key. The second method involves checking certain HTTP headers that are typically added by proxies, including HTTP\_VIA. If any of these headers are present in the visitor's request, the script assumes that the visitor is using a proxy.

The specific actions that the script takes can be configured with various options, including the level of proxy protection you want, whether to log proxy usage, and whether to send email notifications when a proxy server is detected. The script also allows you to customize the page that visitors are redirected to when it detects the use of a proxy.

spam protection.php

Checks for spam protection. It first checks to see if `$settings['spam\_protection']` is equal to 1. If so, it proceeds to query the `$dnsbl\_lookup` database table to get all entries from blacklisted DNSBL databases. It then converts the client's IP address into a reverse string format. For each DNSBL host in the `$dnsbl\_lookup` array that exists in the reverse IP string as a domain name, the `checkdnsrr()` function is called to perform a DNS record lookup. If a DNS entry is found, it means that the IP address is blacklisted and the user is considered a spammer. The script then does the following:

- logs a try if `$settings['spam\_logging']` is equal to 1 by calling the `psec\_logging()` function

- sends an email notification if `$settings['mail\_notifications']` and `$settings['spam\_mail']` are equal to 1 by calling the `psec\_mail()` function

- redirects the user to the page specified in `$settings['spam\_redirect']`

sqli protection.php

Performs SQLi security. It first checks to see if the value of `$settings['sqli\_protection']` is equal to 1. If so, it does the following:

- sets headers for XSS protection, clickjacking protection and MIME type mismatch protection based on the values of `$settings['sqli\_protection2']`, `$settings['sqli\_protection3']` and `$settings['sqli\_protection4' ]`, respectively

- clears all fields and queries if `$settings['sqli\_protection7']` is equal to 1

- cleans and sanitizes input if `$settings['sqli\_protection8']` is equal to 1 by calling `cleanInput()` and `sanitize()`

- looks for malicious patterns in the query string specified in the $patterns array. If the template is found, the script does the following:

- logs a try if `$settings['sqli\_logging']` is equal to 1 by calling the `psec\_logging()` function

- automatically bans the user if `$settings['sqli\_autoban']` is equal to 1 by calling the `psec\_autoban()` function

- sends an email notification if `$settings['mail\_notifications']` and `$settings['sqli\_mail']` are equal to 1 by calling the `psec\_mail()` function

- redirects the user to the page specified in `$settings['sqli\_redirect']`

test-integration.php

The code creates a simple web page with a green box in the center that says "SECURITY integration done correctly." The CSS style is inline and defines the properties of the box, including its position, border style and color, background color, text alignment, font color and size, and width. The #psec\_confbox selector refers to the paragraph element with the id "psec\_confbox". This style is then rendered on the page using the PHP "echo" function. Finally, the message itself is displayed using another "echo" statement.

## Integration

These lines of code must be entered in the index.php file on any site:

include "security/config.php";

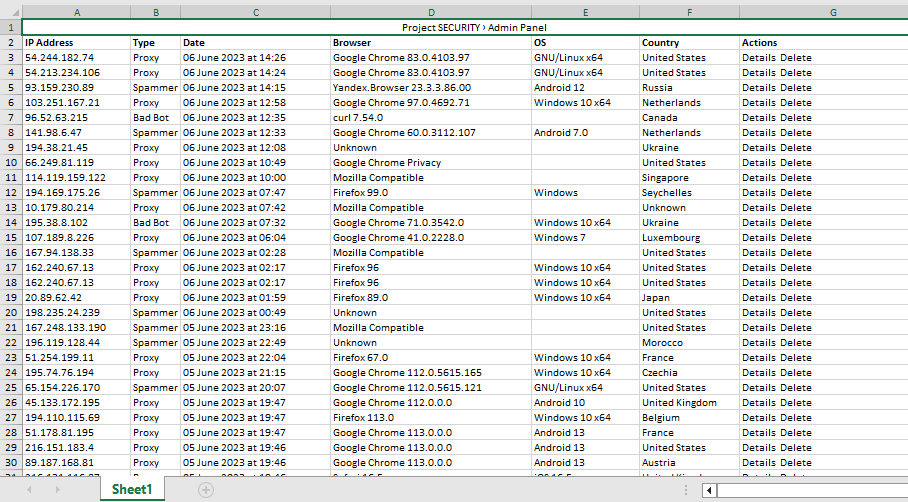
include "security/project-security.php";

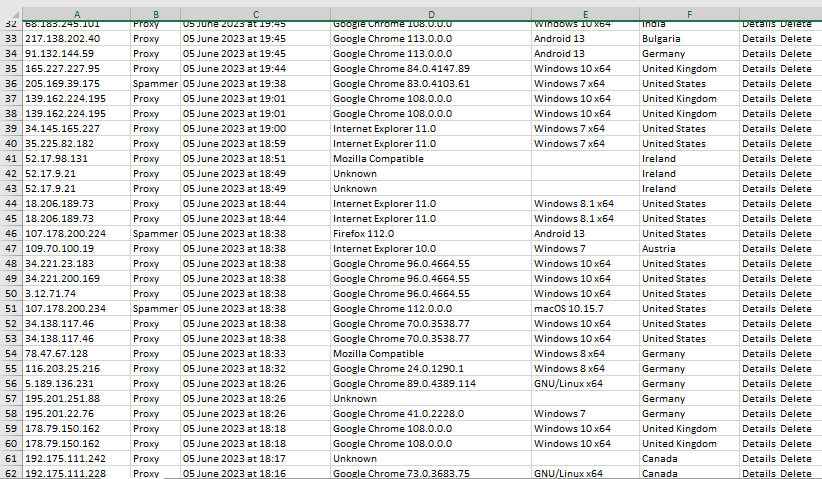
It's not integrating a module as a plugin or extension; it's just connecting the module directly through the entry point.

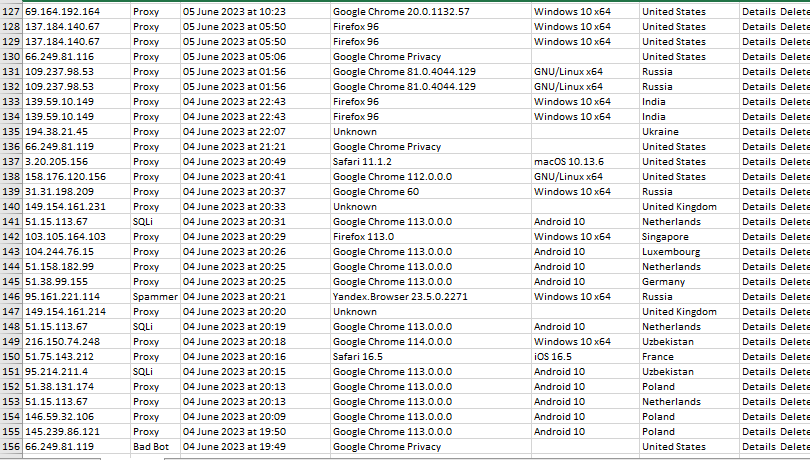
Integration is written as a separate plugin and connected through the site config or CMS

## Statistics of traffics

For making traffics I used website https://marlene.pw/ of my co-mentor from Technovation project. So, I have an access to it. This is statistics for now

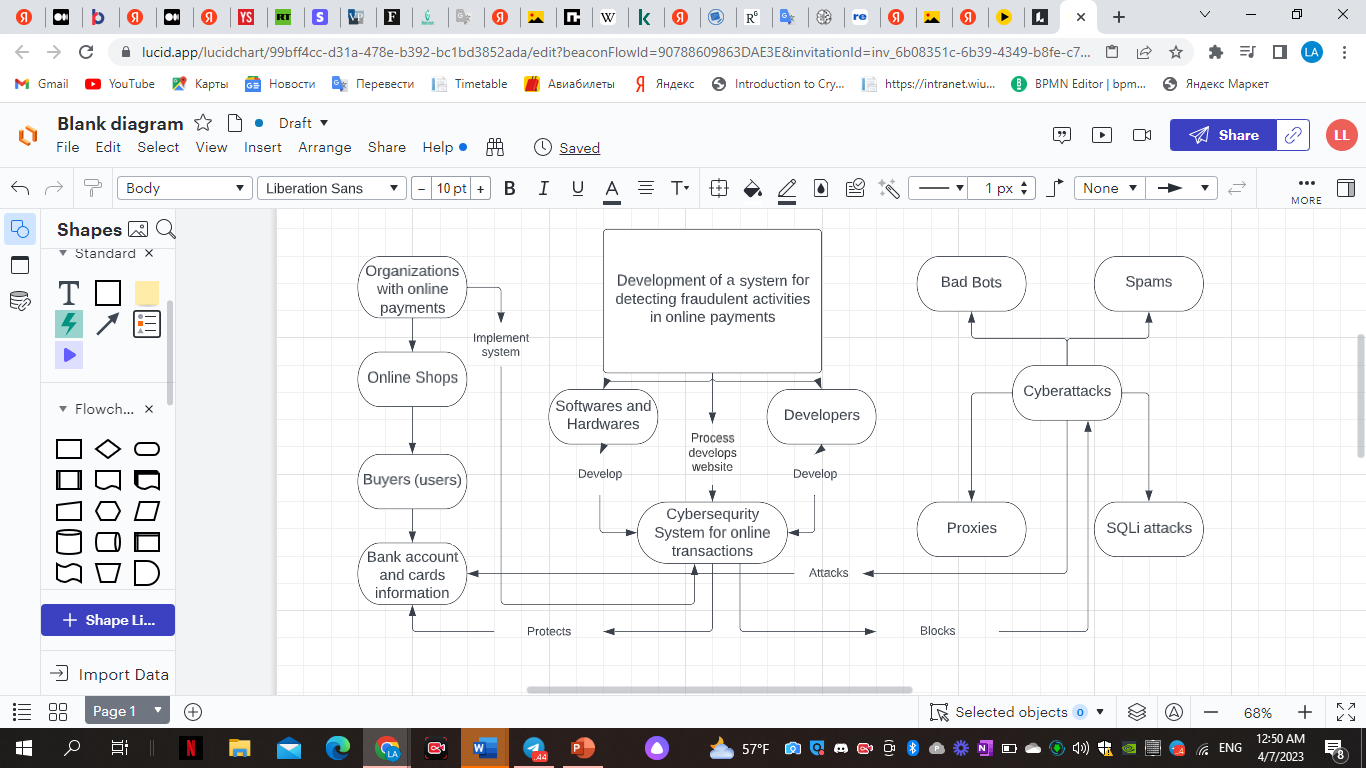




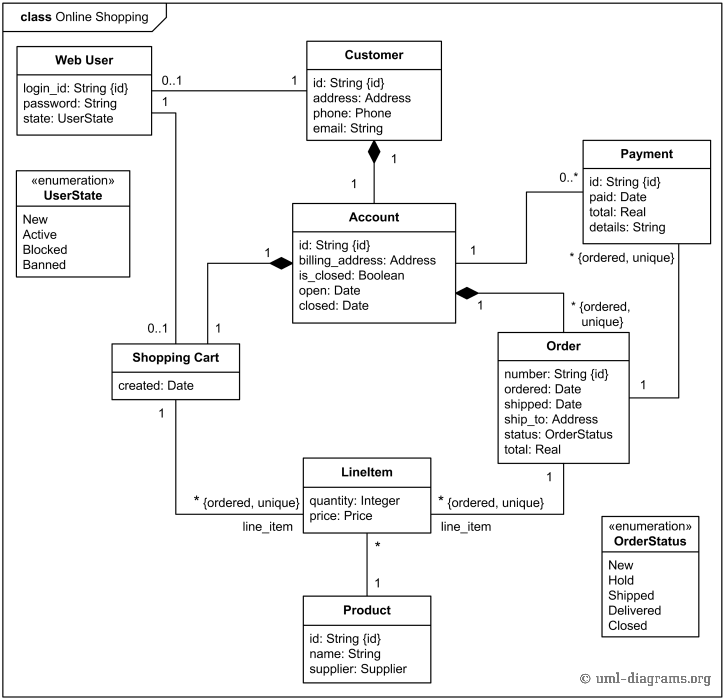


# Diagrams

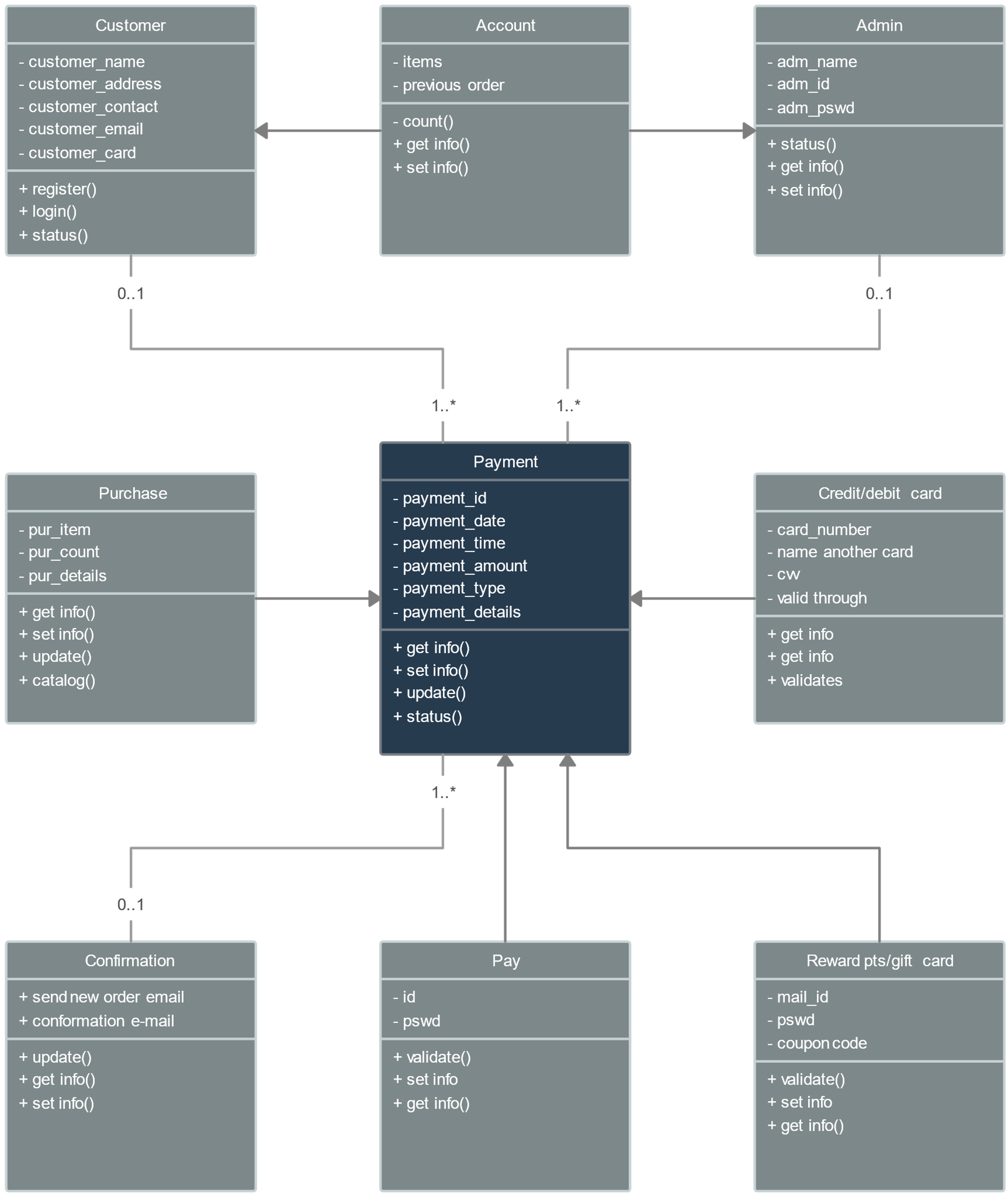
## Concept Map



## UML diagrams

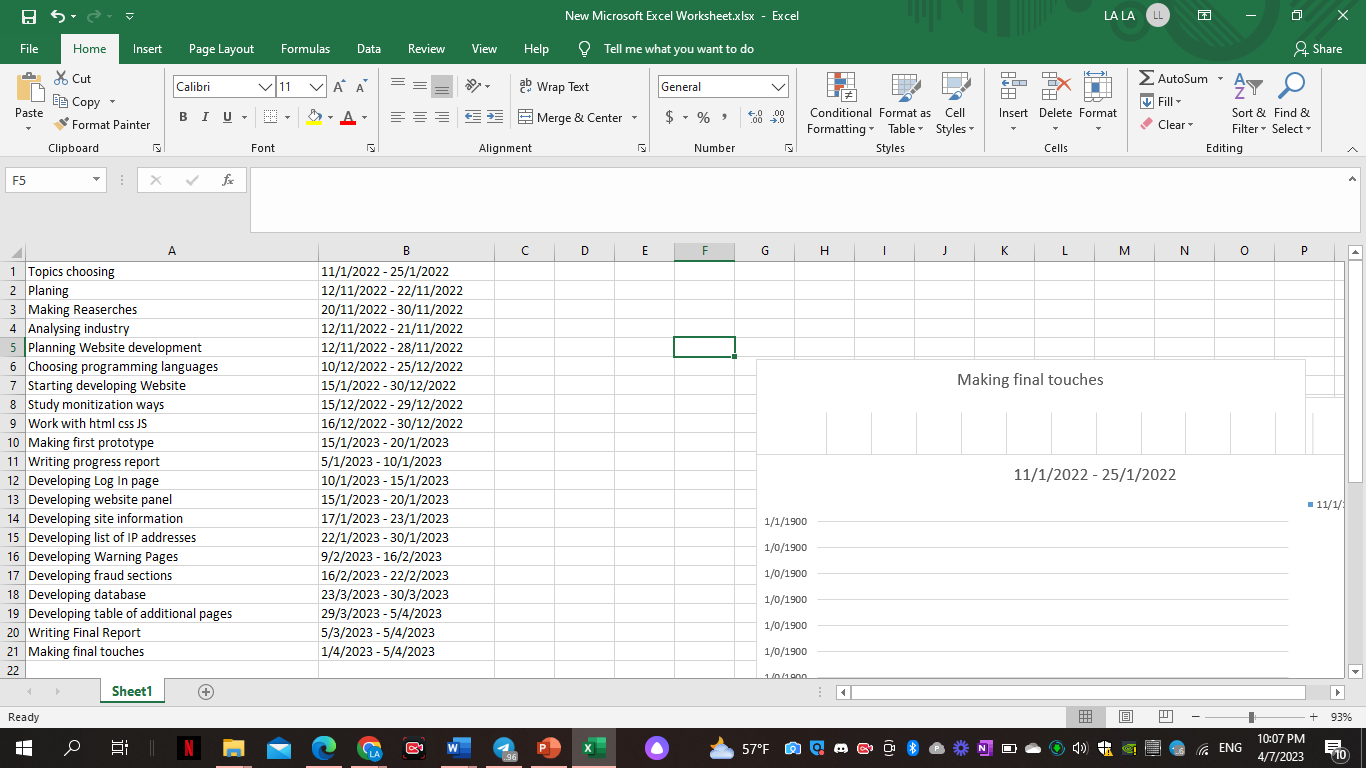


*uml-diagrams.org*



*Kasun Nishshanka*

## Project schedule



# Critical Self Evaluation

## Psychological assessment

My original idea at first was different from the current one. At the beginning of the year, I wanted to develop a website that would help people deal with mental health issues. In the end, I decided to change direction and come up with something more original. But the main goal was to benefit the people from the project. Since last year I was a member of Technovation Central Asia, where we came up with a system for translating from ordinary language into sign language, this project taught me how important it is to think about the problems of the general public. This is the main goal of every profession.

I could develop a good program for mental health care, but I don't have a medical background and would require more medical research to present people with a useful and professional product.

Therefore, I decided to focus my efforts and study on cyber security during online payments. This industry is also suffering from cyber-attacks. This project helped me understand the value of every profession.

## Academic Grade

By taking on this project, I gained tremendous experience in the field of cybersecurity in online payment systems. This is a rather vulnerable industry that suffers from cyber-attacks more and more every year.

Taking this opportunity, I put into practice my knowledge of programming languages such as HTML, CSS, JS, which we took in the second semester of the first course. I practiced my knowledge of MySQL and learned a new programming language - PHP.

There were many difficulties, because I did not know how to combine everything, how to convey my thoughts through the development of the project. As a result, the website turned out to be successful. But there is work to be done in the future.

It is possible to increase the ways to protect against a larger type of fraud, as the site presents limited options.

# Conclusion

In this work, a study was conducted to identify fraudulent transactions related to payment cards. An important contribution to the development of the system is the creation of a practical system for detecting bank card fraud, as well as the use of real data on payment cards to evaluate the effectiveness of the system and demonstrate its effectiveness. This study is aimed at reducing the risks associated with financial losses and uncertainty in the day-to-day activities of institutions. The analysis used 13 statistical and methodological methods. Three sets of digital credit card data were used as benchmarks and were available in a public repository.

Online payment fraud can occur in a variety of ways depending on the type of fraud. This includes bankruptcy scams, theft/counterfeiting scams, application scams, and conduct scams. Each of these sub-categories of fraud has its own definition and details.

It is important to note that several types of credit card transactions and reference databases were used in this study. The same statistics and machine learning methods were used to evaluate performance. Moreover, feature selection was methodical. Feature selection is the key to identifying only important and non-redundant features to improve classification performance while optimizing the computational load for practical implementation.

In my opinion, the project achieved its goal of developing a system for detecting fraud in investigations. However, various types of online payment fraud have been identified and alternative methods used to detect fraud have been explored. Meanwhile, other goods such as consumer finance and retail are also at risk, with serious ethical implications for banks and credit card companies that pay online. It is also planned to develop many other types of systems for detecting fraudulent activities in online payments.

# Reference List

Works Cited

“9 Local E-Commerce Marketing Tips to Drive More Foot Traffic to Your Store.” *Neil Patel*, 30 Mar. 2018, neilpatel.com/blog/drive-more-foot-traffic/.

Brawn, Jihn. “Infographic: Online Banking Rivals Physical Branch Banking.” *Statista Infographics*, 2020, www.statista.com/chart/amp/467/channels-used-for-investment-transactions/. Accessed 7 Apr. 2023.

“Что мешает развитию онлайн-коммерции в Узбекистане и как это исправить? Мнение экспертов.” *Spot – Деловые новости Узбекистана*, 15 Feb. 2018, www.spot.uz/ru/2018/02/15/e-commerce/. Accessed 7 Apr. 2023.

Golden. “Bitdefender Software Antivirus - Discover the Highly Rated Antivirus Software Program.” *Www.bitdefender.com*, www.bitdefender.com/media/html/consumer/new/2020/cl-offer-opt/?pid=60off&cid=aff%7Cc%7Cir. Accessed 7 Apr. 2023.

Hernandez, Jovan. “What Is Apache? In-Depth Overview of Apache Web Server.” *Sumo Logic*, 8 May 2019, translated.turbopages.org/proxy\_u/en-ru.ru.1173d5fa-64302078-0201528a-74722d776562/https/www.sumologic.com/blog/apache-web-server-introduction/. Accessed 7 Apr. 2023.

Howarth, Josh. “8 Huge Cybersecurity Trends (2022).” *Exploding Topics*, 8 Sept. 2021, explodingtopics.com/blog/cybersecurity-trends.

International Monetary Fund. “The IMF and the World Bank.” *IMF*, 2022, www.imf.org/en/About/Factsheets/Sheets/2022/IMF-World-Bank-New.

“Literature Review: Examples, Outline, Format | EssayPro.” *Essaypro.com*, 2022, essaypro.com/blog/literature-review.

Loggie, Nick. “Impact of Coronavirus (COVID-19) on ECommerce Businesses.” *Medium*, 25 June 2020, medium.com/@logz05/impact-of-coronavirus-covid-19-on-ecommerce-businesses-fae2082db9ee?source=post\_internal\_links---------3----------------------------. Accessed 7 Apr. 2023.

“Macy’s– Official Site.” *Macy’s*, 2021, www.macys.com/.

Moran, Claudio. “Vulnerabilities in Online Payment Systems.” *Medium*, 7 Oct. 2022, medium.com/@claudio\_moranb/vulnerabilities-in-online-payment-systems-edd2d3c06905. Accessed 7 Apr. 2023.

Nyxone. “Importance of E-Commerce and Online Shopping and Why to Sell Online.” *Medium*, Medium, 13 Apr. 2017, medium.com/@nyxonedigital/importance-of-e-commerce-and-online-shopping-and-why-to-sell-online-5a3fd8e6f416.

Pereira, Daniel. “Canva Business Model.” *The Business Model Analyst*, 26 Aug. 2021, businessmodelanalyst.com/canva-business-model/.

Shein. “About Us | SHEIN USA.” *Shein.com*, 2019, us.shein.com/About-US-a-117.html.

Sowards, Andy, and infinigeek. “ID Fraud Hits Online Shoppers.” *InfiniGEEK*, 23 Mar. 2017, infinigeek.com/id-fraud-hits-online-shoppers/?noamp=mobile. Accessed 7 Apr. 2023.

Works Cited

Brooks, Chuck. “Cybersecurity Trends & Statistics for 2023; What You Need to Know.” *Forbes*, www.forbes.com/sites/chuckbrooks/2023/03/05/cybersecurity-trends--statistics-for-2023-more-treachery-and-risk-ahead-as-attack-surface-and-hacker-capabilities-grow/?sh=2aa8d57e19db. Accessed 7 Apr. 2023.

Kaspersky. “Kaspersky Cyber Security Solutions for Home and Business | Kaspersky.” *Www.kaspersky.co.uk*, www.kaspersky.co.uk/?ignoreredirects=true. Accessed 7 Apr. 2023.

Maurer, Tim, and Arthur Nelson. “The Global Cyber Threat to Financial Systems – IMF F&D.” *Www.imf.org*, 2021, www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer.htm.

Website. “Log In.” *Lucid.app*, 2023, lucid.app/documents#/documents.

Wiwanto, Frans. “Council Post: As Pandemic Continues, Scams Do Too.” *Forbes*, www.forbes.com/sites/forbesfinancecouncil/2021/05/17/as-pandemic-continues-scams-do-too/?sh=16bcd94240f8. Accessed 7 Apr. 2023.